



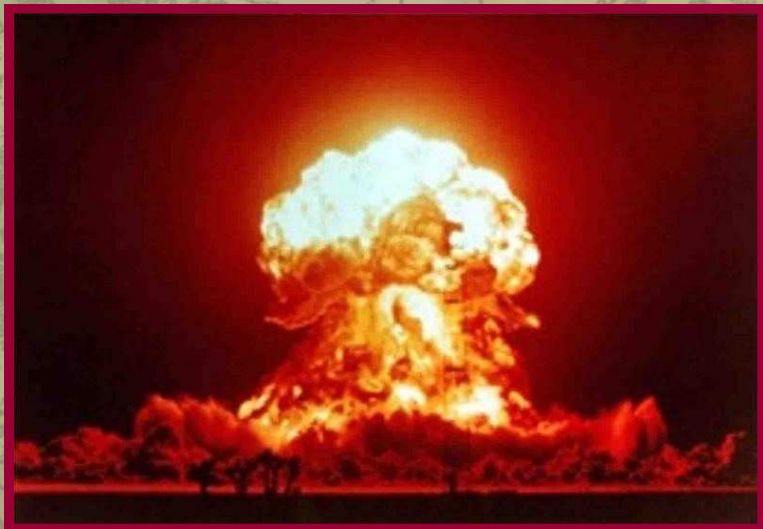
Koninklijk Hoger Instituut voor Defensie



DEFENSIE
VOORRANG AAN VREDE

VEILIGHEID & STRATEGIE
SÉCURITÉ & STRATÉGIE

Nr 100
Juni 2009



**Massavernietigingswapens:
erfenis van de Koude Oorlog
en bedreiging voor de toekomst**

Bart Smedts

.be

ISSN : 0770-9005

**Massavernietigingswapens:
erfenis van de Koude Oorlog
en bedreiging voor de toekomst**

Bart Smedts



Koninklijk Hoger Instituut voor Defensie
Studiecentrum voor Veiligheid en Strategie

Renaissancelaan 30
1000 Brussel



Executive Summary

Since the terrorist attacks in the Tokyo subway of 1995, the frightening consequences of possible use of Weapons of Mass Destruction (WMD) by non-state actors became very real. During the Cold War, WMD were exclusively state ownership. The collapse of the Soviet-Union added an erratic parameter to security issues: weapons under stringent control have become unwanted economic burdens for new States in the Russian Federation. Yet, they may become available on black markets.

The major cause which could possibly initiate a new cascade of proliferation is materialized by the multiplicity of political and (geostrategic) security issues in scattered areas: the covert nuclear weapons programs of North-Korea (DPRK) and Iran, for example, have a major impact on the attitude of direct neighbours and their security considerations. Existing WMD capacity is still a relic from the Cold War: the major operational stockpiles can be found in the five nuclear weapon states, permanent members of the UN Security Council (P5). Additionally, nuclear stockpiles are available in *de facto* nuclear weapon states, i.e. states which own the capacity without being signatory of the Non-proliferation Treaty (India, Pakistan and Israel).

In addition to this state-owned CBRN(E)-threat, terrorist activities have an indirect CBRN(E) capacity on both troops in operation, and civilians, not only in regions of conflict but also in homeland activities. In this framework, Homeland preparedness can be compared to force protection in CBRN(E) environment. Hence, the sequence of actions and materiel that has to be put on scene is comparable. In addition, experience from abroad can be helpful to create additional value for preparation and execution of plans. The minimum requirements for an appropriate action plan encompass a diversity of disciplines as Risk Management Monitoring, Protection for personnel and environment, Render Safe & Disposal of explosives and CBRN material or toxics, Hazard Management, Detection and Sampling and Identification forensics.

The efforts to contain WMD threats can be supported by a strengthened nonproliferation regime. The existing cold war legacy of WMD stockpiles does not necessarily constitute a threat for the future: in that respect, essential upcoming meetings such as the NPT Review Conference in 2010, the BTWC Review Conference of 2011 and the CWC Review Conference of 2013, should not be neglected in order to avoid the “cascade of proliferation”. The position of the new US Administration and a strong common position of the EU will be key elements in the process of confidence building, to manage course changes towards progress and take a stand in the reinforcement of the non-proliferation regime.



Inhoudstafel

Lijst van afkortingen	1
Inleiding	3
DEEL 1: DEFINITIES, PROLIFERATIE, CAPACITEITEN EN TRANSFERS	5
1.1. Definities	7
1.1.1. WMD : Massavernietigingswapens	7
1.1.2. Vectoren voor massavernietigingswapens	9
1.2. Proliferatie van WMD en vectoren	12
1.3. Capaciteiten van landen en invloedsfactoren	19
1.3.1. Capaciteiten van landen	19
1.3.2. Invloedsfactoren	20
1.3.2.1. Motivatie tot verwerving van de capaciteit	20
1.3.2.2. Indicatoren voor de verwerving van de capaciteit	22
1.3.2.3. Voorbeelden: “Declared weapon states”, “NPT-states”, “Non-NPT-states” en “Non-nuclear NPT-states”	25
1.3.2.4. Gevolgen voor een (nucleaire) non-proliferatie strategie en de bedreiging	27
1.3.2.5. Gevolgen voor de bedreiging binnen de EU	28
1.4. Transfers van kennis, technologie en materieel	29
1.5. Deelbesluit	34
DEEL 2: CONCEPT “INDIRECTE BEDREIGING” EN PREVENTIE	39
2.1. “Indirecte CBRN-dreiging”	41
2.1.1. Noodplanning en het CGCCR	45
2.1.2. Risico-evaluatie en risicobeheer (Risk Management Monitoring)	51
2.1.3. Beveiliging voor personeel en de omgeving met inbegrip van veiligheidsperimeters (Protection and security)	53
2.1.4. Het ontwapenen van explosieven en het beveiligen van CBRN materiaal (Render Safe & Disposal)	57
2.1.5. Inperking van besmetting en decontaminatie (Hazard management)	58
2.1.6. Detectie en staalname (Detection & Sampling)	60
2.1.7. Sporenonderzoek (Identification forensics)	61
2.1.8. Nabeschouwingen en bestaande plannen	62
2.2. Initiatieven voor preventie en strijd tegen proliferatie	65
2.2.1. Verenigde Naties	65
2.2.2. Europese Unie	71
2.2.3. NAVO	77
2.2.4. OVSE	81
2.2.5. Nationaal	83
2.3. Deelbesluit	84

DEEL 3 : BELEIDSONDERSTEUNENDE AANBEVELINGEN	87
3.1. Tactische aanbevelingen	89
3.1.1. Noodplanning C ²	89
3.1.2. Aankopen	89
3.1.3. Communicatie op de site van een CBRN incident	90
3.1.4. Sensoren	90
3.1.5. Beschikbaarheid van de informatie	92
3.1.6. Bescherming van het personeel	93
3.1.7. Beveiliging van luchthavens	94
3.1.8. Beveiliging van operationele zones, beschoten met verarmd uranium (DU) : informatieberichten omtrent het gebruik van DU-munitie	94
3.2. Strategische aanbevelingen	95
3.2.1. Wapenwet	95
3.2.2. Nuclear fuel cycle management	96
3.2.3. Internationale verdragen : consolidatie en uitbreiding	97
3.2.4. WMDC samenwerking en nationale vertegenwoordiging	102
3.2.5. “Soft proliferation”	102
3.2.6. Naar een cel risicoanalyse en bescherming kritische infrastructuur (CIP)	103
3.2.7. Welke cellen in CGCCR?	104
3.2.8. Noodplanning CBRN	105
3.2.9. ECDC en bioveiligheid	105
3.2.10. Tijdige waarschuwingsnetwerken : rationalisatie en integratie van verschillende ketens	106
3.2.11. Naar een Europees « Department of Homeland Security » (EDHS) ?	108
3.3. Deelbesluit	110
ALGEMEEN BESLUIT	111
BIJLAGEN:	115
Bijlage 1: Tabel WMD-capaciteiten van landen	117
Bijlage 2: Tekst uitbreiding van het NPT	119
Bijlage 3: Smokkelroutes “Khan-netwerk”	120
Bijlage 4: Confirmed incidents involving HEU and Pu (1993-2006)	121
Bijlage 5: Europese definities kritische infrastructuur	122
Bijlage 6: CBRN-oefeningen in de VS	126
Bijlage 7: Voorbeeld van organisatie van een zone	128
Bijlage 8: Nationale en internationale organen betrokken in noodplanning en WMD/CBRN aangelegenheden (niet exhaustief)	129
Bijlage 9: VN structuur “verdediging tegen terrorisme”	130
Bijlage 10: Instrumenten van de EU in het “CBRN Inventory”	131
Bijlage 11: NATO CBRN defence en NON-proliferatie	144
Bijlage 12 : OVSE Charter voor de strijd tegen het terrorisme	148
BIBLIOGRAFIE:	153
Officiële documenten	155
Boeken	157
Artikels uit tijdschriften en pers	159
Jaarboeken	162
Internet sites	163
Toespraken en conferenties	164
Interviews	165



Lijst van afkortingen

ADR	Accord européen relatif au transport international des marchandises Dangereuses par Route
BIC	Brandweer Informatie Centrum
BDD	Biological Dispersal Device
BTWC	Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction
CANVEK	Commissie van Advies voor de Niet-Verspreiding van Kernwapens
C ³	Command, Control and Communications
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosive
CC	Crisiscentrum
CC Prov	Crisiscentrum van de provincie
CDC	Center for Disease Control
CGCCR	Crisiscentrum van de regering
CIWIN	Critical Infrastructure Warning Information Network
C-Ops	Centrum Operaties (Evere)
CODUN	Working Group on Global Arms Control and Disarmament
CONOP	Working Group on Non-Proliferation
CP-Ops	Commandopost Operaties
CTBT	Comprehensive Nuclear Test Ban Treaty
CWC	Convention on the Prohibition, of the Development, Production, Stockpiling and use of Chemical Weapons and on their destruction.
DHS	Department of Homeland Security
EADRCC	Euro-Atlantic Disaster Response Coordination Centre
EADRU	Euro-Atlantic Disaster Response Unit
ECDC	European Centre for Disease Control
EOD	Explosive Ordnance Disposal
EPCIP	European Program for Critical Infrastructure Protection
ERG	Emergency Response Guide
EU	Europese Unie
FANC	Federaal Agentschap voor Nucleaire Controle
FCCU	Federal Computer Crime Unit
FMTC	Fissile Material Cut-off Treaty
FOD	Federale Overheidsdienst
FRISK	Federal Risk Inventory, Survey and Knowledge building
GNEP	Global Nuclear Energy Partnership Program
HCoC	Hague Code of Conduct
HEU	Highly Enriched Uranium
IAEA	International Atomic Energy Agency
IED	Improvised Explosive Devices Disposal
IC	Incident Commander
ICBM	Intercontinental Ballistic Missile
IRBM	Intermediate Range Ballistic Missile
ITBD	Illicit Trafficking Data Base
KMI	Koninklijk Meteorologisch Instituut
LEU	Low Enriched Uranium
NBC	Nucleair, Biologisch en Chemisch

NICC	Nationaal Instituut voor Criminologie en Criminalistiek
NPT	Nuclear Proliferation Treaty
NRF	NATO Response Force
PSI	Proliferation Security Initiative
RDD	Radiological Dispersal Device
SCK	Studiecentrum voor Kernenergie
SIBCRA	Sampling & Identification of Biological, Chemical & Radiological Agents
SIPRI	Stockholm International Peace Research Institute
SLBM	Submarine Launched Ballistic Missile
SRBM	Short Range Ballistic Missile
MASCAL	Massive casualties
MRBM	Medium Range Ballistic Missile
NIOSH	National Institute for Occupational Safety and Health
NRF	NATO Response Force
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OPCW	Organisation for the Prohibition of Chemical Weapons
TNO	Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
UAV	Unmanned Aerial Vehicle
VITO	Vlaams Instituut voor Technologisch Onderzoek
WHO	World Health Organization
WMD	Weapons of Mass Destruction



Inleiding

De machtsverhoudingen zijn grondig gewijzigd na de aanslagen van 11 september 2001. De daarop volgende anthrax-brieven, de bomaanslagen in Madrid (11 Maart 2004) en Londen (7 Juli 2005) hebben, door hun omvang en organisatie, een ernstige psychologische impact gehad op de Westerse landen. Het gevoel van onveiligheid, dat dagelijks kost is in conflictgebieden, bleek plots ook zeer reëel voor ons! Bovendien konden de aanslagen in eerste instantie niet onmiddellijk toegewezen worden aan een of andere terroristische groepering, zoals men dat gewoon was in de periode tussen 1970 en 1990: in die periode waren auteurs van aanslagen maar al te gretig om hun exploten op te eisen. Vandaag kan de verantwoordelijkheid voor een aanslag niet onmiddellijk vastgesteld worden. Meer en meer ziet men zelfs dat aanslagen (conventioneel of niet) beraamd worden door mensen die in dat land opgroeien, waar ze uiteindelijk hun dodelijke plannen ten uitvoer brengen. De vijand is niet meer (enkel) een buurland of een militaire kernmacht die raketten op ons gericht heeft, maar kan zich al op eigen grondgebied bevinden. In de Politieke Oriëntatienota van de Minister van Defensie Pieter DE CREM wordt de bezorgdheid uitgedrukt omtrent de groeiende tendens in zake proliferatie en internationaal terrorisme. De vervaging van interne en externe veiligheid impliceren aldus een mogelijke dreiging op nationaal grondgebied. Men heeft ondertussen ingezien dat de catastrofale gevolgen van conventionele of niet-conventionele aanvallen op geprojecteerde troepen of op eigen grondgebied, een aangepaste verdediging en respons vereisen. De bestaande doctrines doen het niet meer in deze nieuwe context. Daarom schrijven de NAVO en haar leden (nog in 2008) verder aan doctrines ter verdediging van het eigen grondgebied. Hiervoor baseert men zich op de draaiboeken die klaargestoomd werden door de landen die het slachtoffer werden van de aanslagen, of die inzagen dat er snel een “Nationaal” plan moest komen (voorbeelden zijn de doctrines van Canada en het Verenigd Koninkrijk). De praktische aanpak ligt aan de basis, dus ook oefeningen worden georganiseerd, maar militaire inzet als steun aan de Natie blijft een heikel punt op de agenda. Deze “bottom-up” aanpak is gestoeld op de ervaringsdeskundigen van het terrein. Hieruit werden lessen getrokken voor de toekomst: de doctrines moeten hiervan een weerspiegeling zijn.

Over het hele verloop van deze studie werd zo veel mogelijk beroep gedaan op actuele bronnen: dit geeft de meest recente standpunten weer en de laatste updates met betrekking massavernietigingswapens en de wetgeving, procedures en verdragen hieromtrent. Het valt niet uit te sluiten dat “last minute” ontwikkelingen tijdens de afwerking van dit werk, als aanvulling zullen moeten geraadpleegd worden. Ook interviews van nauw betrokken personen, in uiteenlopende vakgebieden, worden hier weergegeven.

Deel 1 is in hoofdzaak beschrijvend: definities, standpunten met betrekking tot proliferatie, capaciteiten van landen en invloedsfactoren, transfers van kennis technologie en materieel worden kort besproken. Naast het beschrijvend gedeelte, worden reeds enkele besluiten getrokken omtrent het non-proliferatieregime dat verder nog aan bod zal komen. Een laatste aspect dat in dit deel besproken wordt is

het wapenbeleid in België: een korte analyse van de wetgeving omtrent materiaal, gevoelig voor proliferatie, wordt weergegeven.

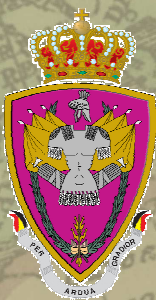
Het tweede deel van de studie is voornamelijk gericht op het aspect “indirecte bedreiging”. In deze studie krijgt dit begrip voornamelijk invulling door de dreiging op eigen infrastructuur of troepen. Terroristische activiteiten kunnen aan de basis liggen, maar het is niet de bedoeling uitgebreide gedeelten van dit werk aan terrorisme te wijden. Een studie van het KHID-CSDS is specifiek op dit onderwerp gericht: aanvullende informatie kan in dit verband teruggevonden worden in het werk van Mr. Stefan DECONINCK. Deze studie biedt meer aandacht voor middelen die beschikbaar zijn in de strijd tegen proliferatie, zowel op internationaal als op nationaal vlak. Een geactualiseerde stand van zaken zal nagaan hoe de nationale inspanningen in die richting worden gecoördineerd. De nadruk wordt hier gelegd op de samenvloeiing van militaire en burgermiddelen en hun inzet op het nationale grondgebied: er zal een onderscheid gemaakt worden tussen een tactische (praktische) benadering enerzijds, en een strategische (beleidsmatige) benadering anderzijds. Naast bestaande structuren en doctrines, krijgt ook de praktische invulling ervan aandacht om uiteindelijk mogelijke hinderpalen bloot te leggen. Voorstellen tot oplossingen in die richting worden geformuleerd.

Het derde en laatste deel geeft voornamelijk aanbevelingen weer. De methodologie die hier werd gevolgd, is gestoeld op de werkwijze in deel twee van dit werk: ook hier wordt besproken wat mogelijke verbeteringen of aanpassingen op praktisch gebied zouden kunnen inhouden (tactische normen en voorstellen). Vervolgens worden de beleidsmatige voorstellen benaderd (strategische normen en voorstellen). Dit gedeelte heeft niet als bedoeling een exhaustief overzicht te geven met betrekking tot de proliferatieproblematiek: voorstellen worden geformuleerd om de eerder opgedoken pijnpunten aan te pakken om tot een redelijke oplossing te komen.

In het besluit zullen de meest dringende problemen nog even aangehaald worden. Onontgonnen gebieden en domeinen die aanleiding kunnen geven tot wetenschappelijk onderzoek in verschillende vakgebieden worden eveneens weergegeven.

De standpunten ingenomen in dit werk reflecteren niet noodzakelijk deze van Defensie.

Deel 1



Definities, proliferatie, capaciteiten en transfers



1.1. Definities

1.1.1. WMD: MASSAVERNIETIGINGSWAPENS

De term « massavernietigingswapen » - in het Engels Weapons of Mass Destruction (WMD)- duidt tegelijkertijd op het destructief en dodelijk vermogen van een wapen: simultaan zo veel mogelijk schade aanrichten en zo veel mogelijk slachtoffers veroorzaken. Tijdens de periode van de koude oorlog, werden hier voornamelijk nucleaire, biologische en chemische (NBC) wapens mee bedoeld. De massale hoeveelheden NBC-wapens die door beide allianties, de NAVO en het Warschau Pact, werden opgestapeld, en de destructieve capaciteit van deze wapens deden de term WMD alle eer aan. In de periode die vooraf ging aan de eerste verdragen ter beperking van proliferatie van kernwapens, werd de strategie immers bepaald door de afschrikking van een onmiddellijke en massale respons (“massive retaliation”) bij de inzet van deze tuigen. De wapenwedloop werd opgedreven tot de twee grote kampen een arsenaal hadden opgebouwd dat een wederzijdse totale vernietiging garandeerde (Mutual Assured Destruction-MAD). Sinds de ineenstorting van de Sovjet-Unie en de reductie van de bestaande wapenopslagcapaciteit, heeft de term massavernietigingswapen een enigszins nieuwe invulling gekregen: chemische wapens kunnen een zeer beperkt aantal slachtoffers maken zonder enige vorm van materiële schade (vb. een mortieraanval in open terrein met chemische granaten). Biologische wapens zijn moeilijk inzetbaar en kennen dezelfde beperkingen als de eerste chemische wapens van Wereldoorlog I: eigen troepen kunnen er zelf het slachtoffer van worden. Van materiële schade is in dit geval evenmin sprake. Het enige wapen dat sinds de eerste inzet nog niets aan zijn kracht heeft ingeboet is terecht het kernwapen.

Niet alle auteurs zijn het eens over de definitie van de term WMD: voor het eerst werd de term gebruikt in een toespraak voor de Verenigde Naties in 1946 waar werd gerefereerd naar « weapons adaptable to mass destruction »¹. Voor de militaire doctrine van de VS, maken radiologische en conventionele wapens zelfs integraal deel uit van de term WMD met name: « ...WMD can be high explosives, or nuclear, biological, chemical and radiological weapons, but exclude the means of transporting or propelling the weapon where such a means is a separable and divisible part of the weapon ».² Andere bronnen gaan zelfs zo ver in hun beschrijving dat de hoeveelheden agentia en springlading of dimensies soms mee in de definitie opgenomen worden³. Om de onenigheid nog te verergeren willen sommige auteurs ook het concept “paniek

¹ Weapons of Mass Destruction, *New York Times Magazine*, 19 April 1998, p.22.

² Department of Defense, Department of Defense Dictionary of Military and associated Terms, 04 March 2008, p.584.

³ US code collection, Crimes and criminal procedure, Title 18, Part I, Chapter 113B, §2332a.

en terreur” in de definitie voegen⁴. In dat geval kunnen zelfs de vliegtuigen die zich op 11 september 2001 in de WTC-torens boorden, beschouwd worden als WMD.

De meest eenvoudige benadering blijft diegene die ook teruggevonden wordt in de definitie van SCHULTE nl. “...WMD consist of nuclear, biological and chemical weapons...These weapons have very different effects but all are capable of causing significant damage or disrupting military operations.”⁵ Het is belangrijk om hier de bemerking te maken dat de nucleaire, chemische of biologische lading op zich géén WMD vormen: uranium, onder de vorm van isotoop⁶ 235 dat in wapens wordt gebruikt, vormt op zich géén kernwapen. Om wel aan die voorwaarde te voldoen, moet men beschikken over een kritische massa⁷ en een springlading in de juiste geometrie. Een WMD bevat dus een nucleair, biologisch of chemisch agens maar wordt pas een wapen wanneer het verwerkt is in een conventionele springlading en/of verspreidingsmechanisme. Het valt buiten het bestek van dit werk om alle agentia te vermelden die in een WMD verwerkt kunnen worden. Men kan een algemene lijst vinden van mogelijke NBC-agentia per categorie in LANGFORD (op. cit.). Voor chemische agentia kan men een meer exhaustieve lijst vinden van gecontroleerde substanties en hun precursoren in bijlage aan de “Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction” (CWC)⁸. Voor de biologische agentia kan men terecht op de site van het Center for Disease Control (CDC)⁹. Kernwapens gebaseerd op kernfissie-reacties worden gebouwd met aangerijkt uranium (HEU) of Plutonium. Volledigheidshalve dient men nog te vermelden dat sommige auteurs niet meer refereren naar WMD om reeds vermelde ambiguïteiten te vermijden. Zo spreken CIRINCIONE et al. Enkel nog over “nuclear, biological and chemical weapons”¹⁰.

Sommige NAVO-landen gebruiken nog steeds de term NBC bekend vanuit de traditie van de koude oorlog. Sinds de terroristische aanslagen met Sarin-gas door de Aun Shinrikyo-sekte in de metro van Tokyo, werden alle NBC-scenario's (nl.gebruik in het kader van een gewapend conflict) aangepast. Vanaf toen werd ook rekening gehouden met het gebruik van WMD in stedelijke omgeving. Meer en meer werd rekening gehouden met het “dirty bomb” scenario. Een zogenaamde “vuile bom” omvat een agens uit de NBC categorie, geassocieerd met een conventionele springlading of ander verspreidingsmechanisme. Vandaar dat de term NBC meer en meer vervangen werd door het acroniem CBRNE¹¹. De letter R in het acroniem verwijst naar radiologisch materiaal dat verwerkt kan worden in een vuile bom om een radiologische besmetting te veroorzaken. Dit is een indirecte verwijzing naar terroristische activiteiten, aangezien splijtstof voor terroristen moeilijker te verkrijgen is dan radiologisch materiaal. Alle risico's van WMD en geïmproviseerde tuigen kunnen zo weergegeven worden door één enkel acroniem.

⁴ LANGFORD, E., Introduction to weapons of mass destruction: radiological, chemical and biological. Wiley-Interscience, 2004, p.1.

⁵ SCHULTE, G., « Responding to proliferation: NATO's role », in *NATO Review*, Vol.43, N°4, July 1995, p 15.

⁶ Isotopen zijn stoffen met dezelfde chemische eigenschappen maar met verschillende atoommassa.

⁷ Voldoende ²³⁵U om een kettingreactie te onderhouden. In de natuur voorkomend Uraniumerts bevat slechts 0.7% ²³⁵U.

⁸ CWC, Bijlage B, pp.51-53: <http://disarmament.un.org/wmd/cwc/cwctext.htm>

⁹ <http://emergency.cdc.gov/agent/agentlist-category.asp>

¹⁰ CIRINCIONE, J., WOLFSTHAL, J., RAJKUMAR, M., Deadly Arsenals: nuclear, biological and chemical threats. Carnegie Endowment for International Peace, 2005, p.1. en p.6.

¹¹ MARCHAND, G., « CBRN Going CBRNE: A New Perspective Behind The Words? », in *IFAS*, Juin 2007, p.3.

Samengevat kan men stellen dat de term WMD nucleaire, biologische of chemische wapens omvat, al dan niet aangehecht aan hun respectievelijke vectoren (zie verder). Het gebruik van WMD zou kunnen leiden tot CBRNE scenario's die zowel tijdens conflicten ten velde, als ook in vreedstijd en in stedelijke omgeving kunnen voorkomen.

1.1.2. VECTOREN VOOR MASSAVERNIETIGINGSWAPENS

Om een massavernietigingswapen te kunnen inzetten moet het tot op het doel kunnen gebracht en afgeworpen worden. Hiervoor zijn de gepaste vectoren i.e. dragers of wapenplatformen vereist. Vectoren zijn dus transportmiddelen die wapens over een zekere afstand transporteren. Hiervoor komen in aanmerking artillerie, raketten, mortieren, vliegtuigen, helikopters en onbemande vliegtuigen (UAV). Ballistische raketten kunnen eveneens gebruikt worden. Indien we dieper ingaan op de definitie die door het Ministerie van Defensie van de VS wordt gehanteerd (zie hoger), dan kan men vaststellen dat raketten zelf een WMD vormen maar vliegtuigen niet: vliegtuigen voldoen immers aan het gedeelte "...but exclude the means of transporting or propelling where such a means is a separable and divisible part of the weapon". Bovendien kunnen WMD afgeleverd worden door snelle vaartuigen, vrachtwagens, of gewone personenwagens al dan niet uitgerust met sproeisystemen. Niet elk wapen kan ingezet worden met om het even welke vector. WMD die door verschillende vectoren afgeleverd kunnen worden, zijn meestal ingedeeld volgens de classificatie van het agens dat gebruikt wordt¹².

Nucleaire wapens zijn initieel ontworpen om door artillerie afgevuurd te kunnen worden. Dit gebruik bleek echter ondoeltreffend wegens het beperkte bereik en het risico om zelf in besmet gebied terecht te komen, al naar gelang de verspreiding van de radioactieve wolk. Tijdens de koude oorlog werden strategische (i.e. lange afstand) bommenwerpers gebruikt omwille van de afmetingen van de ontworpen tuigen. De inertie van deze vliegtuigen en de detecteerbaarheid door vijandige troepen was echter een kritische factor. Meer en meer werd beroep gedaan op ballistische raketten om nucleaire wapens af te vuren. Hier maakt men meestal het onderscheid uitgaande van het bereik van de raket¹³:

TYPE	BEREIK
SRBM(Short Range Ballistic Missile)	< 1000 Km
MRBM(Medium Range Ballistic Missile)	1000-3000Km
IRBM(Intermediate Range Ballistic Missile)	3000-5500Km
ICBM(Inter Continental Ballistic Missile)	>5000Km

Een ballistische raket wordt initieel aangedreven door vloeibare of vaste propergolen, maar na verbranding ervan, volgt het projectiel een ballistische baan naar het doel. Aangezien dit meestal buiten de atmosfeer gebeurt, moeten de projectielen en de agentia die erin verwerkt zijn, bestand zijn tegen de hoge temperaturen bij het binnentreden van de atmosfeer. Ballistische raketten hebben een snelheid die hoger is dan die van het geluid, met als gevolg dat er weinig preadvies is na het afvuren van zo'n tuig¹⁴. Initieel kon slechts één kernkop gebruikt worden per raket, maar de evolutie van de technologie liet al snel toe om meerdere kernkoppen

¹² LANGFORD , E., op.cit. pp 92 e.v.

¹³ Office of the Secretary of Defense, Proliferation: Threat and Response, January 2001, p.115.

¹⁴ CIRINCIONE, J., WOLFSTHAL, J., RAJKUMAR, M., Deadly Arsenal: nuclear, biological and chemical threats. Carnegie Endowment for International Peace, 2005, p.89.

per raket af te vuren en dit zowel vanaf de grond als vanaf onderzeeërs (SLBM). De Verenigde Staten hebben in laatste instantie kruisraketten ontworpen. De propulsie van deze tuigen gebeurt gedurende de volledige tijdspanne van de vlucht. Door de uitrusting van een GPS-systeem, kunnen deze autonoom naar hun doel vliegen en zijn ze accuraat tot op enkele meters (+/- 6m) wat veel beter is dan de klassieke ballistische raketten (type SCUD) die het doel slechts tot op +/- 1000 meter kunnen bereiken¹⁵. Kruisraketten kunnen afgevuurd worden door vliegtuigen, schepen en onderzeeërs. Ten slotte kunnen ook UAV's ingezet worden voor het afleveren van kernwapens. Net als de kruisraketten zijn ze zeer precies, maar de draagkracht kan opgedreven worden tot +/- 900kg. Deze vectoren zijn echter zeer onderhevig aan de weersomstandigheden die de vluchthoogte zal bepalen, waardoor ze in het bereik van vijandelijke luchtafweer kunnen komen.

Vectoren voor biologische wapens daarentegen, zijn beperkt omdat de agentia zelf moeilijk te verspreiden zijn, en de gevolgen ervan niet altijd exact in te schatten: de virulentie van het agens kan beïnvloed worden door de verspreiding en de weersomstandigheden. Bovendien kan men door de inertie van de effecten (incubatie), niet snel genoeg weten wat de gevolgen zijn voor eigen troepen. Indien het agens efficiënt moet ingezet worden, moet het overleven na verspreiding d.w.z. dat mechanismen die grote hoeveelheden springstof bevatten uitgesloten zijn. De schokgolf en temperatuurschommelingen die door de explosie worden gegenereerd zouden het agens onherroepelijk vernietigen. Mogelijk kunnen deze wapens ook ingezet worden tegen de voedselvoorraad van de vijand (dierlijk of plantaardig). Dit zou het risico voor eigen troepen drastisch beperken. Biotechnologie maakt het zelfs mogelijk om bio-agentia selectief te laten werken op soorten met een welbepaalde genetische code (bijvoorbeeld enkel veestapel of graan). Ten velde moet steeds rekening gehouden worden met de natuurlijke vectoren i.e. de dragers van het pathogeen organisme: er bestaan insecten en knaagdieren die natuurlijke drager zijn van ziektekiemen die men als biologisch agens beschouwt, maar die er zelf niet ziek van worden. Inzet van zulke vectoren maakt detectie uiterst moeilijk, maar zal tevens ook de uitwerking bijzonder onvoorspelbaar maken. Men kan dus concluderen dat mechanismen voor verspreiding van bio-agentia van volgende aard zullen zijn:

- sproeisystemen (type verspreidingssystemen van pesticiden bvb met UAV)
- artilleriegranaten (met beperkte springstoflading en sterke bio-sporen zoals anthrax als lading)
- raketten (niet van het type ICBM omwille van de temperatuurschommelingen)
- bommen
- contaminatie van drinkwaterbronnen en/of de voedselketen (met bijvoorbeeld botuline)
- dispersiesystemen (type spuitbussen onder druk): in dit geval noemt men het systeem ook een "Biological Dispersal Device" (BDD).

Voor meer informatie betreffende dosis-respons relaties kan het naslagwerk van LANGFORD¹⁶ antwoorden bieden.

Om het spectrum te vervolledigen, moeten de vectoren van de chemische wapens nog behandeld worden. Deze zijn vergelijkbaar met de vectoren voor bio-agentia zijnde:

- sproeisystemen (type verspreidingssystemen van pesticiden vb. met UAV)
- artilleriegranaten
- raketten (niet van het type ICBM omwille van de temperatuurschommelingen)
- bommen

¹⁵ CIRINCIONE, J., et.al., op.cit., p.90.

¹⁶ LANGFORD, E., op.cit., p.198.

- dispersiesystemen (type spuitbussen onder druk).

Chemische agentia zijn minder gevoelig voor mechanische en /of meteorologische omstandigheden voor wat de vernietiging van het agens betreft. De atmosferische condities zullen echter wel hun rol spelen in de persistentie van het agens d.w.z. hoe lang het agens werkzaam blijft na verspreiding. Dit gaat van zeer persistent (enkele dagen of langer-type VX) tot niet persistent (enkele minuten tot uren - type fosgeen). Ook hier kan men voor dosis-respons relaties terecht bij LANGFORD¹⁷. Men dient nog op te merken dat de meeste van de chemische agentia corrosief zijn. Dit heeft als gevolg dat opslag van chemische munitie erg moeilijk te controleren valt. Niet zelden stelt men vast dat munitie na verloop van jaren begint te lekken door de corrosie van het agens op het omhulsel van de munitie. Dit maakt het vernietigen van deze munitie in het kader van OPCW-akkoorden bijzonder gevaarlijk voor het accidenteel vrijstellen in de omgeving van de opslagplaats.

Vectoren die WMD kunnen afleveren, kunnen eveneens gebruikt worden voor conventionele munitie (springstoffen, bommen, raketten, submunitie of projectielen). Het omgekeerde is niet altijd het geval. Kernwapens bijvoorbeeld kunnen pas gewapend worden indien een voorgeprogrammeerde code wordt ingegeven-mogelijk tijdens de vlucht naar het doel. Bovendien bevatten deze wapens inertieële platformen die de versnelling en vertraging van het projectiel registreren en dan pas gewapend kunnen worden¹⁸.

¹⁷ LANGFORD, op.cit., p.284. Een exhaustieve lijst van agentia en hun uitwerking, alsook toxische dosissen en lethale dosissen is te vinden op : <http://toxnet.nlm.nih.gov>

¹⁸ BUNN, M., WIER, A., Terrorist Nuclear Weapon Construction: How Difficult?, The annals of the American Academy of Political and Social Science, N°607, September 2006, p.133.

1.2. Proliferatie van WMD en vectoren

Het discours over proliferatie is er meestal één over nucleaire capaciteit: zoals verder aangetoond zal worden, is dit deels te wijten aan het feit dat de indicatoren i.e. signalen van proliferatie in de nucleaire discipline duidelijk omschreven zijn. De traceerbaarheid is veel beter omwille van de ingewikkelde technologie en infrastructuur vereist voor het samenstellen van een operationeel kernwapen¹⁹. Voor wat de chemische²⁰ en biologische²¹ wapens betreft, zijn deze indicatoren veel minder uitgesproken: in de actuele context van de (bio-)technologie en de farmacologie, kunnen op het eerste zich vreedzaam ogende installaties, dienst doen als wapen producerende faciliteiten. Materiaal voor “tweeërlei gebruik” (i.e. industrieel materiaal, bijvoorbeeld precursoren en infrastructuur die kunnen gebruikt worden voor militaire programma’s nl. productie van actieve agentia en operationele wapens) maken het onmogelijk om zonder adequate controlemiddelen, de proliferatie van chemische wapens in te schatten. Dit is nog meer het geval wanneer staten er een verborgen agenda op na houden om inspecties te ontlopen. Men kan enkel speculeren dat een proliferator op nucleair gebied, ook biologische en chemische wapens zal proberen aan te maken. Men kan zelfs een stap verder gaan in die redenering en bedenken dat indien een staat jaren lang inzet vertoont om te beschikken over een kernwapen, dat hem met alle middelen wordt ontzegd, met zekerheid zal grijpen naar de goedkopere en meer voor de hand liggende chemische en biologische wapens.

In het nabije verleden hebben reeds enkele landen moedwillig de verplichtingen van de non-proliferatieverdragen naast zich neergelegd (o.m. Irak, Iran en Noord-Korea²²). Dit kan ernstige gevolgen hebben voor een nieuwe golf van proliferatie. Bij deze problematiek voegen zich nog de politieke verschuivingen die nog steeds voortvloeien uit het verval van de Sovjet-Unie: aan de grenzen van de NAVO-alliantie, blijven staten actief in hun zoektocht naar (illegale) productie van WMD of hun vectoren²³. Voormalige Sovjetstaten waren rijk aan WMD-materiaal en kunnen nu een vaak aangesproken partner worden omwille van dit overgebleven materiaal²⁴. Individuen kunnen bovendien profiteren van de globalisatie: een groeiende markteconomie zorgt voor intensieve handel van goederen voor tweeërlei gebruik (zowel voor industrieel gebruik als voor productie van WMD). Dit maakt het niet eenvoudiger om transfer van materiaal en technologie te detecteren, vooral als de eindgebruiker één individu of een kleine groep blijkt te zijn, en géén staat. De non-proliferatieverdragen (zie verder) werden opgesteld om staten ertoe te verplichten open kaart te spelen en aan te tonen dat ze vrijwillig WMD technologie naast zich neerleggen. Weerbarstige spelers in de Wereldpolitiek kunnen zo de schijn wekken

¹⁹ EPSTEIN, G., Technologies underlying weapons of mass destruction, International Security and Commerce Program, December 1993, pp. 119 e.v.

²⁰ EPSTEIN, G., op.cit., pp.36 e.v.

²¹ DANDO, M., Biological Warfare in the 21st Century, Brassey’s Ltd, 1994, p.131.

²² De Democratische Volksrepubliek Korea (Noord-Korea) verliet het NPT in januari 2003 na de formele weigering om inspecteurs van het IAEA toe te laten tot de site van de Yongbyon reactor.

²³ SCHULTE, G., « Responding to proliferation: NATO’s role », in *NATO Review*, Vol.43, N°4, July 1995.

²⁴ CIRINCIONE, J., WOLFSTHAL, J., RAJKUMAR, M., Deadly Arsenals: nuclear, biological and chemical threats. Carnegie Endowment for International Peace, 2005, p.59.

om eerlijk spel te spelen om tijd te winnen en alsnog de technologie te bekomen (eventueel onder de mom van vreedzame technologie, vb. alternatieve energiebronnen). Ook individuen kunnen, omwille van globalisering, binnen een staat of een Alliantie veel gemakkelijker in het bezit komen van de technologie²⁵.

Voormalig VN Secretaris-Generaal Koffi ANNAN had reeds de mogelijkheid geuit voor een hernieuwde wapenwedloop of zoals hij het zelf formuleerde: “a cascade of proliferation”²⁶. Redenen hiervoor waren volgens hem:

- De opdrijving van de kernwapenprogramma’s van Noord-Korea en Iran. Hierdoor kon het onveiligheidsgevoel in Noord-Oost Azië en het Midden-Oosten toenemen, hetgeen anderen naar dezelfde wapens zou kunnen doen grijpen.
- De militaire “build-up” van China en de voortdurende en herhaaldelijke twisten met Taiwan doet de spanning stijgen in Oost-Azië.
- De onmogelijkheid van de VS om tot een snelle en duurzame oplossing te komen in Irak en Afghanistan, zou vragen kunnen doen rijzen over de betrouwbaarheid van het Amerikaans nucleaire schild.
- Globalisatie en netwerken die via de zwarte markt gevoelige technologie aan de man kunnen brengen van Staten die reeds onder toezicht van het IAEA werden geplaatst.
- Technische aanpassingen zorgen ervoor dat illegale materialen moeilijker te detecteren worden m.n. de overstap van plutoniumgebruik in de wapentechnologie naar uranium (via aanrijking door centrifuges).
- De mislukking van de VN om tot nog toe de overtreders van de verdragen op een doeltreffende wijze te sanctioneren.
- Mogelijke coöperatieverdragen van de VS met India (zelf géén ondertekenaar van het non-proliferatieverdrag): dit schept precedentes voor andere staten die eveneens het wapen zouden willen aanschaffen.

Het energetisch probleem vormt eveneens een risico voor proliferatie: de reserves van fossiele brandstoffen zijn beperkt en het gebruik ervan vormt telkens weer een discussiepunt met betrekking tot de opwarming van de aarde terwijl de technologie voor alternatieve energie nauwelijks in de kinderschoenen staan. Een voortzetting van het gebruik van kernenergie is dus een evident “overgangsscenario” voor de komende 10 tot 20 jaar. Dit was één van de agendapunten van de G8-top te St.Petersburg in juli 2006²⁷. Aanpassingen aan de bestaande capaciteit van kerncentrales wordt nauwlettend in de gaten gehouden door het internationaal atoomagentschap (IAEA). Aanbouw van nieuwe centrales kan echter onderhevig zijn aan een zekere inertie omwille van alle vereiste vergunningen, testprogramma’s en controles die het agentschap oplegt: voor de aanleg van een nieuwe kerncentrale moet men in het beste geval, vanaf aanvraag tot operationele inzet, rekening houden met een duur van 9 jaar. Met het oog op een operationele capaciteit tegen het jaar 2015, hebben een aantal landen aanvragen in die zin ingediend in 2006 (zie ook voetnoot 27). Rekening houdend met de operationele werking van dergelijke reactoren van minstens 25 jaar, moet men rekening houden met een programma voor kernenergie dat zeker aanhoudt tot horizon 2040. Men kan echter niet ontgaan aan het feit dat ook

²⁵ RUSSELL, J., WIRTZ, J, Globalization and WMD proliferation: terrorism, transnational networks and international security, Routledge, 2008, p.158.

²⁶ LAVOY, P., Nuclear weapons proliferation in the next decade, Routledge, 2007, p.60.

²⁷ MITROVA, T., G8 St Petersburg, Paper on Global energy security, p.28: “Nuclear power is no more seen as cost-prohibitive, due to which many countries have designed nuclear expansion plans for 2012-2020, and such countries as China, Japan, Russia, and South Korea have been commissioning new nuclear generation facilities since 2004. Nuclear power accounts for around 16% in the current electricity production, and at today’s critical juncture, many national governments either build new or upgrade existing nuclear power plants.”

de globalisatie van dit energetische probleem (uitputting van fossiele brandstoffen vs. beschikbaarheid van alternatieve brandstoffen) een inherent risico voor proliferatie inhoudt²⁸ omwille van volgende factoren:

- Nucleaire brandstofvoorraden: de distributie van uraniummijnen over de hele wereld, zullen steeds speciale aandacht krijgen van kandidaat-proliferatoren, liefst in een scenario van vreedzame zoektocht naar alternatieve energiebronnen.
- Verwerking van nucleaire brandstof: infrastructuur en uitrusting voor het verwerken van uranium-erts en de aanrijking van metallisch uranium kunnen voorkomen in programma's voor energievoorziening maar evengoed in militaire programma's.
- Bestaande kerncentrales of wetenschappelijke programma's kunnen gemakkelijk geheroriënteerd worden naar militaire doeleinden.
- Transport van splijtstof voor energetische doeleinden: het aantal transporten van en naar kerncentrales is ontelbaar en kan dus omgeleid worden om te ontsnappen aan internationale controle. Sommige MOx (metaal-oxides van splijtstoffen in gebruik bij kerncentrales) kunnen zelfs rechtstreeks gebruikt worden in rudimentaire wapens.

Al deze punten verdienen extra aandacht en doorgedreven controles indien men wil vermijden dat bronnen ontsnappen of afgeleid worden voor de productie van wapens.

Initiatieven om een oplossing te vinden voor het argument dat de meeste proliferatoren aanhalen m.n. het recht op de vreedzame ontwikkeling van kernenergie, werden reeds overwogen: levering van kernreactorbrandstof door landen die reeds aanrijkingfaciliteiten bezitten zou hiervoor een oplossing kunnen bieden. Het laatste initiatief in rij was dat van de VS m.n. "Global Nuclear Energy Partnership Program" (GNEP)²⁹. Hoe de problematiek van afvalbeheer in dit voorstel zou behandeld worden blijft onduidelijk in de beschrijving, en dit is net een punt dat gebruikers zou afschrikken: achterblijven met een berg radioactief afval, of moeten betalen voor het behandelen ervan terwijl men net een goedkope energiebron wil uitbaten is geen optie. In dat opzicht verkiezen velen om het proces van het begin tot het einde in eigen handen te houden. Belichten we enkele specifieke regio's met hun eigen problematiek in het kader van proliferatie.

In Zuid-Amerika zijn Argentinië en Brazilië leveranciers van kernenergie ook naar export toe (vb. export van een kernreactor naar Algerije in 1992)³⁰. In het kader van een eventuele export naar Venezuela, zou het gebrek aan technische expertise in dit land een eventueel militair programma vertragen en vroege detectie bevoorcellen.

In Zuid-Oost Azië heeft Noord-Korea reeds meermaals gespannen verhoudingen gehad met het IAEA. Hiermee toont dit land dat, ondanks (misschien wel omwille van) een tanende economie, de wil kan blijven bestaan om te streven naar nucleaire capaciteit. In 2004 schatte men de hoeveelheid kernkoppen van Noord-Korea op 8 stuks, met een bijkomende capaciteit van één kernwapen per jaar dankzij de plutoniumproductie van de Yongbyon-reactor³¹. Hoewel in september 2007 een duidelijke stap bleek gezet in de richting van de ontmanteling van het kernwapenarsenaal van Noord-Korea - in het kader van de "Six-party talks"(Noord-

²⁸ LAVOY, P., Nuclear weapons proliferation in the next decade, Routledge, 2007, p.204.

²⁹ PERKOVICH, G., Universal Compliance: a strategy for nuclear security. 2007 Report Card. Carnegie Endowment for International Peace, June 2007, p.9.

³⁰ LAVOY, P., op.cit., p.191.

³¹ KAMPANI, G., « WMD diffusion in Asia: heading towards a disaster », in *Strategic Asia*, 2004-2005, September 2004, p.393.

en Zuid-Korea, China, Rusland, VS en Japan) - weerhield Noord-Korea zich ervan om bewuste reactor te sluiten en de volledige inhoud van het kernwapenprogramma kenbaar te maken. Hoewel Noord-Korea wel bereid scheen om over te gaan tot ontmanteling voor zover de VS dit land van de lijst zou halen die terrorisme steunen³², voerde het op 25 mei 2009 een nieuwe ondergrondse kernproef uit. Myanmar heeft niet de technologische mogelijkheden om tot die capaciteit te komen, maar onderhoudt wel warme relaties met Noord-Korea: dat zou het voor Myanmar mogelijk maken om materiaal en/of wapens in te voeren. Indonesië is daarentegen altijd voorstander geweest voor vreedzame toepassingen van kernenergie: tenzij het in een regionaal of globaal conflict gedreven wordt, is dit land géén kandidaat voor proliferatie³³.

Volgens MOLTZ³⁴, zijn er zes mogelijke scenario's die proliferatie vanuit Noord-Oost Azië in de hand zouden kunnen werken:

- Kernproeven uitgevoerd door Noord-Korea: Zuid-Korea, Japan, en Taiwan zouden de dreiging buitensporig kunnen ervaren en nieuwe stappen zetten op de weg naar proliferatie.
- Falen van het non proliferatieverdrag (zie verder) zou dezelfde bedreiging doen ervaren en zelfs het verdrag voor het stoppen van testen van kernwapens doen negeren door staten als Rusland en China.
- Uitbreiding van het kernwapenarsenaal van China: dit zou zowel Taiwan als Japan opnieuw doen reageren in dezelfde richting. Indien Japan zou beslissen om een eigen kernwapenarsenaal te ontwikkelen, zonder het beschermende schild van de VS, zou dat het einde kunnen betekenen van hun alliantie. In se zou dit de ergste bedreiging vormen voor de veiligheid van Japan³⁵. Bij uitbreiding van capaciteit van China kan Rusland niet achterblijven. Als bedreigde buur zou India eveneens haar arsenaal uitbreiden en als gevolg daarvan ook Pakistan. Dit scenario zou een nieuwe wapenwedloop uitlokken in de hele regio.
- Hereniging van Korea: nationalistische jongeren uit de regio zien hereniging van Noord en Zuid wel zitten, wat zou uitmonden in een economisch groeiend deel (Z.Korea) dat zou samensmelten met een kernmogendheid (N.Korea). Dit zou onvermijdelijk leiden tot reactie van China met alle gevolgen van dien (zie hoger).
- Vertrek van de VS uit de regio: het wegvallen van het nucleaire schild van de VS voor Taiwan, Japan en Z.Korea, zou deze landen onherroepelijk dwingen tot verder gedreven ontwikkeling naar kernwapentechnologie.
- Herbewapening van Rusland: nationalistische opstoten en een tanende economie zouden Rusland kunnen doen afzien van alle ondertekende verdragen om opnieuw haar kernwapenarsenaal op te bouwen. Dit zou de dreiging van de koude oorlog opnieuw tot leven brengen en de hele regio destabiliseren.

Zowel Japan als India hebben zich in de regio steeds bedreigd gevoeld door de conventionele en niet-conventionele mogelijkheden van China. Om die reden zocht Japan naar een versterking van eigen veiligheid door bilaterale overeenkomsten af te sluiten met burens. Zo werd in maart 2007 een coöperatieakkoord omtrent veiligheid ondertekend tussen Japan en Australië: behalve politie samenwerking werden akkoorden voorzien om smokkel tegen te gaan van WMD materiaal en vectoren³⁶.

³² CARNEGIE ENDOWMENT FOR PEACE, «NKorea almost ready on nuclear statement », in *Proliferation news*, 3 June 2008.

³³ LAVOY, P., op.cit., p.178.

³⁴ LAVOY, P., op.cit., p.167.

³⁵ KAMPANI, G., op.cit., p.395.

³⁶ The National Institute for Defense Studies Japan, *East Asian Strategic Review 2008*, April 2008, p.216.

Met India hield Japan een aantal bilaterale meetings die in december 2006 afgesloten werden door de “Joint Statement Towards Japan-India Strategic and Global Partnership” vervuldigd door de verklaring na de bijeenkomst van augustus 2007 (“Joint Statement on the Roadmap for New Dimensions to the Strategic and Global Partnership between Japan and India”): gericht op het vrijwaren van de veiligheid van de zeeroutes in de Stille en Indische oceaan, werd ook de nadruk gelegd op de samenwerking op het gebied van internationale criminaliteit, terrorisme, piraterij en proliferatie van WMD³⁷.

Centraal-Azië vormt een aparte problematiek: Kazachstan, Kyrgyzstan, Tadjikistan, Turkmenistan en Uzbekistan bezitten allemaal een erfenis aan WMD-materiaal uit het voormalige Sovjettijdperk (spleijstof, ioniserende bronnen en biologische wapentechnologie). Geprangd tussen Rusland en Afghanistan, blijken deze landen ideale smokkelroutes te hebben voor het transport van opiaten die in Afghanistan werden geteeld³⁸. De voor de hand liggende conclusie is dat de geldstromen de andere richting uitgaan. Dit is echter een gevaarlijke evolutie die zou kunnen toelaten dat spleijstoffen op dezelfde zwarte markt terecht komt. Zowel de VS als Rusland hebben reeds geïnventariseerd materiaal uit de regio verwijderd om diefstal te voorkomen. Een grote hoeveelheid bronnen van ioniserende straling (vb. afkomstig uit de medische sector) werd echter nooit geïnventariseerd en zeker niet via de geëigende kanalen afgevoerd wegens te hoge kosten. Deze bronnen kunnen zeker gebruikt worden in een “vuile bom”. Deze regio was ook belangrijk in het Sovjettijdperk voor het onderzoek naar biologische wapens: voormalige onderzoekscentra bewaarden bacillen van pest, tularemie, virussen van hemorragische koorts, anthrax e.a. Deze vormen een mogelijk doelwit voor kandidaat proliferanten of terroristische groeperingen. Ook in het domein van de chemische wapens, had de regio onderzoeksprogramma’s lopen: precursoren voor tweërlei gebruik en corrosie-resistente reactoren werden uit de regio verwijderd, maar hun eindbestemming blijft onduidelijk³⁹. Methodes om mogelijk misbruik tegen te gaan zullen later uiteengezet worden.

In het Midden-Oosten⁴⁰, is voornamelijk Iran in staat om tot een kernwapen te komen. In Natanz zouden reeds in 2004, 1000 centrifuges operationeel zijn geweest voor het aanreiken van Uranium⁴¹. De activiteiten van Natanz werden echter allemaal onder de controle van het IAEA geplaatst⁴². Naast Israël, die de capaciteit reeds bezit (onder een vorm die door geen enkele bron duidelijk omschreven wordt), zouden ook Egypte en Saoedi-Arabië naar het wapen kunnen grijpen. De permanente druk in de regio kan verlicht worden door een multilaterale erkenning van het bestaansrecht van de Staat Israël door alle burens (Palestijnen inclusief). Het creëren van een Palestijnse onafhankelijkheid kan daarenboven rust brengen bij alle andere actoren in de regio. Syrië zou hier wel eens de spelbreker kunnen worden: op 6 september 2007 werd de Syrische militaire installatie van Deir ez-Zor door de Israëlische luchtmacht gebombardeerd. Hiermee werd volgens Israëlische en Amerikaanse bronnen een

³⁷ The National Institute for Defense Studies Japan, op.cit, p.222.

³⁸ KASSENOVA, T., « Central Asia: regional security and WMD proliferation threats », in *Disarmament Forum*, N°4, 2007, p.14.

³⁹ KASSENOVA, T., op.cit., p.18

⁴⁰ LAVOY, P., op.cit., p.155.

⁴¹ KAMPANI, G., op.cit., p.397.

⁴² De aanrijking van Uranium, opgestart in maart 2007, had op 2 februari 2008 een productie van 120 ton uranium (onder de vorm UF₆) opgeleverd. Het kernprogramma van Iran blijft het IAEA echter zorgen baren omwille van de lopende studies voor conversie van uraniumoxide naar uraniumfluoride, de testen van springstoffen en ballistische raketten. De combinatie van deze drie zou een militaire dimensie kunnen geven aan de nucleaire activiteiten van Iran. http://www.armscontrol.org/pdf/20080222_IAEAReport.pdf

nucleaire reactor blootgelegd. Het internationaal atoomagentschap liet bij monde van haar Directeur, Dr. M. EL BARADEI, weten dat er officieel geen nucleaire programma's in Syrië lopen⁴³.

In Europa vormt Turkije een bijzonder geval: enerzijds is het lid van de NAVO, maar anderzijds heeft het een strategisch partnerschap met Israël. Door de permanente explosieve situatie in de regio, is het bijzonder moeilijk voor Europa om te beslissen of Turkije al dan niet moet toetreden tot de EU: de politieke verschuiving naar minder seculier staatsmanschap, de talrijke militaire invallen in Irak (die de VS proberen te bedwingen) en de nauwe banden met Israël zouden de EU, met Turkije als lid, in conflicten kunnen meezuigen. Het steeds weer afhouden van het lidmaatschap van Turkije anderzijds, zou het land in een "nationalistisch reveil" op eigen wegen kunnen drijven die de bestaande NAVO-alliantie in een lastige situatie zou kunnen brengen⁴⁴.

Proliferatie van vectoren is gebonden aan proliferatie van wapens: zoals uitgelegd in punt 1.1, kan men geen wapens afleveren zonder de gepaste vectoren. Staten die vandaag nog een programma hebben voor de ontwikkeling van ballistische raketten met een bereik van meer dan 1000Km omvatten: China, Frankrijk, Rusland, de Verenigde Staten, India, Iran, Pakistan, Israël en Noord-Korea⁴⁵. De nauwkeurigheid en de nuttige lading van ballistische raketten zijn vandaag veruit overtroffen door kruisraketten. Naast verkenningsoopdrachten kunnen UAVs ingezet worden als vectoren voor conventionele wapens of WMD. Deze capaciteit blijft echter theoretisch omwille van het hoge ongevalpercentage dat vastgesteld werd tijdens Amerikaans gebruik in de conflicten van Afghanistan en Irak⁴⁶. Hoewel ballistische raketten zeker een psychologische impact hebben, zijn ze veel minder nauwkeurig om militaire doelen te bestoken. De vijf erkende kernmachten (VS, Rusland, China, Verenigd Koninkrijk, Frankrijk), hebben toegang tot het volledige spectrum van vectoren. Israël, Pakistan en India zijn de facto eveneens kernmachten geworden vóór de uitbreiding van het non-proliferatieverdrag in 1995, maar hebben dit verdrag niet geratificeerd; Noord-Korea en Iran zijn in overtreding met deze verdragen (zie verder). Voor aankoop van gevechtsvliegtuigen, moeten de "niet erkende kernmachten" beroep doen op invoer vanuit Rusland, Europa of de VS. De productie van onderzeeërs met kernwapencapaciteit moet gezocht worden in Duitsland, Frankrijk, Rusland en de VS⁴⁷. De technologie van de ballistische raketten (zeker die met de eenvoudigste technologie) is in handen van alle landen die het kernwapen verworven hebben.

Het valt dus in de lijn van de verwachtingen dat een kandidaat-proliferator, die een verdoken WMD programma wil opstarten, eerder beroep zal doen op de ruwere technologie van de ballistische raketten: minder nauwkeurig, maar met een niet te onderschatten psychologisch impact (cfr conventionele SCUD-aanvallen van Irak op

⁴³ KHAITOUS, T., « Is Syria a candidate for Nuclear Proliferation? », in *Issue Brief*, James Martin Center for Nonproliferation Studies, March 2008. De verschillende machtsverhoudingen in het Midden-Oosten, worden in een afzonderlijke studie nader bestudeerd door Lt Parrein P-J.

⁴⁴ Een uitgebreide omschrijving van de positie van Turkije t.o.v. de EU en de NAVO is te vinden in GASQUARD, S., « La politique de sécurité et de défense de la Turquie: éléments de convergence et de divergence avec la PESC/PESD », in *Sécurité et Stratégie*, N°96, Septembre 2007.

⁴⁵ CIRINCIONE, J., et.al., op.cit., p.89.

⁴⁶ 100 maal meer ongevallen dan bemane vluchten zo blijkt. CIRINCIONE, J., et.al, op.cit., p.91.

⁴⁷ KAMPANI, G., « WMD diffusion in Asia: heading towards a disaster », in *Strategic Asia, 2004-2005*, p.389.

Israël tijdens de eerste Golfoorlog). Ook Iran en Noord-Korea zullen om dezelfde reden eerder beroep doen op ballistische raketten: bewijs hiervoor werd reeds geleverd door de Noord-Koreaanse Taepo-Dong I test op 31 augustus 1998. Bedoeling van deze test was een satelliet te lanceren, hetgeen mislukte. Alle aandacht werd echter gericht op de raket die hiervoor uitgerust bleek met driestapspropulsie⁴⁸. Voor het eerst in de geschiedenis bleken de VS bereikbaar voor raketten van een land dat noch China, noch Rusland was. De psychologische impact was enorm. In de militaire plannen van de VS werd verondersteld dat, tegen horizon 2015, ook Iran deze capaciteit zou bezitten. Verdere proeven blijven die trend bevestigen: Iran testte de Kavoshgar 1 (IRBM) op 4 februari 2008⁴⁹ en Noord-Korea ging verder met het afvuren van korte afstands-raketten op 28 maart 2008⁵⁰. De lancering van de Pakistaanse Shaheen II (IRBM) op 19 en 21 april 2008⁵¹ zullen deels een reactie geweest zijn op de Indiase SLBM testen van 27 februari 2008⁵² en de Agni-I test (SRBM) van 18 maart. India plant op korte termijn de Agni-III (IRBM) te testen en aangezien China verdergaat met modernisering van haar meertrapsraketten voor een bereik over lange afstand, lijkt het er inderdaad op dat het vierde scenario van Moltz meer en meer de realiteit weerspiegelt: de gevreesde wapenwedloop in Noord-Oost Azië zal onafwendbaar zijn indien China bovendien verder blijft streven naar een capaciteit om (observatie-) satellieten neer te halen met geleide raketten. Een eerste test werd in alle discretie uitgevoerd in januari 2007; de VS bracht het experiment aan het licht⁵³. Hoewel in 2007 China en Japan pogingen ondernomen hebben om diplomatieke kanalen te openen, heeft dit incident zwaar gewogen op de lopende initiatieven. Deze test werd door Japan ervaren als een bedreiging en een precedent voor het gebruik van ruimtetuigen in het kader van oorlogsvoering. China hield het bij een laconieke verklaring dat betrokken proef door geen enkele Natie als een bedreiging moest worden ervaren. Toch voerde Japan eind december van dat jaar een eerste test uit voor interceptie van ballistische raketten. Dit verplichtte de VS om gelijkaardige proeven uit te voeren en de raketbescherming rondom Japan te versterken. Het gevolg is dat proliferatie ook nog een “Star Wars”-luik krijgt⁵⁴ indien geen verdere inspanningen geleverd worden om een gedragscode tot stand te brengen om ruimtelijke activiteiten aan banden te leggen.

Het laatste facet dat nog dient vermeld te worden is wat door BOND⁵⁵ “soft-proliferation” wordt genoemd nl. de verspreiding via het internet van technische gegevens en schema’s, data, kennis, expertise en financiële transacties. Dit is een bijzonder moeilijk in te dijken probleem in de actuele context van globalisatie. Initiatieven om deze problematiek in kaart te brengen staan, voor zover bekend, niet eens op de dagorde.

⁴⁸ CIRINCIONE, J., et.al., op.cit., p.83 e.v.

⁴⁹ FORDEN, G., « Smoke and mirrors: Analyzing the Iranian missile test », in *Jane’s Intelligence Review*, April 2008, p.48.

⁵⁰ JOHEE, C., « North Korea Flexes Missile Muscles » op <http://abcnews.go.com/International/Story?id=4541837&page=1>

⁵¹ <http://jdw.janes.com/public/jdw/asiapacific.shtml>

⁵² AUGUSTINE, A., «India missile test to start arms race : Pakistan», *Reuters* van 27 Feb 2008.

⁵³ The National Institute for Defense Studies Japan, *East Asian Strategic Review* 2008, April 2008, p.27.

⁵⁴ Een globale overzichtsmiddeel met de stand van zaken in 2007 is te vinden op volgende site: <http://carnegieendowment.org/publications/index.cfm?fa=view&id=19364>

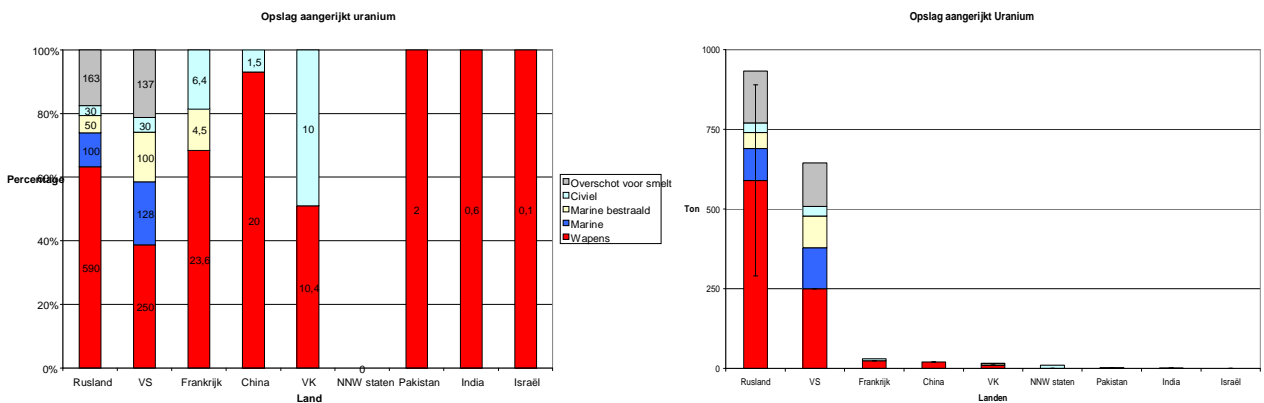
⁵⁵ BOND, R., « The proliferation security initiative: Targeting Iran and North Korea? », British American Security Information Council, BASIC Papers, N°53, January 2007, p.7.

1.3. Capaciteiten van landen en invloedsfactoren

1.3.1. CAPACITEITEN VAN LANDEN

Een bondig overzicht van de bestaande capaciteiten en lopende NBC-programmas wordt weergegeven in bijlage 1⁵⁶. Hierbij moet men vermelden dat de totale erfenis aan splijtstoffen uit de koude oorlog niet in rekening gebracht werd in het overzicht. Voor de volledigheid wordt een overzicht gegeven van de totale reserves HEU in 2007 in volgende figuur:

Figuur 1: verdeling wereldstock aangerijkt uranium (>20%) 2007⁵⁷.



De opslag van plutonium volgt dezelfde tendens voor de militaire capaciteit, hoewel de aantallen beduidend lager liggen (95 +/- 25MT voor Rusland). Bijkomende landen met een (tijdelijke) opslag voor civiele toepassingen zijn diegene met opwerkingsfaciliteiten en onderzoeksreactoren (België, Duitsland, Frankrijk, India, Japan). Een voorstel tot oplossing voor deze enorme reserves zal voorgesteld worden in de aanbevelingen van dit werk.

⁵⁶ Tabel aangevuld uit CIRINCIONE et al., op.cit, p.22. met de bronnen aangegeven in bijlage. Een lijst van kernmachten, hun non-conventionele wapens en raketarsenalen is terug te vinden op <http://www.globalsecurity.org>. Een méér gedetailleerde lijst van alle chemische en biologische programma's, de ondertekening van verdragen en data kan men terugvinden op <http://cns.mis.edu/research/cbw/possess.htm>

⁵⁷ Grafieken stellen een estimatie voor samengesteld uit Global Fissile Material Report 2008, International Panel on Fissile Materials, Princeton University, September 2008, p.11 en http://www.fissilematerials.org/ipfm/pages_us_en/fissile/inventories/inventories.php

1.3.2. INVLOEDSFACTOREN

1.3.2.1. Motivatie tot verwerving van de capaciteit

Verschillende motivaties kunnen de basis vormen voor het verwerven van niet-conventionele wapens. Het realistisch perspectief houdt in dat staten bijvoorbeeld nucleaire arsenalen opbouwen omwille van veiligheidsredenen en internationale dreiging. Dit verklaart echter niet waarom deze staten eerder geneigd zouden zijn om nucleaire wapens te stapelen, dan wel andere niet-conventionele tuigen. Bovendien zou een externe dreiging goed opgevangen kunnen worden door een alliantie met grootmachten of buurlanden. Gezien de continue dreiging, is er een probleem met deze verklaring: het aantal staten dat in dit model de nucleaire capaciteit zou moeten verwerven, zou veel hoger moeten zijn dan het huidige aantal erkende kernmachten. Volgens HYMANS⁵⁸, moet men eerder een uitleg zoeken vanuit een ideologisch standpunt: vanuit nationalistische of culturele, dan wel persoonlijke aspecten, kan men vele aanknopingspunten vinden met betrekking tot de motivatie en de besluitvorming van enkele wereldleiders. Beide benaderingen belichten tot op een zekere hoogte de beperkte vrijheid die leiders genieten; geen van beide opties kan echter verklaren waarom deze beperking politieke beslissingen kan beïnvloeden: een verklaring kan men bijvoorbeeld vinden in internationale competitie of de geloofsovertuigingen van de populatie. Een geldige hypothese voor motivatie tot verwerving van het kernwapen moet zowel de wijzigingen als de continuïteit van een kernwapenprogramma kunnen verklaren. Hiervoor moet men de verklaring zoeken in het onderhouden van de nucleaire mythe. De nationale elite die het land naar een kernwapenprogramma willen drijven zal bijvoorbeeld:

- De nadruk leggen op het gevoel van onveiligheid of de slechte internationale situatie.
- Deze strategie afschilderen als de beste aanpak voor rechtzetting van de precaire situatie.
- Het nastreven van kernwapens afdoen als een haalbaar streefdoel zowel op politiek, economisch als op technisch vlak.
- Deze argumenten proberen te koppelen aan culturele waarden en politieke prioriteiten.
- Ervaren leiders met deze argumenten trachten te overtuigen om ze te aanvaarden en ernaar te handelen.

Het is echter mogelijk dat tegelijkertijd tegenstrijdige visies opduiken en dat tegenstrijdige meningen verkondigd worden aan staatsleiders. Opponenten kunnen net proberen het gevaar van deze politiek te laten inzien door hun leiders. Wie uiteindelijk de beslissing zal doordrukken zal afhangen van verschillende factoren:

- De samenhang van het verhaal en de samenhang van de overwegende culturele achtergrond en politieke prioriteiten.
- De capaciteit om het verhaal te legitimeren en populair te maken onder collega's van de leidende klasse van het land.
- Het succes om de prioriteiten en budgetten om te leggen naar de beoogde objectieven.

Geen enkel van deze argumenten kan echter gebruikt worden zonder ernstig onderliggend veiligheidsrisico: het realistische standpunt zal altijd samen met het ideologische moeten geëvalueerd worden. Er is echter een fundamenteel verschil in

⁵⁸ LAVOY, P., « Nuclear proliferation over the next decade : Causes, Warning Signs and Policy Responses », in *Nonproliferation Review*, Vol.13, N°3, November 2006, p.434 en LAVOY, P., *Nuclear weapons proliferation in the next decade*, Routledge, 2007, p.23.

aanpak tussen beide: het veiligheidsaspect zal aan de basis liggen van de strategische besluitvorming, terwijl het ideologische de aanleiding zal zijn tot politieke debatten die slechts tot hetzelfde eindresultaat kunnen leiden. Aan de basis van het eindresultaat dat bereikt wordt liggen drie kritieke punten:

- Het doel, de inhoud en de logische samenstelling van het verhaal moet samenhangend zijn. Bijvoorbeeld de overtuiging van NASSER dat Egypte kernwapens nodig had om het hoofd te kunnen bieden aan een Israël met kernwapencapaciteit.
- De identiteit, de achtergrond en de overtuigingskracht van de ondersteuner van het ideologisch discours. Vb. BHUTTO en KHAN in Pakistan.
- Het legitimeren en institutionaliseren van kernwapens in de nationale veiligheidspolitiek om soevereiniteit, economische stabiliteit en respect af te dwingen. Vb. de nadruk die Iran legt op het recht op de aanrijkingsexperimenten van uranium, en de verspreiding van deze ideeën naar andere moslimstaten (o.m. Jakarta).

Samengevat is de ideologische benadering gebaseerd op geloof in veiligheid als gevolg van nucleaire wapencapaciteit: mensen beginnen te geloven in de opportuniteit om kernwapens te bemachtigen. Bovendien geloven ze dat het technisch, economisch en politiek haalbaar is om kernwapens na te streven en dus geloven ze deze wapens te kunnen inzetten in een strategische context.

Anderzijds kunnen een aantal (externe) factoren de rechtstreekse oorzaak⁵⁹ zijn om een niet-conventionele wapencapaciteit te verwerven zoals:

- De dramatische toename van het gevoel van onveiligheid door de plotse nucleaire capaciteit van andere staten in de onmiddellijke omgeving.
- De nood aan politiek prestige of herstel van stabiliteit omwille van interne chaos.
- Het ervaren gevoel van (on)betrouwbaarheid van andere partners in een alliantie.
- De verbrokkeling of de groeiende ongeloofwaardigheid van controlesystemen van non-proliferatie.
- Interne factoren zoals persvrijheid en democratie kunnen het verschil maken en de ballans in ene of andere richting doen hellen.
- Het stadium van technologische ontwikkeling van een land kan een beslissende factor zijn om de weg naar WMD te kiezen.

De keuze om de daad bij het woord te voegen zal uiteindelijk niet liggen aan één enkele van voornoemde oorzaken of motivaties. Het zal eerder een combinatie zijn van verschillende factoren die de spreekwoordelijke druppel zal zijn om de stap te zetten naar ontwikkeling van WMD. In de praktijk zal deze keuze in een doctrine moeten terug te vinden zijn, reden waarom doctrines die het gebruik en de verdediging tegen WMD moeilijk te bekomen zijn. Zij legt de onderliggende motivaties bloot die het gebruik of het bezit van WMD moeten verklaren. Inhoudelijk kunnen deze doctrines slechts enkele mogelijkheden bevatten. Officieel zullen doctrines steeds gebaseerd zijn op de verdediging van de Natie⁶⁰:

- Niet conventionele wapens kunnen mogelijks ingezet worden om zowel overweldigende conventionele aanvallen te stoppen als niet-conventionele.
- Een preventieve conventionele aanval kan ondersteund worden om een nabije WMD dreiging te vernietigen.
- Nucleaire respons als gevolg van het eerste gebruik van chemische of biologische wapens. Algemeener kan men zelfs eender welke niet-conventionele respons

⁵⁹ LAVOY, P., op.cit., p.62.

⁶⁰ LAVOY, P., SAGAN, S., WIRTZ, J, Planning the Unthinkable, Cornell University Press, 2000, p.234.

verklaren als gevolg van het gebruik van eender welk andere niet-conventionele aanval.

Deze verklaringen zijn gebaseerd op het behoud van het evenwicht der krachten, maar dit is volgens LAVOY⁶¹ slechts een westerse kijk op de problematiek: nieuwe actoren blijken het gebruik van WMD te plannen om zowel evenwicht te vrijwaren als overmacht af te dwingen. Evolutie van het ene standpunt naar het andere is bovendien niet uitgesloten: defensieve operaties kunnen in een WMD-context snel evolueren naar offensieve operaties. Uiteindelijk zal de militaire doctrine praktische toepassing moeten krijgen in militaire besluitvorming of “command and control” (C²): twee uitersten tekenen het spectrum der mogelijkheden af. Enerzijds kan de besluitvorming gecentraliseerd zijn bij één enkel persoon (cfr. De dictatuur van SADDAM HUSSEIN). Anderzijds kan de besluitvorming gedecentraliseerd zijn en eerder in consensus genomen moeten worden: in dit geval kan men bij één individu hooguit een vetorecht terugvinden. De commandostructuur van de WMD-capaciteit zal een weerspiegeling zijn van de mogelijkheden en de controle uitgeoefend door het betrokken land.

1.3.2.2. Indicatoren voor verwerving van de capaciteit

Wat de nucleaire proliferatie betreft, zijn een eerste reeks indicatoren verbonden met de ideologische benadering van het probleem. Een andere reeks, gebaseerd op de realistische benadering, leggen de nadruk op de veiligheidsproblematiek. Een derde categorie indicatoren behelst verschuivingen in de technische aanpak van een bestaand nucleair programma⁶². De eerste indicatoren zijn gebaseerd op het ideologische karakter van een leider of een staat en omvatten onder meer:

- De inhoud van publieke/politieke toespraken: dit slaat zowel op de uitlatingen van politieke leiders, maar ook op de uitingen van militairen en wetenschappers. De minister van buitenlandse zaken van Noord-Korea kondigde 6 dagen voor de eerste kernproef aan dat in de toekomst kernproeven zouden uitgevoerd worden.
- Politieke debatten over economische, technische en politieke haalbaarheid voor de ontwikkeling van kernwapens en de militaire noodzaak om deze operationeel te houden. De meest gedreven politiek debatten van India i.v.m. kernwapens grepen plaats na de eerste kernproef van China in oktober 1964.
- Reizen van aanhangers van het ideologische gedachtegoed, met name wetenschappers, ingenieurs en iedereen die een kernwapenprogramma ondersteunt. Dit zou kunnen wijzen op de wil om gevoelige technologie te verwerven: de opvolging van de verplaatsingen van A.Q.KHAN hebben ertoe geleid dat zijn netwerk kon ontmaskerd worden.
- Proliferatie gebaseerd op veiligheidsaspecten (realistische visie) is niet altijd vanzelfsprekend. Een ernstige internationale veiligheidsproblematiek kan een noodzakelijke maar geen voldoende voorwaarde zijn om over te gaan tot proliferatie.
- De houding van buurlanden kan cruciaal zijn in de besluitvorming van een land. Hoewel Pakistan initieel verkoos toevlucht te zoeken tot het opdrijven van conventionele wapenarsenalen tijdens het Chinees-Indiaas conflict van 1962 (en de kernproeven van beide partijen), dreef het hopeloos af in de richting van een eigen nucleair arsenaal na de oorlog om Bangladesh in 1971.

⁶¹ LAVOY, P., op. cit., p. 235.

⁶² LAVOY, P., « Nuclear proliferation over the next decade : Causes, Warning Signs and Policy Responses », in *Nonproliferation Review*, Vol.13, N°3, November 2006, p.438.

Verschuivingen in technische aspecten van kernprogramma's zijn de meest betrouwbare indicatoren. Hier stuit men echter op de onwil van sommigen om hun werkelijke bedoelingen prijs te geven, zeker indien een vreedzaam energetisch probleem zijn oplossing vindt in kernenergie. Daarnaast komt nog het feit dat het militaire aspect van kernonderzoeksprogramma's pas aan het licht komt nadat de politieke, economische, technische haalbaarheidsstudies reeds lang uitgevoerd zijn. Daarom is een systeem van tijdige waarschuwingsnetwerken (early warning) nodig en dit is terug te vinden in technische kenmerken:

- Wetenschappelijk onderzoek en opleiding: tenzij er reeds een programma voor kernenergie lopende is, zullen de kandidaat-proliferanten onderzoekers moeten uitsturen om opleiding te volgen.
- Aankoop van specifiek materiaal⁶³, dat onder het waakzame oog van allerhande commissies valt, zal aangekocht moeten worden. Bovendien zal de noodzakelijke infrastructuur reeds moeten bestaan om dit materiaal op te slaan.
- De belopen paden om de technologie te verkrijgen kunnen ook een waardevolle indicatie zijn. Contacten met landen in een uitgesproken militair programma, kunnen wijzen op identieke bedoelingen.
- De wijze om zich de technologie eigen te maken kan sprekend zijn: schijnfirma's, witwaspraktijken en dubieuze geldstromen zullen zeker niet kaderen in een energetisch programma maar eerder in een kader dat het daglicht schuwt zolang het niet operationeel is.

De rol van militairen en veiligheidsagenten in onderzoeksprogramma's wijst zeker in de richting van een verschuiving van de activiteiten naar militaire doeleinden. In Iran bijvoorbeeld heeft het internationaal atoomagentschap er meerder malen op gewezen dat militairen betrokken waren in het beheer van de uraniumertsminen, de processen voor aanrijking van uranium via centrifuges en de verwerking van uraniumerts tot uraniumhexafluoride (UF₆).

Welke lessen kan men hieruit trekken? Kunnen deze indicatoren altijd als maatstaf gebruikt worden? Sinds de uitbreiding van het nonproliferatieverdrag in 1995⁶⁴, wordt iedereen verondersteld het verdrag na te leven omwille van de clausule van "universele uitbreiding" in het verdrag. Een kandidaat die zou streven naar een kernwapenarsenaal, wordt het a priori aanzien als kandidaat proliferator en zal alle aandacht krijgen van de internationale gemeenschap. Bovendien zijn alle landen die de technologie willen aanschaffen in de sector van de kernenergie onderworpen aan stringente controles en inspecties van het IAEA. Om niet op te vallen zal de nieuwkomer moeten starten met geheime programma's. Een ander optie is het opstarten van ogenschijnlijk vreedzame programma's op basis van kernenergie met als enig doel zich later terug te trekken uit het non-proliferatieverdrag. Dit hoeft niet noodzakelijk snel te gebeuren: een gestage toename van de capaciteit zal tijd doen winnen om aan de eisen van het internationaal atoomagentschap te voldoen en ondertussen alle stappen te ondernemen om de uiteindelijke assemblage van het wapen mogelijk te maken.

Indicatoren voor chemische capaciteit kunnen op twee manieren getraceerd worden nl. door de inspecties die opgelegd worden binnen het kader van de OPCW en door terugkoppeling uit alternatieve bronnen zoals inlichtingendiensten, satellietbeelden, etc. Zoals reeds vermeld zijn indicatoren voor productie van chemische wapens veel minder uitgesproken dan voor kernwapens. Men dient

⁶³ EPSTEIN, G., Technologies underlying weapons of mass destruction, International Security and Commerce Program, December 1993, p.119 e.v.

⁶⁴ Zie bijlage twee voor de tekst van het verdrag.

bovendien in gedachten te houden dat geen van de volgende indicatoren op zich voldoende zal zijn om te besluiten dat er daadwerkelijk chemische WMD activiteit opgestart is: het samengaan van verschillende indicatoren zal een sterke aanwijzing zijn, maar het ultieme bewijs zal pas geleverd worden door het vinden van dergelijke wapens. De mogelijke voortekenen van een dergelijke activiteit zijn te vinden in⁶⁵:

- Wetenschappelijk onderzoek: wetenschappelijke publicaties in het domein van de scheikunde kunnen een aanwijzing zijn van de lopende activiteiten van een betrokken land/persoon. Meer nog zal het uitblijven van dergelijke publicaties misschien wijzen op een militarisering van het lopende programma. Informatie verkregen van wetenschappers uit de betrokken gebieden kan natuurlijk ook bijdragen tot het vinden van verdoken agenda's. Betrouwbaarheid van de verkregen informatie moet in dit geval nagezien worden.
- Productiecapaciteit: landen met een lopend chemisch WMD-programma, zullen chemische agentia willen aanschaffen of produceren. Rechtstreekse aanschaf zal slechts mogelijk zijn vanuit landen die reeds de capaciteit bezitten. Aanschaf van precursoren voor eigen productie van chemische agentia is slechts mogelijk door het leveren van eindgebruikers certificaten. Deze documenten worden door leveranciers gevraagd, maar bieden natuurlijk geen garantie indien gebruik gemaakt wordt van tussenpersonen. Indien zowel precursoren als stabiliserende additieven worden aangeschaft of gebruikt kan men de productie van chemische agentia niet uitsluiten. Omgekeerd is de afwezigheid van stabilisatoren geen garantie voor de afwezigheid van een chemisch wapenprogramma. Uitvoer van reactorvaten met specifieke corrosiewerende samenstelling kan een bijkomende indicatie zijn. Controles ter plaatse kunnen nog meer aan het daglicht brengen zoals warmtewisselaars, afstandsbediening van de reactorvaten, afgedichte lokalen in onderdruk en een afvalstoffenbeleid buiten proportie.
- Visuele indicaties (satellietfotografie): chemische productiefaciliteiten worden in zeer verschillende vormen gebouwd. De enige aanwijzingen in dit geval kan men bijvoorbeeld vinden in een constructie die niet vermeld werd in de pers, de geïsoleerde locatie, de uitzonderlijke veiligheidsmaatregelen rond de site, de eigenaardige samenstelling van de gebouwen (om bijvoorbeeld luchtaanval te vermijden), de nabijheid van een munitiefabriek, de nabijheid van transportcapaciteit en de timing van transporten, de aanwezigheid van dode dieren of plantaardig materiaal in de omgeving en uiteindelijke de signalen van een ernstig ongeval dat niet terug te vinden is in de pers.

De biologische wapencapaciteit verdient eveneens een bijzondere aandacht. Zeer kleine hoeveelheden actief agens kan (eventueel na een incubatieperiode) vele slachtoffers maken; verspreiding ervan kan tamelijk eenvoudig gerealiseerd worden en de productie van biologische wapens kan in zeer kleine fabrieken gebeuren die eventueel zelfs in stedelijke omgeving niet zullen opvallen. Ook hier zijn mogelijke signalen terug te vinden van een dergelijke activiteit⁶⁶:

- Wetenschappelijk onderzoek zal niet altijd duidelijk zijn: vooral indien slechts kweekprogramma's onderhouden worden, zal weinig wetenschappelijk werk vereist zijn en dus indicatie kunnen geven van het beoogde doel.
- Inlichtingen van voormalige werknemers kunnen ook hier hun bijdrage leveren.
- Productiecapaciteit: visuele indicatie kan voornoemde informatie eventueel bevestigen nl. excessieve veiligheidsmaatregelen met een infrastructuur voor het onderhoud van grote hoeveelheden proefdieren. Ook hier zal gezorgd worden

⁶⁵ EPSTEIN, G., Technologies underlying weapons of mass destruction, International Security and Commerce Program, December 1993, p.36 e.v.

⁶⁶ EPSTEIN, G., Technologies underlying weapons of mass destruction, International Security and Commerce Program, December 1993, p.100 e.v.

voor de veiligheid van de installaties (biosecurity), evenals voor de veiligheid van de operatoren en de omgeving: men zal er bovendien ook voor moeten zorgen dat micro-organismen niet uit de productiefaciliteiten kunnen ontsnappen (biosafety). Biochemische merkers en DNA-strengen zullen slechts ter plaatste ontdekt kunnen worden.

- Opslag: bioagentia zullen in gekoelde installaties moeten opgeslagen worden. Koelwagens, gekoelde bunkers of laboratoria uitgerust met cryogene ruimten kunnen een goede aanwijzing zijn.
- Gebruik van wapens: of het nu over een ongeval gaat of een vrijwillig gebruik, epidemiologisch onderzoek zal uitsluitel moeten geven over de waarschijnlijkheid van de “natuurlijke oorzaak” van een epidemie. Het opduiken van een endemische ziekte zal meestal in die richting wijzen.

Samenvattend kan men stellen dat de “beste” manier om zo snel mogelijk WMD-capaciteit te verwerven diegene zal zijn die toelaat stapsgewijs de capaciteit op te bouwen zonder argwaan te wekken door:

- Gebruik te maken van materiaal voor tweërlei gebruik, wat per definitie geen ondubbelzinnige indicator kan zijn voor proliferatie.
- Zich te beperken tot het strikte minimum bijvoorbeeld door infrastructuur en personeel te voorzien, maar nog niet noodzakelijkerwijze een samengesteld wapen. Op deze manier voorziet men al het nodige “mocht de noodzaak zich voordoen”.
- Een waas van onzekerheid te onderhouden over het einddoel van technologische programma’s: gezien de moeilijkheid om met absolute zekerheid een WMD capaciteit in wording aan te duiden (zelfs een vreedzaam programma voor kernenergie kan plots een nieuwe wending krijgen), is het eenvoudig te beweren recht te hebben om voor land technologische ontwikkeling beschikbaar te stellen.

1.3.2.3. Voorbeelden: “Declared nuclear weapon states”, “NPT-states”, “non-NPT states” en “non-nuclear NPT states”

Met “Declared nuclear weapon states” bedoelt men de landen die reeds voor de ondertekening van het non-proliferatieverdrag beschikten over het kernwapen. Dit zijn de vijf kernmachten: de Verenigde Staten, Rusland, het Verenigd Koninkrijk, Frankrijk en China. De strategische context in elk van deze landen was duidelijk: in de naoorlogse context van massale bewapening, hebben alle vijf zo snel mogelijk het wapen ontwikkeld, getest, geproduceerd en ontplooid met de capaciteiten die ter beschikking waren. Ook vandaag is de strategische visie op het gebruik van kernwapens soms onthutsend⁶⁷: de VS vervagen de lijn tussen conventionele en niet-conventionele wapens, terwijl Rusland in 2000 in haar nucleaire strategie rekening hield met een beperkte kernwapenoorlog met inzet van strategische kernwapens. In 2006 liet president CHIRAC nog weten dat voor Frankrijk nucleaire afschrikking de basis blijft voor haar veiligheid en die van de overzeese gebieden⁶⁸. In dit opzicht is en blijft het kernwapenarsenaal een gaullistisch prestigeproject voor een land dat zelf erkent niet onder rechtstreeks bedreiging te staan. In China ziet men het kernwapenarsenaal in een doctrine dat twee luiken beslaat: als afschrikking enerzijds, maar ook als nucleaire respons op een nucleaire aanval. Ook het Verenigd Koninkrijk

⁶⁷ PERKOVICH, G., Universal Compliance: a strategy for nuclear security. 2007 Report Card. Carnegie Endowment for International Peace, June 2007, pp.15 e.v.

⁶⁸ DUMOULIN, A., WASINSKI, C., La dissuasion nucléaire française : Paramètres doctrinaux, politiques et techniques. Révolution ou inflexion de la stratégie en post-guerre froide (1990-2006) ?, Ibidem, n°2006/1, Septembre 2006, p.82.

blijkt zijn huidige status te willen behouden: het plant een nieuwe klasse kernreactor aangedreven onderzeeër (gewapend met ICBM) te bouwen tegen 2020 om de huidige klasse duikboten te vervangen⁶⁹.

Het traject van India, Pakistan en Israël was enigszins anders. Géén van deze landen heeft het non-proliferatie verdrag ondertekend (vandaar de classificatie onder non-NPT states), met als gevolg dat de ontwikkeling van de capaciteit kon plaatsgrijpen zonder inmenging van IAEA. Bovendien hebben ze de capaciteit verworven vóór de uitbreiding van het NPT. India heeft pas 24 jaar na de opstart van haar kernwapenprogramma een eerste kernproef uitgevoerd (mei 1998). Als voornaamste reden om het kernwapen te bemachtigen werd de Chinese dreiging aangevoerd⁷⁰(veiligheidsmotivatie). Pas na de Indiase testen heeft ook Pakistan kernproeven uitgevoerd: de angst voor de dreiging vanuit het buurland India (veiligheidsmotivatie), maar ook de ideologische motivatie om het kernwapen in handen te hebben van een islamitisch land, waren de belangrijkste drijfveren. Diezelfde maand voerde Pakistan haar eerste proef uit. Israël daarentegen heeft nooit testen uitgevoerd en heeft zich nooit uitgeroepen als kernmacht. Er wordt aangenomen dat het kernwapens bezit uit veiligheidsoverwegingen (weinig territoriale ruimte voor beweging van conventionele troepenmacht en onuitputtelijkheid van troepenmacht van buurlanden). In 1981 veranderde het defensief concept van Israël naar een conventionele offensieve positie (bombardement van de kernreactor van Osiraq-Irak) om te verhinderen dat een nabijgelegen land kernwapens zou kunnen ontwikkelen.

Tijdens de conferentie van New-York van 11 mei 1995 werd het NPT herzien en uitgebreid⁷¹. Ten gevolge van de uitbreiding, worden alle landen die vanaf dan nucleaire wapens zouden nastreven, aanzien als NPT landen zonder kernwapencapaciteit (non-nuclear NPT states⁷²). Hierdoor krijgt het internationaal atoomagentschap, door het verdrag aangeduid als controleorganisme, algemeen toezicht op alle daaropvolgende nucleaire activiteiten.

In deze aangepaste situatie is het aanneembaar dat, zoals eerder vermeld, Noord-Korea en Iran op gespannen voet leven met het IAEA door hun streven naar het kernwapen. Hoeveel kernwapens Noord-Korea reeds geproduceerd heeft is niet bekend, maar een onderzoeksreactor voor de productie van plutonium is operationeel in Yongbyon⁷³. Wat Iran betreft, blijven de activiteiten in het kader van onderzoek naar springstof en vectoren zorgen baren aan het internationaal atoomagentschap en de Verenigde Naties. Wat voor Iran een vreedzaam kernenergetisch programma is, kan op basis van wat eerder werd uiteengezet, een verschuiving aanduiden naar militaire doeleinden.

⁶⁹ Stockholm International Peace Research Institute, SIPRI Yearbook 2007. Armaments, Disarmament and International Security, Oxford, Oxford University Press, 2007, p.20.

⁷⁰ CIRINCIONE, J., WOLFSTHAL, J., RAJKUMAR, M., Deadly Arsenals: nuclear, biological and chemical threats. Carnegie Endowment for International Peace, 2005, p.223.

⁷¹ Zie bijlage 2.

⁷² Dus niet India, Pakistan of Israël aangezien deze landen reeds over het wapen beschikken.

⁷³ Op 25 april 2008 werd door de CIA gesuggereerd dat de Syrische infrastructuur in aanbouw te Deir ez-Zor en vernietigd door een Israelische luchtaanval op 6 september 2007, een plutonium-opwerkingsfabriek betrof, gebouwd met de hulp van Noord-Korea (naar het voorbeeld van de Yongbyon-reactor).

1.3.2.4. Gevolgen voor een (nucleaire) non-proliferatie strategie en de bedreiging

Om proliferatie verder in te dijken, is een snelle aanpak noodzakelijk: hiervoor moeten een aantal alarmsignalen herkend worden om een nieuwe kandidaat-proliferator ondubbelzinnig als dusdanig te kunnen identificeren. Gebaseerd op de motivatie om een kernwapen te bemachtigen kunnen een aantal maatregelen genomen worden: in het kader van het ideologische model, moeten staten meer en meer betrokken worden tot internationale allianties. Zoals aangetoond in de NAVO en de EU is een alliantie de (voorlopig) beste garantie om proliferatie een halt toe te roepen. Om die reden ook zouden zowel de NAVO als de EU zich meer moeten inzetten om aan te tonen dat er meer te winnen is bij een goed verdrag en politieke openheid (confidence building measures) dan bij het streven naar onconventionele wapens. Verder moet er nagestreefd worden om de politieke, technische en economische hindernissen tot het bekomen van dergelijke wapens onoverbrugbaar te maken: dit zijn vereisten die de geloofwaardigheid van controleorganismen (bijvoorbeeld het IAEA in het geval van kernwapens) zal vrijwaren en andere staten zal afschrikken om nutteloze pogingen te ondernemen (zoals Libië) of zware investeringen aan te vangen in een land dat reeds het slachtoffer is van een tanende economie.

Sinds de aanval met saringas in Tokio (1995) en de aanslagen op de Twin Towers in de VS (2001), zijn de kaarten echter grondig herschud: niet enkel landen hebben het monopolie in het gebruik van WMD, maar ook niet-staatsactoren kunnen ze bemachtigen. Het gevolg is dat alle concepten en doctrines vanaf dan moesten herschreven worden: NBC-verdediging wordt niet enkel meer beschouwd als een strategisch concept dat ergens ten velde moet kunnen toegepast worden, maar ook op eigen grondgebied en zelfs (voornamelijk) in stedelijke omgeving. Non-proliferatie moet bijgevolg uitgebreid worden en eveneens de aandacht richten naar het verhinderen van smokkel van WMD-materiaal, controle van export en van geldstromen van/naar niet-staatsactoren die WMD willen bemachtigen. De voorstellen om vreedzame kernenergie toegankelijk te maken voor iedereen is een lovenswaardig initiatief dat verder bestudering vereist. Uitvoeringsmodaliteiten en een strikte controle zullen moeten garanderen dat de beschikbare brandstof niet afgeleid wordt voor militaire doeleinden. In dit opzicht is het ook moeilijk te aanvaarden dat in 2005 de VS (kernwapenstaat die de conventie voor stopzetting van kernproeven nog niet heeft geratificeerd) een akkoord sluit met India (een land in overtreding met NPT) om brandstof te leveren voor energieproductie. De goedkeuring van deze akkoorden werden bekrachtigd door het IAEA, de NSG, en het Congres van de VS in de loop van 2008. Het akkoord voorziet zelfs dat India in ruil enkele reactoren onder internationale controle zal plaatsen, maar zelf de keuze zal maken over welke installaties onder het militair programma blijven opereren (en dus buiten de controles van het IAEA zullen vallen)⁷⁴. Pakistan zal deze evolutie niet aanvaarden en blijven ijveren om haar kernwapenarsenaal op peil van de grote buur te houden. In het vooruitzicht van de herziening van het NPT in 2010 wordt hier een gevaarlijke aanzet gegeven tot nieuwe initiatieven tot proliferatie in Zuid-Azië. Het moment leek nochtans gunstig om India te dwingen deel te nemen aan de NPT-akkoorden: natuurlijke uraniumbronnen zijn beperkt in India en de huidige productie blijkt volgens sommige analyses beperkt te worden door de uitputting van deze bronnen⁷⁵. Amerika heeft er anders over beslist. De enige zinnige verklaring die men hieraan kan geven is dat de VS een duidelijk signaal willen sturen naar China (dat evenmin de conventie voor stopzetting van kernproeven ratificeerde) om zo de druk op India te

⁷⁴ SOKOLSKI, H., Pakistan's nuclear future: worries beyond war. DOD, Strategic Studies Institute, January 2008, pp. 153 e.v.

⁷⁵ SOKOLSKI, H., op.cit., p.186.

verlichten. Hierdoor komen op kort termijn zowel Pakistan als de VN in een moeilijke positie: door deze bilaterale akkoorden, wordt het NPT de facto genegeerd en Pakistan zal zich verplicht voelen ook haar arsenaal op te drijven.

1.3.2.5. Gevolgen voor de bedreiging binnen de EU

Gezien de hoger vernoemde elementen, kan men zich de vraag stellen welke de actuele dreiging is voor de EU en welke vorm die zou aannemen. Dat er een dreiging is, is ondertussen duidelijk: er is enerzijds een capaciteit zowel bij staten als niet-staatsactoren, en anderzijds een wil om die capaciteit in te zetten⁷⁶. De dreiging kan echter verschillende vormen aannemen:

- Dreiging op globaal vlak: in het kader van de globalisatie van de economische markten en het proliferatieregime dat de kop opnieuw zou kunnen opsteken, is er een dreiging voor gewapende conflicten in gebieden verspreid over de hele wereld. Bovendien kan er omwille van de tanende economische groei, meer en meer druk op de wapenindustrie komen om te verkopen.
- Verval van verdragen: zoals reeds vermeld, werden door vele partijen de non-proliferatieverdragen niet nageleefd omdat ze er niet werden toe verplicht. De biologische wapen conventie (BTWC) werd nooit geconcretiseerd naar uitvoering toe en het non-proliferatieverdrag is meermaals met de voeten getreden zonder efficiënte internationale reactie. Indien de opgelegde normen niet nageleefd worden door een aantal actoren, zou de wapenwedloop in alle deeldomeinen van het CBRN gebeuren kunnen hervatten.
- Regionale dreiging: gebieden die grenzen aan de EU (en zelfs kandidaat-lidstaten zoals Turkije of Georgië) zijn vaak verwickeld in regionale conflicten. Het bezit van CBRN wapens door staten of niet-staatsactoren kan regionale conflicten aan de poorten van Europa in een CBRN scenario dompelen.
- Directe bedreiging: zowel lidstaten als instellingen kunnen, gezien de gebeurtenissen in de reeds vermelde hoofdsteden van Spanje en het VK, rechtstreeks bedreigd worden. Dit was trouwens het geval voor groeperingen die zichzelf, al dan niet rechtmatig, het “Al-Qaeda” lidmaatschap toeschreven.
- Dreiging op personeel of geprojecteerde troepen: het toenemende aantal vredesondersteunende operaties (geprojecteerde militaire troepen) overal ter wereld, en het toenemende aantal NGO's vormen een gemakkelijk doelwit. De inplanting zelf van dit personeel kan soms in gebieden zijn die verlaten industriële sites of verlaten industriële- of wapenopslagplaatsen herbergen. Hierdoor is zelfs een accidentele besmetting mogelijk.
- Onrechtstreekse bedreiging door aantasting van economische belangen: de talrijke politieke en economische belangen van de EU wereldwijd kunnen ernstig in het gedrang komen in een regio waar proliferatie opnieuw de norm wordt.
- Ongeval op eigen grondgebied: de problematiek van de opslag en de veiligheid van NBC materiaal kan een belangrijke bedreiging vormen voor de bevolking van de EU. Zoals reeds aangetoond is de dreiging voor aanslagen op eigen grondgebied reëel. Het bestaan van vitale infrastructuur die onvoldoende bewaking/bescherming geniet zou door beschadiging (en eventuele daaruit voortvloeiende besmetting van bevolking) zowel politieke, economische als sociale instabiliteit veroorzaken in betrokken landen en de EU in haar totaliteit.

⁷⁶ We verwijzen in dit verband opnieuw naar de aanslagen in Tokyo, New-York, Madrid en Londen. Voor de impact van een nucleaire besmetting van beperkte aard kan men verwijzen naar de maatregelen en opsporingen die uitgevoerd werden naar aanleiding van de vergiftiging van LITVINENKO met een bron van ioniserende α -straling.

1.4. Transfers van kennis, technologie en materieel

Transfer van WMD-materiaal en technologie naar staten en niet-staatsactoren, werd meermaals vastgesteld. Men kan hier enkele voorbeelden aanhalen:

- Het netwerk van A.Q.KHAN, een Pakistaanse wetenschapper, werd in 2003 blootgelegd: dit netwerk opereerde tussen 1982 en 2002 en onderhandelde met o.m. Noord-Korea, Libië, Irak en Iran⁷⁷. Leveringen van technologie en materieel werden aangebracht langs verschillende smokkelroutes via land-, zee- en luchttransport (zie bijlage 3). Opmerkelijk is dat in het geval van Khan vooral staten eindgebruiker waren en dat het onderwerp van de onderhandelingen vooral nucleaire technologie betrof.
- Ook vanuit Centraal-Azië en de Kaukasus, werden tussen 2001 en 2006 meer dan 171 gevallen van illegale transfers gemeld⁷⁸. In het geval van Centraal-Azië ging het in 95% van de gevallen over transfers van radioactieve bronnen (bruikbaar voor RDD of “vuile bommen” maar niet voor kernwapentechnologie of kernenergie). In slechts 1 geval was een chemisch agens betrokken (Mosterdgas uit Georgië, 2003) en in één ander geval een biologisch agens (niet-pathogeen Ebola uit Oekraïne, 2002). Deze smokkel werd voornamelijk georganiseerd door criminele organisaties of werkloze wetenschappers: eindgebruikers waren in dit geval niet-staatsactoren.
- De regio rond de Zwarte Zee blijkt een uitgelezen bron van onrechtmatige transacties in zake WMD-materiaal⁷⁹. Deze streek lijkt zeer gegeerd voor illegale transfers van materiaal en technologie voor tweeeërlei gebruik: de regio speelt immers een prominente rol in transport per schip (onder meer van olie en gas). De weg voor transport van illegale goederen ligt dus open in deze gebieden waar de voorgeschreven controles niet kunnen nageleefd worden omwille van gebrek aan technologie of de onmogelijkheid om het toezicht te verscherpen omwille van de enorme kwantiteit van de voorziene transporten.

Een aspect waar voorlopig weinig informatie over te vinden is betreft “soft proliferatie” m.n. transfers van technische gegevens, kennis, expertise en financiële transacties via internet. Uit de eigenschappen van het Net om de communicaties voor iedereen toegankelijker te maken, vloeit voort dat illegale activiteiten langs dit medium hun weg zullen vinden, ook op het gebied van proliferatie.

De algemene trend, die men kan vaststellen in gevallen van transfer, komt overeen met de vaststelling die gemaakt werd bij de bespreking in het kader van proliferatie nl. dat voornamelijk het nucleair materiaal zeer gegeerd is. Chemisch en biologisch materiaal komen ook hier minder vaak aan bod omdat zowel materiaal als

⁷⁷ SOKOLSKI, H., Pakistan's nuclear future: worries beyond war. DOD, Strategic Studies Institute, January 2008, pp.9-10.

⁷⁸ Conferentie « Terrorism, Transnational Networks and WMD Proliferation: Indications and Warning in an Era of Globalization » georganiseerd door Center for Contemporary Conflict, Monterey, 25-27 July 2006, bijdrage van Dr. S.B. OUAGRHAM: kaart van gebruikte routes voorgesteld in bijlage 3b.

⁷⁹ NELSON, D., « Trafficking in Destruction », *Center for Arms Control and Non-Proliferation*, June 2007, p.1.

grondstoffen tamelijk eenvoudig verkrijgbaar zijn zonder getraceerd te worden. Synthese en verwerking van eindproducten kan door de eindgebruiker (staat of individu) zelf gebeuren. Hierdoor komen biologische en chemische agentia veel minder vaak op de zwarte markt voor. Het IAEA heeft sinds 1993 een lijst bijgehouden van alle incidenten met betrekking tot bronnen van ioniserende straling onder de naam "Illicit Trafficking Data Base" (ITBD): een uittreksel hiervan is terug te vinden in bijlage 4. Opmerkelijk in deze lijst is dat het betrokken materiaal eveneens van dien aard is dat het niet kan gebruikt worden in kernwapens (ofwel is de concentratie splijtstof te laag, of de totale hoeveelheid splijtstof is te klein, of het gaat eenvoudig om materiaal dat geen kernreacties onderhoudt maar wel bron is van ioniserende straling). Men dient wel rekening te houden met het feit dat de ITBD een repertorium is van vrijwillig aangegeven incidenten door de staten zelf. Anderzijds komen er ook de incidenten in voor die gecatalogeerd werden uit het naslaan van open bronnen. Geslaagde transacties die in de clandestiniteit gebeuren, kunnen per definitie niet voorkomen op deze lijst. Het is echter wel duidelijk dat de trend die zich aftekent van 1991 tot 2005 een afname inhoudt van smokkel in splijtstof en een sterke toename van ioniserende bronnen. Deze laatste zijn veel gemakkelijker te verkrijgen. Hoewel deze stoffen niet bruikbaar zijn voor de samenstelling van kernwapens of kleine kernwapens, zijn ze wel geschikt om in radiologische dispersiemechanismen te gebruiken (Radiological Dispersal Device, RDD of vuile bom). Indien men de leveranciers, tussenpersonen en gebruikers van dergelijk materiaal erop natrekt komt men tot volgende vaststellingen⁸⁰:

- Leveranciers zijn meestal burgers die voordien werkzaam waren op sites waar radioactieve bronnen werden gebruikt. Verkoop van dergelijk materiaal moest hun het nodige geld opbrengen om het levensnoodzakelijke te kopen na het verval van de Sovjet-Unie. Hoog radioactief materiaal, eventueel uit kernwapens, werd eerder door militairen op de zwarte markt gebracht. In beide gevallen ging het eventueel over bewakingspersoneel dat gemakkelijk toegang had tot de installaties. Zeer uitzonderlijk werden diefstallen gepleegd door buitenstaanders maar ook in dat geval was winstbejag de drijfveer.
- Tussenpersonen en smokkelaars waren in de meeste gevallen amateurs, in sommige gevallen zakenlui (met eventueel firma's als dekmantel). Georganiseerde criminaliteit hoort ook thuis in deze categorie: omwille van de bestaande netwerken en relaties is het hen gemakkelijker om dergelijk materiaal aan de man te brengen.
- Eindgebruikers kunnen zowel staten (Noord-Korea, Iran, Irak) als niet-staatsactoren zijn: in deze categorie vallen terroristische groeperingen, sectes, criminele bendes en afscheidingsbewegingen.

Opvallend is dat de grote meerderheid aan incidenten zich hebben afgespeeld in de voormalige Sovjet-Unie. Het bewijs dat de dreiging wel degelijk reëel is werd reeds geleverd in 1995: tijdens de Tsjetsjeense opstand liet S.BASAJEV vier radioactieve vaten begraven in het IZMAILOVSKY park van Moskou. Omdat de vaten zeker gevonden zouden worden, verwittigde hij zelf de TV stations⁸¹. Drie jaar later werd een RDD gevonden naast de spoorweg van Argun: dezelfde afscheidingsbeweging werd verantwoordelijk geacht voor dit incident.

Om transfers/smokkel van wapens en materieel voor tweeërlei gebruik tegen te gaan, werd in de EU de verordening EG 1334/2000⁸² uitgevaardigd die de basis vormt voor het wapenexportbeleid van alle landen van de EU. In België zijn het

⁸⁰ ZAITSEVA, L., HAND, K., « Nuclear smuggling chains », in *American Behavioral Scientist*, Vol.46, N°6, February 2003, pp. 822-844.

⁸¹ ZAITSEVA, L., HAND, K., op.cit., p.838.

⁸² Deze verordening werd voor het laatst gerectificeerd op 21 november 2007.

wapenexportbeleid en export van goederen voor tweërlei gebruik geregionaliseerd sinds 2003. In onze buurlanden zijn in-, uit-, en doorvoer een nationale aangelegenheid. In principe zijn in België gewestelijke decreten van toepassing. Indien die niet uitgevaardigd werden, blijft de nationale wetgeving van toepassing.

Naast deze wet op in-, en uitvoer, is ook de wapenwet van kracht in ons land. Deze is echter niet van toepassing op in-, uit-, of doorvoer van materiaal voor tweërlei gebruik. Het bekomen van een vergunning voor wapenhandel wordt wel voorafgegaan aan de criteria van deze wapenwet⁸³.

Uitvoer van militair materieel is onderworpen aan de Belgische in-, uit-, en doorvoerwet van 5 augustus 1991⁸⁴. Bovendien geldt de vergunningsplicht voor deze goederen alsook eventuele programmatuur, technologie of machines voor ontwikkeling, onderhoud of gebruik. De Minister van Economische zaken is verantwoordelijk voor de aflevering van vergunningen via de Dienst Controle Wapenbeleid. Deze dienst zal eerst een administratieve controle uitvoeren, vervolgens een technisch, juridisch en ten slotte een politiek advies verlenen:

- Het technisch advies zal voornamelijk betrekking hebben tot mogelijke toepassingen van het materieel door de eindgebruiker.
- Het juridisch advies zal zich richten op de naleving van de geldende internationale verdragen omtrent proliferatie.
- Het politiek advies wordt gegeven met betrekking tot de naleving van de EU-gedragscode⁸⁵.

Deze procedure is eveneens van toepassing voor de uitvoer van materieel voor tweërlei gebruik. De basis voor deze procedure is de doorvoerwet van 1962, maar de verordening EG 1334/2000 heeft hier een vernieuwing gebracht m.n. een lijst van materieel onderworpen aan een vergunning voor uitvoer of wederuitvoer. Transacties binnen de EU vereisen in principe geen vergunning behalve voor goederen opgenomen in bijlage 4 van de verordening, maar binnen de Benelux (vertrekpunt en eindbestemming) is zelfs die vergunning niet vereist. Om te verhinderen dat nucleair materiaal, installaties en uitrustingen, nucleaire technologie of goederen voor tweërlei gebruik, ook zouden worden gebruikt voor de ontwikkeling of vervaardiging van kernwapens, kan een uitvoervergunning voor dergelijke goederen slechts worden verleend na het bekomen van een voorafgaande machtiging van de bevoegde ministers, namelijk de minister van Buitenlandse Zaken en de minister van Economie. De ministers baseren hun beslissing op het advies van de Commissie van Advies voor de Niet-Verspreiding van Kernwapens (CANVEK). Deze commissie is in het leven geroepen overeenkomstig het K.B. van 12 mei 1989: ze zal de vergunningsaanvraag onderzoeken en eventueel, gebaseerd op advies van experts ter zake (vertegenwoordigers van alle Federale Overheidsdiensten en ministeries), verder onderzoek verrichten naar:

- Het materiaal dat onderwerp uitmaakt van de aanvraag: er moet zekerheid bestaan dat het materiaal, de technologie of de uitrusting niet zullen gebruikt worden tijdens het productieproces van kernwapens.
- Het land van bestemming: dit zal garanties moeten voorleggen via het IAEA dat het voldoet aan de geldende internationale non-proliferatieverdragen (en de waarborgovereenkomst, beter bekend onder de Engelse benaming “safeguards-agreement”).

⁸³ Een vergelijkende studie van het wapenexportbeleid: Vlaanderen en zijn burens, Vlaams vredesinstituut, Rapport maart 2007, p.16.

⁸⁴ Aangepast door de wet van 12 augustus 2003.

⁸⁵ Het Vlaams wapenexportbeleid: een analyse van de juridische context, Vlaams vredesinstituut, Rapport oktober 2007, p.116.

- Fysieke bescherming om diefstal of onrechtmatig gebruik te voorkomen.
- Verhandeling: er moeten voldoende garanties bestaan dat het materiaal, de uitrusting of de technologie, niet verder zullen uitgevoerd (doorgevoerd) worden zonder voorafgaande toestemming van België.

Men kan hier de bemerking maken dat een aanpassing van het wettelijk kader ook de basis zou kunnen leggen voor een regeling omtrent de problematiek van “soft proliferatie”(voorstellen in die zin zullen geformuleerd worden in deel 3 van dit werk).

Doorvoer van militaire goederen is onderworpen aan de nationale wetgeving. In principe gelden hier dezelfde regels als voor uitvoer, maar doorvoer wordt door de douanereglementering beschreven⁸⁶ en deze is geen nationale maar een gewestelijke bevoegdheid! Hierdoor wordt doorvoer enkel onderworpen aan vergunningen indien de bestemming niet binnen de EU ligt en er een verandering van transportmiddel gebeurt. Bovendien zijn in dit geval noch het internationaal invoercertificaat, noch het certificaat van eindbestemming vereist. Voor goederen met tweërlei gebruik, vervalt bovendien de vergunningsplicht indien reeds (elders) een communautaire uitvoervergunning werd verleend. Bovendien is er zelfs geen meldingsplicht voor doorvoer die niet onderworpen is aan een vergunning. Hier zou men zich kunnen afvragen waarom doorvoer niet op zijn minst nationaal wordt beheerd. Een eerste stap in de goede richting zou kunnen gezet worden door de oprichting van een nieuwe nationale cel en de invoering van de meldingsplicht. Deze cel zou doorvoer kunnen traceren en doorgeven naar een hoger echelon (EU). Bovendien kan op die manier een databank bijgehouden worden (op nationaal niveau) dat zowel de aard van materieel, de bestemming en de gevolgde route bijhoudt. Vlaanderen (door zijn zee- en luchthavens) en Wallonië (als transit) vormen (samen met Luxemburg) een ideaal doorstroom voor goederen voor tweërlei gebruik. Het rapport Vlaanderen van 2008⁸⁷ vermeldt: “... Terwijl er in 1999 nog 136 Nederlandstalige doorvoervergunningen werden uitgereikt, ligt dit cijfer in 2007 met 16 doorvoervergunningen opvallend laag (een vermindering met factor 8,5). De vaststelling dat eind jaren negentig een groot aantal doorvoervergunningen werd aangevraagd en goedgekeurd, toont aan dat logistieke knooppunten in Vlaanderen wel degelijk gebruikt worden om militair materieel⁸⁸ door te voeren. Dat in 2007 niet meer dan 16 doorvoertransacties voor militaire goederen werden vergund, wekt dan ook verbazing, aangezien het totale vrachtvervoer in Vlaanderen de afgelopen jaren niet is gedaald.”

Dit zou kunnen betekenen dat doorvoer van materieel voor tweërlei gebruik (zonder registratie of zonder verandering van transportmiddel) niet is verminderd. Aangezien het niet kan worden getraceerd wanneer het niet op een lijst van goederen voorkomt die onderworpen is aan een vergunningsaanvraag, is er geen sluitende traceerbaarheid. Een argument dat in die richting wijst kan men vinden in heit feit dat het aantal individuele exportlicenties voor goederen voor tweërlei gebruik in 2007, een zelfde orde van grootte betrof als die voor export van militair materieel.

Het Federale niveau is nog steeds bevoegd voor wapenhandel van Defensie of de Federale Politie. Ondanks de door de federale wapenwet vastgelegde rapportageplicht (per land, per categorie van bestemming, met vermelding van het

⁸⁶ Een vergelijkende studie van het wapenexportbeleid: Vlaanderen en zijn burens, Vlaams vredesinstituut, Rapport maart 2007, p.57.

⁸⁷ Vlaamse buitenlandse handel in wapens en goederen in tweërlei gebruik 2007, Vlaams vredesinstituut, Rapport maart 2008, pp.47-48.

⁸⁸ Eigen onderstropping.

totaalbedrag en de weigering of toekenning van de vergunning), levert FOD Economie slechts heel beknopte verslagen (tabellen en cijfers zonder uitleg).

Wallonië heeft geen gedetailleerde statistieken tussen 2003-2005. Het eerste rapport, die naam waardig, is het "Rapport armes 2006". Een beoordeling van het rapport laat blijken dat voor de eerste maal melding wordt gemaakt van het aantal toegekende licenties en hun respectievelijke bedragen. Men kan echter niet terugvinden wie de klant is en welk type materieel verhandeld werd. Bovendien kan men enkel de informatie vinden voor de toegekende exportvergunningen: er is nergens spoor van geweigerde vergunningen, noch voor import, noch voor doorvoer. Deze gegevens zijn nochtans nuttig omwille van transparantie zelf, maar ook om de besluitvorming te achterhalen die aan de basis ligt voor het toekennen of het weigeren van licenties. Een laatste opmerking kan men nog geven over de tijd nodig om een rapport te publiceren (in mei 2008 was slechts het rapport van 2006 beschikbaar).

Het Brussel Hoofdstedelijk Gewest publiceert in haar verslagen zowel de gegevens van import als export en doorvoer. Voor ieder betrokken land worden het aantal vergunningen, hun prijswaarde, het type materieel en de klant aangegeven. Sinds de regionalisering van 2003 is echter geen enkele vergunning geweigerd door dit Gewest.

Vlaanderen ten slotte geeft voor alle vergunningen (import, export en doorvoer) ook alle betrokken klanten weer. Iedere vergunning wordt bovendien afzonderlijk vermeld, of het nu om een positief of een negatief advies gaat. Verder worden ook de marktwaarde weergegeven, de aard van het materieel en de eindgebruiker. Dit is het enige Gewest dat de EU-gedragscode met betrekking tot rapportering in zake nomenclatuur van de verschillende goederen naleeft.

Ook hier zou meer transparantie en uniformiteit tot een betere (inter)nationale cohesie kunnen leiden. Vlaanderen heeft algemeen een wapenbeleid dat sterk lijkt op deze van onze buurlanden, maar er is nog verbetering mogelijk. Ook in het toekennen van vergunningen zouden meerdere overheidsdiensten betrokken moeten worden, zoals dat bij onze bureaus het geval is: dit laat toe om meer informatie uit te wisselen en sterkere controle uit te oefenen op de transacties. FOD Buitenlandse Zaken zou altijd betrokken moeten worden in de besluitvorming (zelfs wanneer de gewestelijke instanties in principe autonoom kunnen beslissen) m.n. in het domein van doorvoer.



1.5. Deelbesluit

Op het gebied van proliferatie merkt men verschillende mogelijke scenario's die zich kunnen afspelen in de toekomst. Vooral Azië schijnt de komende jaren (horizon 2030) nog in de schijnwerper te zullen blijven, voornamelijk op het gebied van kernenergie, kernwapens en hun vectoren. Regionale conflicten kunnen een nieuwe escalatie uitlokken in de bewapening van de betrokken gebieden. Vooral Noord-Korea (dat zich terugtrok uit het non-proliferatieverdrag) en Iran (lid van het NPT maar biedt geen ondubbelzinnige klaarheid ten opzichte van het IAEA) baren de internationale gemeenschap zorgen. De vijfjaarlijkse herziening van het non-proliferatieverdrag in 2010 zal een belangrijke hindernis zijn die ongedeed overwonnen moet worden. Het falen van de samenhang en de consensus rond dit verdrag zou een nieuwe aanzet geven tot ongecontroleerde verspreiding van alle niet-conventionele wapens. Om dit te vermijden moeten ook de vijf kernmachten verder ontwapenen binnen het kader van de bestaande akkoorden. Als permanente leden van de VN-veiligheidsraad, geven zij ook de richting aan van de internationale besluitvorming. Het is niet aanvaardbaar, vanuit het standpunt van een land dat onderworpen is aan het NPT, om normen en beslissingen opgelegd te krijgen van één of meerdere landen die reeds de capaciteit bezitten maar zelf niet moeten voldoen aan alle eisen die aan anderen wel worden opgelegd. Net daarom is het zo belangrijk dat de vijf kernmachten het voorbeeld geven: dan pas zal men op legitieme en ondubbelzinnige wijze de naleving van de verdragen kunnen afdwingen van Iran en Noord-Korea.

De uitbreiding van het NPT van 1995 zou bovendien moeten nageleefd worden door de kernmachten de facto (India, Pakistan, Israël). Dit zou de lont uit het kruitvat halen in vele regio's: Israël moet op die manier haar bestaansrecht gegarandeerd zien door alle Arabische landen. India kan op die manier de conflicten met Pakistan oplossen. Ook vanuit dit standpunt ziet men de bevestiging van het belang van de afbouw van de kernwapencapaciteit van de kernmachten. India zal immers nooit aanvaarden om haar wapens af te bouwen, indien China als buurland geen inspanningen levert om het kernwapenarsenaal te verminderen en verder proeven blijft uitvoeren. In dat geval kan men ook Pakistan niet overtuigen tot nucleaire afbouw omwille van het veiligheidsrisico. In dit kader zou het onaanvaardbaar zijn dat erkende kernmachten akkoorden sluiten met de facto kernmachten omtrent nucleaire activiteit: dit zou een impliciete erkenning zijn van de actuele toestand en bijgevolg ieder initiatief tot definitieve regeling van conflicten in het gedrang brengen. Het initiatief van de administratie BUSH om bilaterale akkoorden voor de levering van splijtstof aan India valt dus ook niet toe te juichen.

Naast het rechtstreekse gevaar voor het voortbestaan van het NPT, zijn er onrechtstreekse gevaren voor het voortbestaan van het NPT verbonden aan dit commercieel akkoord: Pakistan heeft zich steeds bedreigd gevoeld door India. Als buurlanden hebben de twee reeds meerdere conflicten uitgevochten en blijven actuele spanningen in regio's als Kashmir beide protagonisten onder druk zetten. Hierin heeft Afghanistan eveneens een rol te spelen: Pakistan heeft in deze regio zowel strategische (als mogelijke terugvalbasis bij mogelijke aanval), als economische belangen (Afghanistan biedt toegang tot de olie- en gasreserves van Centraal Azië). De onherbergzame grensstreek tussen Pakistan en Afghanistan is echter een veilige basis voor Talibanstrijders. Bij het begin van het ambtstermijn van president

ZARDARI in september 2008⁸⁹, werd de Pakistaanse overheid door de Taliban meermaals bedreigd en Pakistan schijnt niet de gepaste respons te kunnen bieden ten aanzien van deze bedreiging op eigen grondgebied: een toenemende invloed van niet-staatsactoren in een (verzwakte) kernwapenstaat als Pakistan is wel het ergste scenario dat men zich zou kunnen inbeelden. Veiligheidsgaranties voor Pakistan en India kunnen ervoor zorgen dat onderlinge conflicten een halt wordt toegeeroepen en dat de Taliban-contaminatie in Pakistan adequaat wordt aangepakt.

Nieuwe initiatieven zullen op korte termijn (2010) genomen moeten worden om het NPT in stand te houden. In dat opzicht lijkt er, als we de Franse president SARKOZY mogen geloven, een goede weg ingeslagen te zijn. Inderdaad, tijdens de toespraak te Cherbourg op 21 maart 2008, ter gelegenheid van de voorstelling van de nieuwe kernonderzeeër “Le Terrible”, stelde hij een actieplan voor in het kader van de voorbereiding van de conferentie in 2010 ter herziening van het NPT. Hij detailleerde dit actieplan als volgt⁹⁰: «...J’invite ainsi tous les pays à ratifier le Traité d’Interdiction Complète des essais nucléaires, à commencer par la Chine et les Etats-Unis qui l’ont signé en 1996. Il est temps de le ratifier. J’engage les puissances nucléaires⁹¹ à démanteler tous leurs sites d’essais nucléaires, de manière transparente et ouverte à la communauté internationale. Je propose de lancer sans délai les négociations sur un traité d’interdiction de production de matières fissiles pour les armes nucléaires et de mettre en place un moratoire immédiat sur la production de ces matières. J’invite les cinq puissances nucléaires reconnues per le Traité de Non Prolifération Nucléaire à s’entendre sur des mesures de transparence. Je propose l’ouverture de négociations sur un traité interdisant les missiles sol-sol de portée courte et intermédiaire. Je demande à tous d’adhérer et de mettre en œuvre le Code de conduite de la Haye contre la prolifération des missiles balistiques, comme l’a fait la France.... ».

Belangrijk in deze toespraak is dat afstand wordt genomen van het traditionele gaullistisch standpunt voor het principieel behoud van het kernwapenarsenaal als prestige-project. Bovendien worden ook de vectoren ter sprake gebracht met name de ballistische raketten: door ook het bezit van vectoren bespreekbaar te maken, kan de hele regio van Zuid- en Oost-Azië maar ook het Midden-Oosten teruggebracht worden tot een veilig evenwicht. Daarom moeten de nieuwe eisen, die gesteld werden in het kader van de programma’s voor de voorziening van kernenergie tegen horizon 2015 niet onderschat worden. Door de beperkte voorraden aan fossiele brandstoffen en de (te) langzame groei van de beschikbaarheid aan alternatieve energiebronnen, blijft kernenergie de enige mogelijke transitie. Deze energievoorziening kan zoals aangetoond risico’s inhouden voor nieuwe proliferatie, zowel voor staten als niet-staatsactoren. Andere initiatieven werden reeds genomen om verspreiding van aanrijkingstechnologie van nucleaire brandstof voor reactoren te beperken (vb. GNEP). Het probleem is dat ook hier een monopolie zou gecreëerd worden ten gunste van de huidige kernmachten indien enkel de bestaande installaties gebruikt zouden worden voor de productie van splijtstof. Voorstel is om de levering en transfer van kernbrandstof onder toezicht te plaatsen van het IAEA. Hiervoor zullen de transacties van nucleaire brandstof rechtsreeks onder controle van de VN moeten geplaatst worden (eventueel een daarvoor speciaal opgerichte commissie). Het is belangrijk dat de vijf erkende kernmachten (P5) met hun permanente zetel in de VN-

⁸⁹ Bomaanslag op het Marriott-hotel in Islamabad en Taliban-ultimatum om tegen 15 januari 2009 in de Swat provincie alle meisjesscholen te sluiten.

⁹⁰ Volledige toespraak beschikbaar via <http://www.ambafrance-uk.org/Presentation-du-SNLE-Le-Terrible.html>

⁹¹ Te weten de vijf kernmachten met inbegrip van India, Pakistan en Israël.

veiligheidsraad, niet mogen gedreven worden om een monopolie-positie te verwerven voor levering van nucleaire brandstof.

Deze oplossing zal eveneens moeten zorgen voor een billijke bepaling van de prijs van de geproduceerde brandstof evenals alle modaliteiten voor afvalverwerking. Dit betekent dat ook de afvalverwerking of opslag van kernbrandstofafval moet geregeld worden door bijvoorbeeld terugvoer van het afval naar het land van oorsprong te reglementeren. Het kan en mag niet de bedoeling zijn om het kernafval bij de gebruiker te laten en zo een nieuw probleem te creëren m.n. de mogelijkheid van proliferatie van kernafval dat mogelijk weer in handen van niet-staatsactoren zou kunnen belanden via criminele netwerken die er munt zullen uit slaan. Verder moet er controle zijn op het goed gebruik van de brandstof nl. enkel met het oogmerk energie op te wekken. De transparantie zal moeten verzekerd worden door rapportage naar internationale instanties d.w.z. dat alle materiaal geïnventariseerd zal moeten worden en dat gebruikte hoeveelheden zowel kwantitatief als kwalitatief getraceerd moeten kunnen worden. Hiermee zijn alle mogelijke lopende eisen op bezit van vreedzame kernenergie overbodig: de redelijke prijs kan gegarandeerd worden, en het monopolie van de P5 wordt onder toezicht geplaatst.

Controle op bestaande opslag en verloren bronnen moet verder opgedreven worden. Dit zal op zich een enorme uitdaging zijn aangezien tot op heden geen volledige inventaris bestaat van de bestaande opslag aan fissiemateriaal. Smokkel kan in het voorgestelde scenario nog enkel voor wapens; uitvoer moet nog strenger aangepakt worden. Daarom moeten de controles van het internationaal atoomagentschap opgedreven worden. In dit kader kunnen deskundigen, opgeleid bij kandidaat-proliferatoren ook nuttig zijn. Een tekort kan opgevuld worden door deze wetenschappers die anders in de criminaliteit zouden kunnen belanden omwille van een te laag inkomen. Omscholing en inzet in internationale instellingen kan een oplossing bieden. Dat is niet alleen het geval voor kernfysici: chemici kunnen eveneens hun weg vinden bij de OPCW. Biologen en bio-technologen kunnen tewerk gesteld worden bij de wereldgezondheidsorganisatie: hun kennis en kunde kan ingezet worden om endemische ziekten in Afrika te bestrijden, pandemieën te voorzien en in te dijken, vaccins te produceren en te verdelen in een internationale samenwerkingsakkoord.

Men zal meer aandacht moeten schenken aan het probleem “soft proliferatie” en geldstromen die ermee verbonden zijn. Controleorganismen moeten verbanden kunnen leggen tussen witwaspraktijken en de smokkel van illegaal WMD-materiaal. Meer en meer transacties kunnen uitgevoerd worden via het Internet. Het kan niet de bedoeling zijn dat deze mogelijkheden uitgebraat worden door kandidaat-proliferatoren of individuen op zoek naar de technologie van massavernietigingswapens. Nochtans is het tot op heden mogelijk om bijvoorbeeld toegang te verkrijgen tot officiële rapporten (beperkte verspreiding) van het IAEA⁹² of wetenschappelijke documenten⁹³ te downloaden die gebruikt kunnen worden om “vuile bommen” samen te stellen. Hoewel meer en meer controle wordt uitgevoerd op de verspreiding van deze informatie door bijvoorbeeld zelfcensuur in de

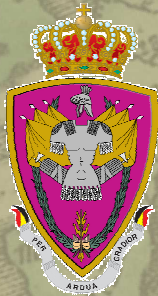
⁹² IAEA documenten betreffende NPT safeguards voor Iran op http://www.isis-online.org/publications/iran/IAEA_Iran_Report_26May2008.pdf (beperkte verspreiding enkel voor officieel gebruik) en <http://www.iaea.org/Publications/Documents/Board/2008/gov2008-4.pdf> (beperkte verspreiding, beschikbaar in februari 2008; vrijgegeven in maart 2008).

⁹³ <http://ann.sagepub.com/cgi/reprint/607/1/133> over de mogelijkheid tot samenstelling van een kernwapen. Zie ook: WILLIAMS, B., «Getting nuclear bomb fuel out of radiopharmaceuticals», in *The Lancet*, Vol.371, March 2008, pp.795-797.

wetenschappelijke wereld, mag dit niet ontaarden in de volledige verlamming van de wetenschappelijke wisselwerking: een moeilijke oefening waarvoor oplossingen zullen moeten gevonden worden. Men moet de gulden middenweg vinden tussen de geheimhouding die noodzakelijk is voor het vrijwaren van gevoelige informatie en anderzijds de wetenschappelijke openheid die steeds gebaseerd is geweest op de uitwisseling van informatie om de controle op en reproduceerbaarheid van experimenten te verzekeren.

Ook op het gebied van nationale wapenwetgeving kunnen nog initiatieven genomen worden om de transparantie te vergroten in verband met de handel van WMD-goederen en goederen voor tweeërlei gebruik: jaarverslagen kunnen ook rekening houden met doorvoer van goederen. Indien dit tot op heden niet mogelijk was, moeten hiervoor de noodzakelijke wettelijke middelen voorzien worden op nationaal en internationaal niveau. Men kan vaststellen dat zelfs in België nog werk is op dat gebied.

Deel 2



Concept
« indirecte bedreiging »
en preventie

2.1. «Indirecte CBRN-dreiging»

Uit de voorgaande dreigingsanalyse is duidelijk dat terroristische activiteiten gevolgen kunnen hebben voor troepen in operaties, maar ook voor eigen bevolking. Gezien de globalisatietrend kunnen ook niet-staatsactoren hieruit hun voordeel halen. In deze context kan en is reeds gebruik gemaakt van CBRN materiaal. BUNN⁹⁴ heeft reeds vermeld dat ook terroristen, mits te kunnen beschikken over fissie-materiaal, in staat zouden zijn om een klein nucleair wapen te laten ontsteken. Chemische, biologische en radiologische agentia behoeven zelfs geen ingewikkelde mechanismen om verspreid te worden. Zelfs indien de toegang tot deze middelen wordt ontzegd, kunnen conventionele springladingen of sabotage op bestaande opslag- of productiecapaciteit dezelfde gevolgen veroorzaken. Deze indirecte CBRN-dreiging omhelst net alle incidenten die voortvloeien uit een aanval op eigen installaties of troepen. Meer bepaald op nationaal grondgebied, omvat het alle scenario's in een CBRN-context die een rechtstreekse bedreiging vormen voor de bevolking, de infrastructuur of de goede werking van de instellingen en diensten. Door de overheid werd een studie besteld bij de universiteit van Luik met betrekking tot verschillende scenario's met nationale gevolgen: de vier meest waarschijnlijke gevallen vielen onder het CBRNE-luik. Hoe de scenario's precies verlopen kon niet achterhaald worden. Men kan echter wel inschatten hoe dergelijke scenario's zullen verlopen. Vermelden we hier enkele mogelijke gevallen:

- Besmetting van grondwater of drinkwatervoorziening met een giftig agens (biologisch of chemisch).
- Besmetting van de voedselketen door bacteriën.
- Detonatie van een springlading die gehecht is aan een tankwagen gevuld met TIM (chloorgas bijvoorbeeld).
- Besproeiing van een CBRN-agens door middel van een vliegtuig tijdens een massabijeenkomst in een festivalweide of een stadion.
- Sabotage of aanval op een site van een kernreactor of een site die radiologisch materiaal of afval stockeert.
- Verspreiding van toxische gassen in een metronetwerk.
- Aanval op het transport van kernafval of kernbrandstof.
- Gebruik van gerecupereerde toxische munitie uit opslagplaatsen.
- Conventionele springlading gecombineerd met toxische stoffen in een overheidsgebouw of openbaar vervoer.

Wat eigen is aan deze scenario's is dat ze zowel op eigen grondgebied als op geprojecteerde troepen kunnen plaatsgrijpen. Dergelijke scenario's moeten ingeoefend worden, zowel op gebied van Commando en Controle (C²) (denkoefeningen), als op het terrein (praktische uitvoering).

Ons land, de hoofdstad in het bijzonder, is rijkelijk bezaaid met nationale en internationale instellingen en deze vormen een ideaal doelwit. Ook de industrie, de

⁹⁴ BUNN, M., WIER, A., Terrorist Nuclear Weapon Construction: How Difficult?, The annals of the American Academy of Political and Social Science, N°607, September 2006, pp.146-147.

energievoorziening, de communicatiemiddelen en toegangswegen kunnen een doelwit worden. Bovendien moeten we rekening houden met de constante evolutie van de dreiging: daar waar op het vlak van de luchtvaart bijvoorbeeld sinds 2001 vooral aandacht werd gevestigd op de veiligheid op vliegtuigen en hun bemanning, moet men tot de vaststelling komen dat op het gebied van aankomst- en vertrekhalles van vliegvelden weinig veranderd is op het gebied van beveiliging. Dit maakt deze vaak overbevolkte zones ideale doelwitten voor terroristische activiteiten die ook in dat geval de volledige luchthaveninfrastructuur zou lam leggen. Teneinde een aangepaste omschrijving te hebben van deze kritische infrastructuur, werd door het crisiscentrum van de regering een lijst opgesteld van kritieke, vitale en gevoelige punten die bijzonder aandacht vereisen. Deze lijst wordt onder de vorm van een databank bijgehouden onder de naam CRIVISEN (CRItiques, VItaux, SENSibles). Deze databank werd opgesteld op basis van twee documenten:

- De beschrijving van vitale en gevoelige punten zoals vastgelegd in het protocolakkoord van 1997 tussen de ministers van Binnenlandse Zaken en Landsverdediging.
- Een invulling aan de definitie “kritieke infrastructuur” die voortvloeit uit de wet betreffende de analyse van de dreiging⁹⁵. Hierin worden vitale, gevoelige en gevaarlijke punten enkel beschouwd als een onderdeel van kritieke punten.

Na de gebeurtenissen van 11 september 2001, kreeg het begrip ‘kritieke punten’ een nieuwe invulling m.n. “Personen (politieke of morele autoriteiten, al dan niet Belgisch), gemeenschappen, instellingen, gebouwen, installaties, plaatsen en goederen die voorwerp kunnen uitmaken van een reële of potentiële dreiging. Deze dreiging kan zowel van politieke of louter criminele aard zijn”⁹⁶. Deze benadering is duidelijk niet in overeenstemming met de voorstellen tot definitie van kritieke infrastructuur zoals ze werden weergegeven in het Groenboek van de Europese Commissie van 2005⁹⁷ en het daaropvolgende voorstel tot richtlijn van 12 december 2006⁹⁸. Kol SBH DE KIMPE heeft een nieuw voorstel tot definitie vastgelegd als volgt⁹⁹:

- “Gevoelige punten zijn personen, gemeenschappen, instellingen, gebouwen, installaties, plaatsen of goederen die omwille van hun aard, ligging of functie, potentieel het voorwerp kunnen uitmaken van een beschermingsactie omwille van:
 - a. een terroristische of criminele dreiging of aanval
 - b. een catastrofe van natuurlijke en/of menselijke oorsprong
- Nationale infrastructuur is het geheel van structuren, organisaties en netwerken van ons industrieel potentieel, onze instellingen, onze productie-, distributie- en dienstencapaciteit die moeten instaan voor een betrouwbare stroom van goederen en diensten, een harmonieuze werking van onze instellingen, het welzijn van onze burgers en onze maatschappij.
- Vitale infrastructuur vormen die onderdelen van de nationale infrastructuur waarvan de vernietiging of langdurige buitendienststelling catastrofale gevolgen heeft voor:
 - a. het socio-economische leven van de natie
 - b. de staatsrechtelijke functionering van de Staat, inclusief Defensie

⁹⁵ Art. 2 van het K.B. van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging.

⁹⁶ Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Activiteitenverslag 2005, 2006, p.102.

⁹⁷ COM(2005)

⁹⁸ COM(2006) 787 final.

⁹⁹ Kol SBH DE KIMPE, J., op.cit., p. 17.

- c. de gezondheid en de veiligheid van een groot deel van de bevolking en het milieu.”

Het is hier niet de bedoeling om opnieuw een invulling te geven aan dit begrip. Deze analyse werd door Kol SBH DE KIMPE reeds uitgevoerd: in zijn werk heeft hij de veelvuldigheid aan discrepanties tussen bestaande definities aangetoond¹⁰⁰. Het gevolg van deze discrepantie is wel dat de bestaande CRIVISEN-lijst (13650 punten in een access databank) niet in de huidige vorm uitbaatbaar is. Niet alle gelijste punten zijn relevant in het kader van verdediging van kritische infrastructuur: de lijst is hiervoor te lang. Bovendien bevat ze ook fysieke personen die een bijzondere bescherming of aandacht vereisen. De rol van hun bescherming is niet vergelijkbaar met de bescherming van kritische infrastructuur. Seveso en aanverwante bedrijven (opslag), daarentegen, worden niet systematisch opgenomen omwille van de moeilijkheid informatie te verkrijgen van privébedrijven. Het is duidelijk dat deze lijst volledig herzien zal moeten worden om te voldoen aan de EPCIP-criteria (European Program for Critical Infrastructure Protection). Dit initiatief werd ingevuld door de uitvaardiging van een nieuwe Europese richtlijn 9403/08 in juni 2008. Onder kritische infrastructuur wordt volgens deze richtlijn verstaan “de voorzieningen en systemen of delen daarvan op het grondgebied van de lidstaten die van essentieel belang zijn voor het behoud van de vitale maatschappelijke functies, de gezondheid, de beveiliging, de economische welvaart of het maatschappelijk welzijn, waarvan de versterking of vernietiging in een lidstaat aanzienlijke gevolgen zou hebben doordat die functies ontregeld zouden raken”¹⁰¹.

Belangrijk om melden is dat het “ICT” gedeelte dat voorkwam in het voorstel tot richtlijn niet meer opgenomen wordt in deze nieuwe richtlijn. Nochtans zijn de financiële sector, telecom-bedrijven (GSM netwerken), luchtvaartmaatschappijen of bijvoorbeeld kerncentrales vragende partij om ICT specifiek te laten opnemen in de definitie. Dat zou ook de beveiliging ervan mogelijk maken op Europees niveau. Dit zou ook toelaten om risicobeheer op een Europees niveau te standaardiseren. Actueel staan vermelde systemen bloot aan zogenaamde “BOTNET”-aanvallen¹⁰² welke zichtbaar zijn. Nog meer verontrustend zijn de ongemerkte intrusies die bedoeld zijn om vitale informatie te stelen.

Hierbij moet wel de bemerking gemaakt worden dat in bijlage van het Groenboek van de Europese Commissie (zie bijlage 5) de definitie van Critical Infrastructure (CI) wel het aspect cybernetwerken omvatte. Op nationaal vlak werd in deze materie reeds een initiatief genomen door de opstelling van een witboek¹⁰³ door het overlegplatform voor de informatieveiligheid¹⁰⁴. Ook in dit document wordt gesteld dat¹⁰⁵ “men ...een inventaris zou moeten maken van kritieke informatie-infrastructuren van het land (voetnoot: in nauwe samenwerking met het Crisiscentrum-zie databank Crivisen¹⁰⁶)... wat een passende reglementering vereist.” De gebeurtenissen in Estland in mei 2007 hebben het belang van dergelijke initiatieven aangetoond. Federal Computer Crime Unit (FCCU) heeft in het kader van het Belgian Network for Information Security (BENIS), het initiatief genomen om:

¹⁰⁰ Kol SBH DE KIMPE, J., op.cit., p.15 e.v.

¹⁰¹ Art.2 van de richtlijn inzake de inventarisatie van de Europese kritieke infrastructuur, Juni 2008.

¹⁰² Acroniem gegeven door het Federaal Computer Crime Network voor roBOT/NETwork-aanvallen op ICT systemen.

¹⁰³ White paper opgesteld door het overlegplatform voor de informatieveiligheid, Juli 2007.

¹⁰⁴ Overlegplatform opgericht door de Ministerraad van 30 september 2005.

¹⁰⁵ White paper, op.cit., p.9.

¹⁰⁶ Gezien de voorafgaande analyse kan men stellen dat samenwerking met de crisiscel aangewezen is maar de verwijzing naar CRIVISEN is ongelukkig gekozen.

- Een werkgroep op te richten voor Network Information Security (o.m. classificatie, homologatie en accreditatie van informatie).
- Een werkgroep op te richten naar ICT bescherming van kritische infrastructuur.

Dit heeft als einddoel een nationaal Computer Security Information Response Team (CSIRT) op te richten naar Amerikaans voorbeeld. Helaas is in die zin nog geen vooruitgang geboekt om tot uitvoering over te kunnen gaan.

De risicoanalyse (analyse van de bedreiging en analyse van impact/gevoeligheid van infrastructuur) op nationaal grondgebied kan, in de actuele stand van zaken, niet volledig passen in een internationaal kader omwille van aangehaalde verschillen i.v.m. definities: hierdoor is een impactanalyse niet in overeenstemming met die van onze buurlanden. Wat de dreigingsanalyse betreft, wordt in ons land beroep gedaan op het Coördinatieorgaan voor de dreigingsanalyse (OCAD)¹⁰⁷. Volgens de wet dient OCAD zowel strategische als punctuele analyses uit te voeren op het vlak van terrorisme en extremisme. In het kader van een dreigingsanalyse stelt men zich de vraag of er een vijand bestaat die de capaciteit en de wil bezit om actief te worden op nationaal grondgebied. Naargelang de resultaten van de analyses wordt het dreigingsniveau bepaald van laag (niveau 1) tot zeer ernstig (niveau 4). Voor een meer gedetailleerde bespreking van de taken van dit organisme wordt verwezen naar het K.B. van 28 november 2006¹⁰⁸.

Daar waar CRIVISEN een initiatief was van het crisiscentrum van de regering (CGCCR¹⁰⁹), moet OCAD (onder meer) rapporteren aan het CGCCR. CGCCR werd immers in het leven geroepen om nationale nood- en interventieplanning te coördineren. In dit orgaan zouden dus zowel de bedreigingsanalyse als de kwetsbaarheidsanalyse moeten kunnen samenvloeien tot een risicoanalyse. In 2004 is hiervoor een studie uitbesteed aan de Universiteit van Luik onder de naam Federal Risk Inventory, Survey and Knowledge building (FRISK). Gezien de snelle evolutie van politieke, sociale en economische omstandigheden zou een dergelijke risicoanalyse op regelmatige basis moeten geactualiseerd worden om efficiënte maatregelen te kunnen aanwenden. De te volgen methode hiervoor werd reeds gedefinieerd in de FRISK-studie. De conclusie van het rapport vermeldt in dit verband: “Les méthodes et outils développés lors de cette recherche doivent être mis à l’épreuve du temps et être utilisés dans un contexte opérationnel pour aider tant à la définition des objectifs qu’à la rédaction des plans (ils ont été conçus comme tels). Les résultats ne doivent pas être considérés comme étant un aboutissement, mais bien comme étant les fondations sur lesquelles le CGCCR peut construire une analyse de risque fiable...De même, la liste de risque utilisée ici doit être mis à jour, que ce soit parce que certains plans ont été établis, parce que de nouvelles menaces font surface, ou bien encore parce que les compétences changent.”¹¹⁰

In de praktijk blijkt echter dat actualisatie van deze studie niet werd uitgevoerd.¹¹¹ Uit het eindrapport van 2004 werden de 20 risico’s met hoogste

¹⁰⁷ Opericht door de wet van 10 juli 2006 betreffende de analyse van de dreiging, bekrachtigd door het KB van 28 november 2006.

¹⁰⁸ Art. 11 van het K.B. van 28 november 2006 tot uitvoering van de wet van 10 juli 2006 betreffende de analyse van de dreiging. Voor een commentaar omtrent de werking van OCAD wordt verwezen naar DE KIMPE, J., Bescherming van vitale infrastructuur. Welke rol voor Defensie? Kabinet Defensie, 2007, pp.35-37.

¹⁰⁹ Centre Gouvernemental de Crise/Crisiscentrum van de regering

¹¹⁰ CORNELIS B. et al., FRISK, rapport final révision 1, Université de Liège, novembre 2004, p.54

¹¹¹ Onderhoud Col COLLINS d.d. 29 Jul 2008.

prioriteit gedistilleerd¹¹². Vandaag wordt nog steeds dezelfde top-20 gehanteerd (zowel wat noodplanning als ordehandhaving betreft) hoewel een nieuwe analyse misschien andere prioriteiten aan het daglicht zou brengen¹¹³. Voorstel is om deze taak van actualisatie te laten uitvoeren door een “permanente cel risicoanalyse” in de schoot van het CGCCR. Dit betekent dat uitgaande van de dreigingsanalyse (verantwoordelijkheid van OCAD) de gevoeligheidsanalyse en het daaruit voortvloeiende risico op kritische infrastructuur moeten geëvalueerd worden. Dat betekent dat de dreigingsanalyse zelf ook gericht zou moeten worden op kritische infrastructuur in een geactualiseerde en bruikbare databank die geraadpleegd kan worden door alle diensten die betrokken zijn in deze risico-evaluatie. Aan elk van deze kritische punten kunnen vooraf maatregelen en middelen voorzien worden om de bescherming te garanderen. De analyse zal dan toelaten de nodige maatregelen en middelen te selecteren die aan de aanwezige dreiging het hoofd kunnen bieden. Hier kan men dieper ingaan op de organisatie van CGCCR en de noodplanning in het algemeen.

2.1.1. NOODPLANNING EN HET CGCCR

De noodplanning in België wordt wettelijk onderbouwd door het KB van 31 januari 2003 (Koninklijk besluit tot vaststelling van het noodplan voor crisisgebeurtenissen en –situaties die een coördinatie of een beheer op nationaal niveau vereisen), het KB van 16 februari 06 (Koninklijk besluit betreffende nood- en interventieplannen) en de Ministeriële omzendbrief van 26 oktober 2006 (Ministeriële omzendbrief NPU-1 betreffende de nood- en interventieplannen). De noodplanning kan in verschillende fases geactiveerd worden:

- Gemeentelijke fase: beleidsniveau burgemeester. De beleidscoördinatie gebeurt in het gemeentelijk crisiscentrum (CC).
- Provinciale fase: beleidsniveau gouverneur. De beleidscoördinatie gebeurt in het provinciaal CC.
- Nationale fase: beleidsniveau Minister Binnenlandse Zaken. De beleidscoördinatie gebeurt in de CGCCR.

Activering en overgang van de ene naar de andere fase worden expliciet aangegeven in vermelde KB's en omzendbrief.

Door de aard van het CBRNE-incident zal de aanpak multidisciplinair moeten gebeuren. De verschillende disciplines die aan bod komen worden in de Ministeriële omzendbrief onder titel IV nog even op een rijtje gezet:

- Discipline 1: hulpverleningsoperaties uitgevoerd door brandweer bijgestaan door eenheden van Civiele Veiligheid. De leiding van de hulpverlening berust bij de directeur brandweer (Dir-BW).
- Discipline 2: medische, sanitaire en psychosociale hulp. De operationele leiding berust bij de directeur medische hulpverlening (Dir-Med). Deze, als ook de optredende medische diensten blijven onderworpen aan het gezag van de federale

¹¹² Uit de klemtonen van de activiteitenrapporten CGCCR (zie verder) kan men als prioriteitrisico's o.m. vinden: gebruik van CBRN agentia, problemen met kerncentrales, problemen met energievoorziening, incidenten met Seveso-bedrijven, ontploffingen/uitwasemingen met toxisch industrieel materiaal (TIM), overstromingen, pandemie.

¹¹³ Dat zou ook de reden kunnen zijn waarom beveiliging van ICT-netwerken nog géén onderwerp uitmaakt van een specifiek nationaal plan of enige andere prioriteit geniet.

gezondheidsinspecteur. Opvang en afvoer van gekwetsten moet rekening houden met het feit dat de slachtoffers mogelijk besmetting hebben opgelopen. Dit zal gevolgen hebben voor de opstelling van de decontaminatieketen, de behandeling van de slachtoffers en de bescherming van de hulpverleners.

- Discipline 3: politie van de plaats van de noodsituatie. Vermelden we hier de taak om de organisatorische perimeters af te bakenen en te beveiligen. De operationele leiding van deze discipline berust bij de directeur politie (Dir-Pol). In hoofde van de overleden slachtoffers vermeldt de omzendbrief dat "...de identificatie...is een opdracht van de bestuurlijke politie. Dit zal zo nodig gebeuren met inschakeling van het Disaster Victim Identification (DVI)-team van de federale politie en andere gespecialiseerde diensten." Belangrijk in dit verband is dat vermelde slachtoffers gecontamineerd zullen zijn en dat identificatie dus eveneens onderworpen zal zijn aan beschermingsmaatregelen voor het aangeduide personeel.
- Discipline 4: logistieke steun. De opdrachten in dit kader worden uitgevoerd door de operationele eenheden van de Civiele Bescherming. Bij uitputting van de middelen kan de bijstand van het leger overwogen worden. De operationele leiding van deze discipline berust bij de directeur logistiek (Dir-Log): dit is de aanwezige met de hoogste graad van de operationele eenheid van de Civiele Bescherming.
- Discipline 5: informatie. Verstrekking van de informatie aan de bevolking gebeurt door de burgemeester (tijdens de gemeentelijke fase van het noodplan), de gouverneur (tijdens de provinciale fase) of de bevoegde minister (tijdens nationale noodplanning).

Een exhaustieve lijst van alle taken en verantwoordelijkheden van elke discipline is terug te vinden in de omzendbrief. Het is duidelijk dat de samenwerking van alle disciplines gecoördineerd zal moeten worden. Deze operationele coördinatie gebeurt in de commandopost operaties (CP-Ops). Hierin vinden we zowel de Dir-BW, Dir-Pol, Dir-Med, Dir-Log, als Dir-Info (of zijn vertegenwoordiger) terug. De leiding van de CP-Ops (Dir CP-Ops) wordt waargenomen door de aanwezige brandweerofficier met de hoogste graad. In de verdere uiteenzetting zal Dir CP-Ops vervangen worden door de term « Incident Commander » (IC).

Krachtens het KB van 31 januari 2003 wordt de nationale fase van het noodplan geactiveerd door evolutieve of plotse overgang van provinciaal naar de hogere fase mits aan volgende voorwaarden wordt voldaan:

- Twee of meerdere provincies of het nationale grondgebied zijn betrokken.
- De aan te wenden middelen overschrijden de middelen waarover een provinciegouverneur beschikt.
- Bedreiging van of aanwezigheid van talrijke slachtoffers (gewonden of doden).
- Plots voorkomen van of dreigend gevaar voor grote invloeden op de omgeving of de voedselketen.
- Inbreuken of dreigend gevaar voor inbreuken op de vitale belangen van de natie of op de essentiële behoeften van de bevolking.
- Noodzaak tot inwerkingstelling en coördinatie van verschillende ministeriële departementen of federale instellingen.
- Noodzaak tot een algemene informatie van de bevolking.

Het is duidelijk dat voor de inzet van Defensie, aan de voorlaatste voorwaarde voldaan is en bijgevolg de nationale fase van het noodplan geactiveerd zal zijn in het kader van CBRN incidenten. Hierdoor wordt binnen CGCCR drie organen geactiveerd (zie schema 1):

- De beheerscel vormt het centrale sluitstuk van de beleidscoördinatie van de nationale noodplanning. Ze is samengesteld door de ministers van wie de

departementen betrokken zijn in het incident. Het voorzitterschap wordt waargenomen door de Minister van Binnenlandse Zaken.

- De evaluatiecel is samengesteld uit deskundigen ter zake. Deze zullen in permanente wisselwerking treden met de beheerscel en de nodige input geven om tot concrete besluitvorming te komen. In de praktijk blijkt dat de evaluatiecel fysisch samen met de beheerscel vergadert. De beslissingen worden via de crisiscel van de provincie doorgegeven aan de Dir-CP Ops voor praktische uitvoering. Omgekeerd zal Dir CP-Ops (IC) alle relevante informatie doorspelen naar het crisiscentrum van de provincie (CC Prov), waar de gouverneur in permanent contact staat met de beheerscel. De coördinatie van de hulpverlening gebeurt eveneens op niveau van CC Prov.
- De informatiecel (communicatiecel) zal de genomen beslissingen toelichten aan de bevolking. Via de media zal deze cel alle relevante informatie verspreiden om de bevolking op de hoogte te houden van de evolutie van de toestand en eventuele vragen te beantwoorden.

Wanneer deze cellen niet geactiveerd zijn, staat CGCCR zelf in voor het opstellen en coördineren van noodplannen overeenkomstig het KB van 18 april 1988. Op vraag kan ook een economische cel geactiveerd worden die de impact van lopende incidenten zal evalueren op de nationale economie.

Vermelden we hier nog dat voor een kernramp een specifieke procedure wordt gevolgd die niets te maken heeft met het Nationaal Noodplan CBRN. Specifiek voor dit geval werd het K.B. van 17 oktober 2003 opgesteld met betrekking tot vaststelling van het nucleair en radiologisch noodplan voor het Belgisch grondgebied. Dit KB heeft betrekking op nucleaire installaties of kerncentrales¹¹⁴.

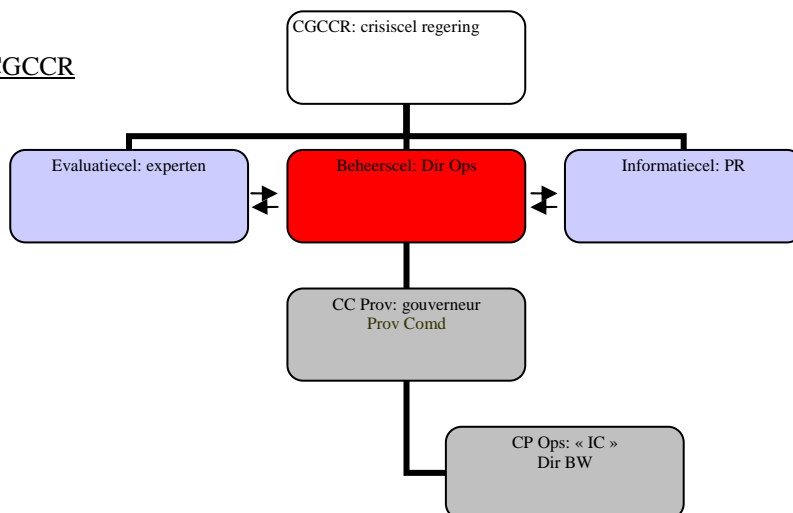
Wat chemische noodplanning betreft dient nog vermeld dat specifiek voor de “beheersing van de gevaren van zware ongevallen waarbij gevaarlijke stoffen zijn betrokken” de Seveso-richtlijn 2003/105/EG van het Europees Parlement van kracht is. Nationaal werd deze richtlijn vertaald naar een samenwerkingsakkoord tussen de federale staat en de gewesten. Ook in deze gevallen zal de structuur van het CGCCR aangesproken worden omwille van de omvang van de problematiek. In het geval van de Kernramp zal voornamelijk het FANC¹¹⁵ de internationale contacten beheren ten einde buurlanden en Europese instanties te informeren eventueel door middel van het ECURIE-netwerk.

Zowel het nucleair/radiologisch als het Seveso-incident worden geregeld door een afzonderlijke wetgeving inzake nood-en interventieplanning. Ook de praktische aanpak is fundamenteel verschillend van de Noodplanning CBRN Nationaal. Omwille van de inzet van Defensie op nationaal grondgebied en de praktische inzet en coördinatie van de vereiste hulpverlening, is een specifieke benadering vereist voor de beheersing van een CBRN-incident.

¹¹⁴ Doel, Tihange, Chooz, Borssele, Mol, Dessel, Fleurus.

¹¹⁵ Federaal Agentschap voor Nucleaire Controle.

Schema 1: CGCCR



Men kan echter betreuren dat, ondanks de gebeurtenissen in de VS, het VK, Japan en Madrid er nog steeds geen ondertekend noodplan CBRN bestaat. In het Verenigd Koninkrijk bestaat er sinds 2004 reeds een uitgebreid werkplan om Defensie en civiele instanties gecoördineerd te laten samenwerken bij nationale rampenplanning¹¹⁶. Bij ons is dat nog niet het geval. Omwille van het wegblijven van een definitieve versie of goedkeuring van dit plan, is het ook niet mogelijk om gedetailleerd informatie hieromtrent te verkrijgen. Het is wel de bedoeling dat alle FODs ten dienste zouden staan van de gemeenschap om een lopende crisis operationeel en gecoördineerd aan te pakken. Bovendien zullen in CBRN-omstandigheden zeker middelen van Defensie ingezet moeten worden. Vragen gericht aan CGCCR in dit verband werden niet beantwoord. Wel werd voor officiële standpunten verwezen naar jaarverslagen. Indien men die erop naslaat kan men merken dat het activiteitenrapport 2005¹¹⁷ volgend informatie vermeldt: “...CBNR-terrorisme (sic) is een nieuwe tendens binnen het internationaal terrorisme. Er werden in België meerdere initiatieven genomen om dit fenomeen te bestrijden. Zo kunnen we de gezamenlijke omzendbrief van de Minister van Justitie en van het College van Procureurs-Generaal vernoemen en ook de uitwerking van de procedure “verdachte pakketten in het kader van de CBNR-dreiging”. Die procedure werd recent herzien en geactualiseerd. Dit gebeurde in samenwerking met de Federale Politie, het Federaal Parket, de Civiele Veiligheid en het FOD Volksgezondheid.”

Merken we op dat in dit domein nog geen vermelding wordt gemaakt van Defensie. Men zou kunnen tegenwerpen dat de procedure verdachte verzendingen geen tussenkomst van Defensie vereist. In de praktijk rijst hier echter een probleem: FOD Volksgezondheid noch het NICC¹¹⁸ aanvaarden brieven die mogelijk nog springstof zouden kunnen bevatten. De Dienst voor Ontmanteling en Vernietiging van Ontploffingstuigen van Defensie (DOVO) zou echter in het geval van verdachte brieven enkel kunnen nagaan of er al dan niet een ontstekingsmechanisme aanwezig

¹¹⁶ Operations in the UK: The Defence Contribution to Resilience. Interim Joint Doctrine Publication 02. Ministry of Defence, December 2004.

¹¹⁷ Algemene Directie Crisiscentrum, Activiteitenrapport 2005. Federale Overheidsdienst Binnenlandse Zaken, 2006, p.12.

¹¹⁸ Nationaal Instituut voor Criminologie en Criminalistiek.

is. Dit neemt niet weg dat de inhoud nog steeds van pyrotechnische aard kan zijn of zelfs springstoffen kan bevatten die ontsteken door frictie. Hiervoor kan DOVO géén garantie geven en is dus een geïntegreerde aanpak vereist door samenwerking van verschillende diensten. Een overkoepelend organisme is noodzakelijk om de eerste screening van de mogelijke gevaren uit te voeren. Dit kan gebeuren in daartoe uitgeruste installaties van Defensie.

Het rapport gaat verder met volgende stelling¹¹⁹: “In 2005 werd ons land opnieuw geconfronteerd met het probleem van verdachte pakketten...De enveloppen werden geanalyseerd door Coda-Cerva, het NICC en door het studiecentrum voor Kernenergie (SCK-CEN) voor respectievelijk de biologische, toxische en radiologische agentia. Testen op chemische of biologische agentia bleken negatief. De radiologische test was daarentegen wel positief...”

Ook hier blijkt dat géén rekening werd gehouden met mogelijk explosieve of brandbare inhoud. Nochtans werden dergelijke incidenten reeds waargenomen (o.a. in “brandbrieven”¹²⁰). Bovendien spreekt men van chemische analyse (verondersteld naar chemische oorlogsagentia) terwijl in het rapport geen sprake is van het enige door het OPCW erkende laboratorium in België met name het laboratorium chemische analyse van DLD (Peutie). Het is bovendien duidelijk dat de brieven een sequentiële aanpak hebben gezien en van het ene laboratorium naar het andere werden verstuurd. Dit is zeker niet in overeenstemming met de vereisten van een geïntegreerde aanpak van CBRN- risico’s. In extremis zou dit zelfs gevolgen kunnen hebben voor besmetting van bijvoorbeeld het laboratorium van het NICC met biologische of chemische agentia. Het activiteitenrapport 2006¹²¹ vermeldt in dit verband: “...de uitwerking van de procedure “verdachte pakjes in het kader van de CBRN-dreiging”. Om de gevolgen van een CBRN-aanslag gecoördineerd aan te pakken werkt de Algemene Directie Crisiscentrum een aangepast noodplan uit in samenwerking met haar partners. Vooraf werd met Frankrijk samengewerkt om na te gaan hoe de Franse noodplanning op dit vlak in elkaar zit...”

Het gaat blijkbaar in dit geval eveneens (zie activiteitenrapport 2005) om verdachte pakketten (niet uitsluitend anthrax-brieven), met als gevolg dat twee procedures in de rapportering door elkaar worden gehaald: enerzijds het Nationaal Noodplan CBRN, anderzijds de procedure verdachte verzendingen (m.n. poederbrieven). Deze aanpak komt opnieuw aan het licht op de Internet-pagina¹²² van het crisiscentrum door de vermelding: “Wanneer een verdacht pakket of omslag wordt aangetroffen, treedt een procedure in werking. Die procedure bepaalt wie de vaststellingen doet, wie het pakket komt ophalen, welk labo het onderzoek voert, enzovoort. Daarbij wordt ook een dreigingsevaluatie uitgevoerd.”

Met deze dreigingsevaluatie doelt men dan¹²³:

- Stap 1: Inlichtingendiensten maken een dreigingsanalyse.
- Stap 2: Op basis van de analyse worden veiligheidsmaatregelen genomen of bijgestuurd.

¹¹⁹ Algemene Directie Crisiscentrum, op.cit., p.58.

¹²⁰ Als dusdanig vermeld op de site van CGCCR zelf:
http://crisis.ibz.be:cases/verdachte_omslagen.php

¹²¹ Algemene Directie Crisiscentrum, Activiteitenrapport 2006. Federale Overheidsdienst Binnenlandse Zaken, 2007, p.21.

¹²² http://crisis.ibz.be:cases/verdachte_omslagen.php

¹²³ <http://crisis.ibz.be/evaluatie>

- Stap 3: De betrokken instanties worden op de hoogte gebracht van de maatregelen.
- Stap 4: De maatregelen worden uitgevoerd.

Het is duidelijk dat een dreigingsanalyse op zich niet kan leiden tot het nemen van maatregelen. Vooraleer er maatregelen met kennis van zaken kunnen genomen worden, moet een risicoanalyse uitgewerkt worden. Zoals eerder vermeld, kan die pas voltooid worden door de samensmelting van de resultaten die voortvloeien van dreigingsanalyse enerzijds en de impactanalyse anderzijds.

Vermelden we hier nog dat in het kader van pakketten, DOVO steeds ter plaatse zal geroepen worden om na te gaan of er mogelijk springstoffen of ontstekingsmechanismen aanwezig zijn. Om deze mechanismen onschadelijk te maken, wordt gebruik gemaakt van de disruptor i.e. een mechanisme dat water onder druk door het pakket schiet. In geval van CBRN dreiging is dit een actie die te vermijden is. Alleen zal men in eerste instantie niet altijd op de hoogte zijn over de mogelijke CBRN-inhoud. Het is voor de hand liggend dat zonder noodplan hieromtrent er geen geïntegreerde en gestandaardiseerde aanpak is: verdachte pakketten vallen in deze categorie niet sequentieel van het ene laboratorium naar het andere overgedragen te worden ter identificatie van een agens. Omwille van de mogelijkheid van de aanwezigheid van alle risico's in een CBRN incident, moeten mensen ingezet worden die, na een risicoanalyse, op een veilige manier (voor bevolking en eigen personeel) de (gedesactiveerde) substanties naar de geschikte laboratoria kunnen vervoeren. Dit kan niet uitgevoerd worden door één enkele dienst. Zoals uit het gesprek met Maj FEROOZ (ACOS O&T/Div D&R)¹²⁴ is gebleken, is de adequate aanpak van CBRNE incidenten (zowel nationaal als geprojecteerd) onderworpen aan volgende vereisten:

- Risico-evaluatie en risicobeheer (Risk Management Monitoring).
- Beveiliging voor personeel en omgeving; veiligheidsperimeters (Protection for Pers & Env, safety and security perimeters).
- Het ontwapenen van explosieven en beveiligen van CBRN materiaal (Render safe & disposal of explosive, CBRN, Toxics).
- Inperking van besmetting en decontaminatie (Hazard Management).
- Detectie en staalname (Detection & sampling).
- Sporenonderzoek (Identification forensics).

Al deze elementen moeten ter beschikking zijn van de “incident commander” m.n. de persoon die ter plaatse de acties coördineert. Het ontbreken of wegvallen van één van deze elementen, brengt de operaties ernstig in gevaar. Men dient nog te vermelden dat de “incident commander” (IC) niet dezelfde zal zijn op nationaal grondgebied als in het geval van geprojecteerde troepen: tijdens operaties is het mogelijk dat deze functie door een militair zal uitgeoefend worden. In internationaal kader (NRF-Athene 2004), is een dergelijke inzet reeds gebeurd. Voor operaties in het kader van steun aan de Natie, kan Defensie enkel optreden als ondersteunend element d.w.z. dat haar diensten aangeboden worden, maar dat de leiding van de operaties eventueel door een brandweercommandant of een geneesheer zal gebeuren. De operationele controle van de ingezette militairen blijft in ieder geval onder militair commando (Prov Comd via COps), maar de leiding zal bij de IC liggen en de beleidsverantwoordelijkheid bij de CGCCR.

Hier dringt zich een afzonderlijke toelichting op van de essentiële vereisten voor aanpak van een CBRN(E)-incident.

¹²⁴ Interview d.d. 22 Apr 2008.

2.1.2. RISICO-EVALUATIE EN RISICOBEEHER (RISK MANAGEMENT MONITORING)

Vooraf dient men hier rekening te houden met het feit dat met betrekking tot deze problematiek een studie lopende is welke ongetwijfeld een nuttig werkdocument zal produceren om op een gestandaardiseerde manier aan risicoanalyse en risicobeheersing te doen. Specifiek in de problematiek die ons aanbelangt, vermeldt de opzet van de studie¹²⁵: "...Teams will provide technical advice to the Incident Commander within their own respective domain of expertise (different safety distances, protection postures, location of the command post...). The IC is then in charge to manage the whole spectrum of possible choices, asses the risks to be taken and deconflict contrasting advices and data."

Wat in afwachting van de resultaten van vermelde studie kan aangebracht worden is dat efficiënt crisisbeheer volgens Kol SBH DE KIMPE¹²⁶ aan volgende vereisten moet voldoen:

- Een heldere rolverdeling en rolvastheid
- Eenheid van doctrine (complementariteit in de uitvoering)
- Op elkaar afgestelde werkwijzen
- Een uniform informatienetwerk

Wat de rolverdeling en de rolvastheid betreft moet men verwijzen naar de voorlopige versie van het Noodplan CBRN waarin de taken van alle actoren beschreven staan. Hoewel alle taken opgesomd zijn en de taakverdeling uitgevoerd is, is het nog niet duidelijk wie wanneer zal optreden (en wie aangeduid zal worden als IC). Naar de eenheid van doctrine (complementariteit in uitvoering) wordt grondig gewerkt door het uitwerken van een militaire doctrine voor "Homeland Operations" enerzijds en Tactische Operationele Instructies anderzijds. Dit zal het militair kader omschrijven en de militaire middelen beschrijven die aangeboden kunnen worden als steun aan de Natie. Deze documenten zullen echter moeten passen in het Nationaal Noodplan CBRN en het interministerieel protocolakkoord, welke meer moeten inhouden dan een opsomming der middelen en verantwoordelijkheden: het Nationaal Noodplan moet concrete en ondubbelzinnige invulling geven van de verwachtingen van iedere actor op het terrein en in de beslissingsketen.

Om over op elkaar afgestelde werkwijzen te beschikken moeten er niet alleen plannen bestaan maar moeten die ook ingeoefend worden. Wat de oefeningen betreft kan men zich nog volgende bedenking maken: zoals reeds vermeld, werden inter-FOD oefeningen in samenwerking met Defensie enkel als C² oefening uitgevoerd d.w.z. als denkoefening met eventueel gebruik van communicatiemiddelen en inbreng van de scenarioschrijvers. Nooit werden er op nationaal niveau met alle betrokken partners daadwerkelijk oefeningen op het terrein georganiseerd in het kader van CBRN noodplanning. In 2003 werden nochtans drie "table-top" oefeningen georganiseerd (respectievelijk op 27-28 mei, 9-10 september en 20-21 oktober). Het activiteitenverslag van dat jaar vermeldt¹²⁷: "Uit de drie NBCR-oefeningen kwamen meerdere onvolmaaktheden aan het licht en op basis daarvan werden verscheidene

¹²⁵ Draft outline description (07 Nov 2007) FINABEL G28R: CBRN EOD Risk Management tool for the Incident Commander within an EU BG operation.

¹²⁶ Kol SBH DE KIMPE, op.cit, p.30.

¹²⁷ Algemene Directie Crisiscentrum, Activiteitenrapport 2003. Federale Overheidsdienst Binnenlandse Zaken, 10 juli 2004, p. 44.

aanbevelingen gedaan om de verschillende interveniërende diensten beter voor te bereiden op zulke gebeurtenissen...Het werd snel duidelijk dat er geen specifiek nationaal plan terrorisme opgesteld moet worden. De bestaande noodplanning volstaat indien ze met een specifiek onderdeel terrorisme wordt aangevuld.”

De beleidsnota van de Minister van Binnenlandse zaken vult trouwens in dit verband aan dat¹²⁸: “...de organisatie van oefeningen zal meer vanuit beleidsondersteunend opzicht benaderd worden.”

Nochtans vindt men één jaar later in het activiteitenrapport¹²⁹ volgende terechte vermelding over oefeningen in het kader van noodplanning: “In het kader van de noodplanning en het crisisbeheer is het houden van oefeningen een belangrijk aspect. Immers, bij een reëel incident krijgen we slechts één kans....Via oefeningen kunnen we onze eigen werking testen, de procedures evalueren en knelpunten detecteren. Oefenen mag dus helemaal geen bijkomstigheid zijn....Het is het ultieme middel om de efficiëntie van onze samenwerking te evalueren.”

Als dat het geval is voor denkoefeningen en scenario's, dan is dit zeker het geval op het terrein waar nog tal van praktische hinderpalen te voorschijn zullen komen om een efficiënte inter-FOD samenwerking te realiseren. Illustratie hiervan vinden we terug in de accidentele uitstoot van radioactief jodium uit de installatie van IRE Fleurus (weekeinde van 23-24 Aug 2008): ondanks een duidelijk noodplan voor kernrampen en regelmatig ingeoeffende scenario's hebben we moeten vaststellen dat de activering van het CGCCR en de verspreiding van maatregelen via de media dagen op zich heeft laten wachten. Wat moet men verwachten van een incident dat nog niet werd ingeoeffend op het terrein? Vier jaar na de beleidsnota van 2004 lezen we in de beleidsnota van 2008¹³⁰: “Het Crisiscentrum werkt verder aan het opstellen van nationale noodplannen over prioritaire¹³¹ risico's, zoals...het plan CBRN-risico's...”.

Dit betekent dat we na meer dan vijf jaar na het KB van 31 januari 2003 tot vaststelling van het noodplan voor de crisisgebeurtenissen en -situaties die een coördinatie of een beheer op nationaal vlak vereisen, nog steeds beperkt zijn tot een voorlopige versie van het Nationaal Noodplan CBRN.

In het kader van dit Noodplan wordt trouwens voorzien dat de Minister van Binnenlandse Zaken beslist over een oefeningenprogramma. In de VS maakt men al geruime tijd werk om dit type scenario's op grote schaal op het terrein uit te testen (zie voorbeeld in bijlage 6). Intern Defensie werden reeds demonstraties gehouden (ook t.v.v. andere overheidsdiensten). Ook binnen Defensie moet men toegeven dat tijdens het verloop van dergelijke demonstraties verkeerde indrukken worden gewekt: voor bezoekers worden de eenvoudigste scenario's gedemonstreerd. Zeer zelden worden mankementen aan de man gebracht. Gevolg is dat toeschouwers (binnen of buiten defensie) vaak de verkeerde indruk krijgen dat een capaciteit reeds operationeel is met de bestaande middelen. Zo werd in 2006 een dergelijke demonstratie gehouden ten voordele van een buitenlandse delegatie: medewerkers waren de Cie CBRN en MHKA met medewerking van de Civiele Veiligheid. Gekwetsten werden opgehaald door Cie CBRN en ontsmet ter plaatse. Volledig in

¹²⁸ Algemene beleidsnota van de minister van Binnenlandse zaken, Belgische Kamer van volksvertegenwoordigers, DOC 51 1371/021, 24 november 2004, p.7.

¹²⁹ Algemene Directie Crisiscentrum, Activiteitenrapport 2004. Federale Overheidsdienst Binnenlandse Zaken, 26 oktober 2005, p. 60.

¹³⁰ Algemene beleidsnota van de minister van Binnenlandse zaken, Belgische Kamer van volksvertegenwoordigers, DOC 52 0995/010, 11 april 2008, p.14.

¹³¹ Eigen onderstreping.

overeenstemming met de Medische doctrine¹³², werden slachtoffers afgevoerd door ziekenwagens en ontkleed/ontsmet door de Civiele Veiligheid alvorens de spoeddienst te betreden. Nadien werden ziekenwagens ontsmet door Cie CBRN. Zelfs na dergelijke demonstraties (geen volwaardige oefeningen) kunnen reeds enkele positieve lessen getrokken worden:

- Afvoer van gekwetsten gebeurde na een snelle decontaminatie door de Cie CBRN. Transport werd voorzien door een ziekenwagen naar de sorteerzone door Civiele Veiligheid. De opmerking die men hier dient te maken is dat de ziekenwagens achteraf extern werden ontsmet, maar niet intern. Contaminatie van het voertuig aan de binnenzijde dient in de toekomst vermeden te worden.
- Er werden geen communicaties voorzien tussen de ploegen van Civiele Veiligheid die de gekwetsten moesten opvangen en de ploegen onderweg. In de praktijk kan dit de aanvoerwegen naar de sorteerzone ernstig verstoren. Efficiënte (beveiligde) communicatie tussen Defensie en andere hulpverleners moet ter beschikking gesteld worden van de verschillende actoren.
- Civiele Veiligheid bleek niet uitgerust met detectiemiddelen ter controle van de restbesmetting achteraf noch tijdens het proces van overdracht naar de spoedafdeling van het hospitaal. Bij aanwezigheid van restbesmetting zal dit voor gevolg hebben dat het agens binnengebracht wordt in de installaties van het hospitaal.
- Decontaminatie van ziekenwagens werd extern uitgevoerd, maar alle afvalwater vloede rechtsreeks in de rioleringen. Tot hier toe is er nog geen capaciteit voorzien voor opvang van afvalwater. Naar de toekomst toe zal “waste management” eveneens in de prioriteiten voorkomen, wat enkel toegejuicht kan worden.

De belangrijkste les die hieruit te trekken is, is de volgende: elk scenario moet afzonderlijk getraind worden naar de bestaande plannen. De mankementen zijn er niet om mensen terecht te wijzen, maar net om duidelijk te maken dat er oplossingen moeten komen. Het verdoezelen ervan kan slechts tot verkeerde conclusies of foute beslissingen lijden met zelfs slachtoffers tot gevolg. Men mag al aanvoeren dat betrokken plannen nog niet ondertekend zijn, dit verhindert de betrokken partners niet om de verschillende benaderingen en werkwijzen op het terrein reeds in te oefenen en op elkaar af te stemmen. Dit zou toelaten om tijdig tekortkomingen recht te trekken vooraleer ze in werkelijke situaties tot catastrofes leiden.

2.1.3. BEVEILIGING VOOR PERSONEEL EN DE OMGEVING MET INBEGRIIP VAN VEILIGHEIDSPERIMETERS (PROTECTION AND SECURITY)

In hoofde van de functie van “Incident Commander” (IC) moet een overzicht kunnen bewaard worden over de acties van de tussenkomende actoren en de veiligheid van deze actoren. “Protection” duidt in dit verband op de individuele en collectieve bescherming die het interventiepersoneel moet genieten tijdens het uitvoeren van de opdracht. Veiligheidsafstanden en meteorologische informatie vallen ook onder dit bestek. “Security” daarentegen houdt verband met de fysieke bescherming (door politie of militaire macht).

¹³² Doctrine de mise en œuvre de la capacité d’appui médical en environnement CBRN, draft 1 verkregen van LCL CHENOIS.

Met individuele of collectieve bescherming doelt men de beschermingsmiddelen die ter beschikking van het personeel zullen staan (na risicoanalyse) teneinde de opdracht uit te voeren. Hier is duidelijk een verschillende aanpak vanuit de Civiele Veiligheid ten opzicht van Defensie. Civiele Veiligheid benadert systematisch incidenten met de hoogst mogelijke beschermingsuitrusting nl. gaspakken. Daar waar dat voor grote rampen en snelle interventie voor het dichten van lekken gepast is, is dat misschien minder het geval wanneer staalname en forensisch onderzoek moeten uitgevoerd worden vooraleer de site te ontsmetten. De gaspakken leveren een beperkte autonomie nl. die van de perslucht die een drager kan meenemen. Praktisch moet men rekening houden met een autonomie van 1 uur met 1 gasfles. Hierbij moet men decontaminatietijd in rekening brengen. De praktijk heeft echter aangetoond dat een CBRNE incident snel 2 uren (of meer) in beslag kan nemen. In dat geval zijn reeds meerdere ploegen vereist, hetgeen niet ten goede komt aan de operaties. Omgekeerd gaat Defensie ervan uit dat een lager beschermingsniveau vaak voldoende is (gasmasker en chemische beschermingskledij). Duidelijke afspraken hieromtrent bestaan er niet en ook hier is het een kwestie van persoonlijke inschatting om te bepalen wanneer welke kledij aangetrokken zal worden. Uitgaan van het standpunt dat de risico's verwaarloosbaar zijn omwille van het hoge aantal valse meldingen is niet aan de orde: ieder incident kan reëel zijn en een professionele benadering van elk incident is een minimum wat de bevolking mag verwachten. Een compromis tussen de twee posities kan gevonden worden: er bestaan reeds normen die de aard van het risico koppelen aan het vereiste beschermingsniveau. De beschermingsniveaus werden opgesteld door het Occupational Safety and Health Administration (OSHA)¹³³. Zelfs al worden ze herzien na intensieve studie, toch kunnen ze nu reeds hun nut bewijzen door langdurige inzet in gaspak te beperken indien mogelijk en de te beperkte bescherming op te drijven indien nodig.

De veiligheidsperimeter is een operationele veiligheidszone die enkel vastgelegd wordt door de aard van het tuig dat het onderwerp uitmaakt van de interventie en/of de hoeveelheid/type agens dat in het incident betrokken is. Ook de windrichting zal hierin een rol spelen. De zone wordt enkel betreden door personeel in beschermingsuitrusting (bijvoorbeeld voor staalname of decontaminatie van infrastructuur) en heeft niets te maken met de organisatorische zones die verder besproken worden onder het gedeelte "security": ziekenwagens moeten bijvoorbeeld toegang krijgen tot de rode zone zonder daarom binnen de veiligheidsperimeter te komen. De vastlegging van deze perimeter wordt bepaald door de IC. Men kan zich de vraag stellen wat de ideale opstelling zou zijn van alle hulpdiensten op de plaats van een incident. Hiervoor kan men best terecht bij de ervaringsdeskundigen: instanties die reeds geconfronteerd werden met meerder simultane incidenten hebben op dat gebied een stapje voor en het loont dus de moeite om hun ervaring te toetsen aan hetgeen ons wettelijk wordt opgelegd door het KB en de Ministeriële omzendbrief in zake nood- en interventieplanning. Ter illustratie van de positionering van de veiligheidsperimeter binnen de organisatie van de zone van een incident, wordt in bijlage 7 een schema gegeven van de mogelijke opstelling van hulpdiensten op de plaats van één CBRN-incident¹³⁴. Als hulpmiddel voor het vastleggen van de veiligheidsperimeter in deze zone kan hij hiervoor gebruik maken van de Emergency Respons Guidebook (ERG-editie 2008): hierin wordt voor iedere gevaarlijke substantie (ook CBRN-agentia) zowel voor grote als kleine hoeveelheden, de

¹³³ General description and discussion of the levels of protection and protective gear te vinden op http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9767

¹³⁴ Schema aangepast uit: Operations in the UK: The Defence Contribution to Resilience. Interim Joint Doctrine Publication 02. Ministry of Defence, December 2004, bijlage 9c.

aangeraden veiligheidsafstanden weergegeven. Bovendien maakt dit document het onderscheid tussen transport of opslagcapaciteit van deze substanties. Ook incidenten bij dag of tijdens de nacht worden anders behandeld als eerste inschatting van gewijzigde meteorologische situaties. Bij gebrek aan nationale richtlijnen is dit een bruikbaar instrument. Contact met brandweerkorpsen uit alle provincies toont echter aan dat men slechts in twee provincies effectief gebruik maakt van dit document. De meeste korpsen steunen hun besluitvorming op ervaring of de “regel van de natte vinger”. In sommige gevallen wordt als vuistregel een afstand van 50 meter gebruikt. In andere gevallen verwacht men bijkomende input van politie of civiele veiligheid alvorens een veiligheidsperimeter vast te leggen. Deze exclusiezone wordt vaak gecombineerd met een steunzone van 300 meter: deze afstanden werden bepaald in het kader van gaslekken¹³⁵. Twee korpsen verwijzen naar het KB van 6 juli 1991 (gepubliceerd op 18 juli 1991) betreffende het bepalen van risicozones: dit KB houdt rekening met maximale stralingswarmte, druk of luchtconcentraties. Het probleem is dat in CBRN-scenario's de concentraties niet altijd te bepalen zijn in situ omdat het betrokken agens niet altijd onmiddellijk te identificeren is¹³⁶. Bijgevolg is deze wetgeving in deze niet bruikbaar. Tot slot zijn er korpsen die zich baseren op het “Brandweer Informatie Centrum gevaarlijk stoffen” (BIC), een geïnformatiseerd systeem van FOD Binnenlandse Zaken. Dit is echter een databank die voor elk product informatie verschaft over brandbaarheid en toxiciteit. Veiligheidsafstanden worden er niet aan verbonden en bijgevolg kan men dezelfde opmerking maken als bij het vermelde KB van 1991. Bruikbare databanken zijn reeds beschikbaar op het Internet (Toxnet of Hazardous Substance Data Base bijvoorbeeld). Het brandweerkorps dat het best op de hoogte blijkt omtrent de CBRNE problematiek is de brandweer van Gent: deze maakt, naar Nederlands voorbeeld, gebruik van meerdere bronnen m.n. ERG, het schadescenarioboek van TNO¹³⁷ en werkbladen (flow-charts om tot gestandaardiseerde besluitvorming te komen). Men kan enkel betreuren dat, enkel al voor het bepalen van een veiligheidsperimeter, deze dispariteit op nationaal niveau op de voorgrond treedt en dat men in sommige provincies zelfs niet weet wat wordt bedoeld wanneer men over CBRN-agentia spreekt. Nationale normen en een uniforme aanpak tot de besluitvorming in dit domein zijn van cruciaal belang en vormen de basis voor de daaropvolgende acties tijdens een incident. Benadrukken we hier nogmaals dat de operationele coördinatie wordt toegewezen aan de IC (zoals eerder vermeld is dit de Dir CP-Ops dus meestal Dir BW) voor nationale noodplanning. Voor geprojecteerde troepen kan men hopen dat de rol van IC toebedeeld wordt aan de ploegoverste van SIBCRA¹³⁸-eenheden. Deze officieren zijn vertrouwd met de informatie die in de ERG terug te vinden is en baten die ten volle uit. Natuurlijk zal de (eventuele) aanwezigheid van een springtuig mee de veiligheidsperimeter bepalen (zeker in initiële fase m.n. voor en tijdens de ontwapening van het tuig). De meest stringente veiligheidsperimeter zal moeten in beschouwing genomen worden, met een eventuele aanpassing na de ontmanteling van het springtuig of verspreidingsmechanisme. Specifiek in het kader van radiologische incidenten heeft het IAEA een leidraad uitgegeven met vermelding van veiligheidsafstanden en te ondernemen acties door de IC¹³⁹.

Een element dat mee de omschrijving van de veiligheidsperimeter zal bepalen zijn de weersomstandigheden: eventuele verspreiding of rookpluimen kunnen zich

¹³⁵ In navolging van de gasramp van Gellingen.

¹³⁶ Bovendien geven CBRN detectoren vaak enkel een orde van grootte van de gedetecteerde hoeveelheden en een idee van de klasse agens in het meest gunstige geval.

¹³⁷ Handleiding voor de schatting van schadegebieden bij ongevallen van brandbare en giftige stoffen.

¹³⁸ Sampling and Identification of Biological Chemical and Radiological Agents

¹³⁹ Manual for First Responders to a Radiological Emergency. International Atomic Energy Agency, October 2006.

verplaatsen en de gevaarlijke zone nog uitbreiden. Ook in dit geval kan de ERG een eerste hulp bieden, maar dit blijft slechts een ruwe benadering. Volgens het nationaal rampenplan doet het CGCCR beroep op het KMI om luchtstromen te voorspellen. Uit contacten met het KMI blijkt echter dat enkel de beweging van hoge luchtmassa's kunnen worden voorspeld. Voornamelijk in het geval van rampenplanning op nucleair gebied, levert het KMI bijstand door het gebruik van diffusiemodellen van luchtmassa's: het Europees Centrum Middellang Termijn levert wereldwijd een dagelijkse analyse. Lokaal kan een diffusiemodel met hogere resolutie gebruikt worden om, aan de hand van gemeten emissie, verwachte concentraties te bepalen. Deze modellen houden echter enkel rekening met dominante windstromen en niet met de micro-meteo die men kan terugvinden in stedelijke omgeving i.e. lokale weersomstandigheden die sterk kunnen afwijken vooral op gebied van windsnelheid en windrichting. Een bijkomend probleem in steden is het fenomeen dat bekend staat als "street canyons" m.a.w. de perturbatie van de luchtstromen aan de kruising van straten en gebouwen. Dit fenomeen laat toe dat besmetting zich ook kan uitbreiden naar straten die loodrecht lopen op het traject van de plaats van het incident. Turbulenties zullen eveneens voorkomen indien het incident zich voordoet in een ondergrondse garage of een metrostation: luchtkokers zullen voor een schouweffect zorgen. Het is dus niet uitgesloten dat de contaminatie zich kan uitbreiden tot aan de oppervlakte.

Een incident van het type CBRNE zal zich meer dan waarschijnlijk voordoen in stedelijke omgeving of haar onmiddellijke omgeving. Daarom zijn aangepaste modellen nodig die rekening houden met infrastructuur en voormelde fenomenen. Bovendien is een mobiel meteo-station, in de onmiddellijke omgeving van het incident van cruciaal belang. Een plots opkomende of draaiende wind, kan het hele dispositief inclusief de bevolking in gevaar brengen. Mobiele meetstations worden niet geleverd door het KMI maar het VITO beschikt wel over dergelijke uitrusting. Bovendien kan dit station metingen uitvoeren van "deeltjes" hetgeen bijzonder nuttig kan zijn in het geval van anthrax-incidenten. Een onderscheid kan hier worden gemaakt tussen deeltjes met een diameter kleiner dan $10\mu\text{m}$ (PM10) of zelfs kleiner dan $2.5\mu\text{m}$ (PM2.5). Temperatuur, windrichting, windsnelheid en vochtigheid worden eveneens geregistreerd. Het station heeft een autonomie van 24Hr. Tot hiertoe is het niet mogelijk om datacommunicatie te voorzien voor meteorologische gegevens. Andere gegevens kunnen wel doorgeseind worden in real-time (bijvoorbeeld naar het CGCCR). Dit mobiel meetstation kan zelfs uitgerust worden met sensoren op aanvraag (bijvoorbeeld tijdens de kwikmetingen op en rond de Brusselse kleine ring in april 2008). De capaciteiten van dergelijke uitrusting moeten zeker in overweging genomen worden voor mogelijke inzet in het kader van het Nationaal Noodplan CBRN.

Om de problematiek van de veiligheidsperimeter af te sluiten, moet men nog rekening houden met de tijd die nodig zal zijn om eventuele besmettingen ongedaan te maken. Hoe klein ook de besmette zone, decontaminatie kan een ruime periode vereisen. Als voorbeeld kunnen we teruggaan naar het incident met de anthrax-brieven van 2001 in de VS: de grondige ontsmetting van het getroffen gebouw nam twee weken in beslag. Gedurende de volledige periode was de zone niet betreedbaar. Neem hetzelfde voorbeeld in centrum Brussel en men kan zich een idee vormen van de chaos die zal veroorzaakt worden.

Security behelst onder meer de organisatie van de interventiezone en de veiligheid van het personeel dat erin opereert. Dit aspect omvat het geheel aan middelen die voorzien worden om veiligheid van het personeel tijdens hun activiteiten te garanderen. Op nationaal gebied kan men een vergelijking trekken met de omschrijving uit het KB van 16 februari 2006. Dit voorziet in art. 25 een zoneverdeling in:

- Een Rode Zone begrensd door een uitsluitingsperimeter en is enkel toegankelijk voor hulpdiensten, technici en deskundigen mits toelating van Dir-CP-Ops.
- De Oranje Zone: binnen deze zone wordt de logistieke steun van de hulpdiensten georganiseerd. Toegang tot personen die er wonen en werken wordt verleend door Dir-CP-Ops binnen de isolatieperimeter.
- De Gele zone wordt omsloten door een ontradingsperimeter m.a.w. personen die er niet wonen, werken of interventie moeten uitvoeren worden uit deze zone geweerd.

Bijlage 7 van dit werk toont de invulling van de vermelde zones in een bestaande organisatie naar Angelsaksische model. Het is duidelijk dat de toegangscontrole tot de zones onder de bevoegdheid van discipline 3 (politieopdracht) valt. Het incident zal een toevloed van hulpverleners, onderzoekers en specialisten veroorzaken. De veiligheid van die mensen moet ook gegarandeerd worden. Gezien de technieken van terroristen om sequentiële of gelijktijdige aanvallen uit te voeren (bijvoorbeeld in Irak), is het niet ondenkbaar dat een zelfmoordcommando ter plaatse blijft om zo veel mogelijk mensen te treffen na de vaststelling van het incident. Daarom moet iedere actor op de plaats van het incident geïdentificeerd worden en toegang tot de zone verkrijgen van Dir-CP-Ops die deze taak kan delegeren naar een klein secretariaat: iedere hulpverlener zou een duidelijk zichtbare identificatie moeten dragen met aanduiding van de functie die hij ter plaatse uitoefent. Ook tussen de slachtoffers kunnen zich mensen verschuilen die geen zuivere bedoelingen hebben. Daarom moeten deze prioritair uit de zone verwijderd worden.

De eerder vermelde veiligheidsperimeter zal bepalend zijn voor de omvang van de vermelde omliggende organisatorische zones. Dit wil zeggen dat omwille van eventuele evacuatie en impact op de samenleving, het van cruciaal belang zal zijn een gepaste inschatting te maken van de veiligheidsperimeter. De veiligheidsperimeter bepaalt de veilige afstand van hulpverleners in de voorbereiding tot de betreding van de exacte locatie van het incident. Deze perimeter is gelegen binnen de rode zone. Voor de bepaling van de omvang van de veiligheidsperimeter werden hoger voorstellen geformuleerd. Binnen de rode zone zal ook de decontaminatieketen en eventueel een ziekenwagen voorzien moeten worden voor opvang van hulpverleners. De sequentie voor het betreden van de zone moet omwille van veiligheidsredenen (overbelasting van de decontaminatieketen, vrijwaren van sporen, weren van potentiële daders en rampoeristen) vooraf in de plannen opgenomen worden. Bovendien zal men rekening moeten houden met het feit dat de gecontamineerde zone kan uitbreiden door de meteorologische omstandigheden.

Deze organisatie kan ook in een geprojecteerd scenario toegepast worden. Bij geprojecteerde troepen kan de afbakening van de zones versterkt worden door gewapende troepenmacht in functie van de lopende operaties in de nabije omgeving.

2.1.4. HET ONTWAPENEN VAN EXPLOSIEVEN EN HET BEVEILIGEN VAN CBRN MATERIAAL (RENDER SAFE & DISPOSAL)

De bedoeling van deze activiteiten worden in extenso weergegeven in de EU NBC EOD Policy¹⁴⁰ met name:

- Vrijwaren van mensenlevens zowel van burgers, veiligheidstroepen als alle leden van de EOD-ploeg.

¹⁴⁰ EU NBC EOD POLICY, Headline Goal Task Force, Februari 2006, enclosure 1, p.4.

- Verwijdering van de bedreiging: zowel de springstof als de CBRN elementen van het tuig moeten vernietigd kunnen worden.
- Beperking van materiële schade en de schade aan het milieu.
- De situatie herstellen naar de oorspronkelijke staat.
- Indien mogelijk forensisch bewijsmateriaal vrijwaren: de samenstelling van het tuig kan duidelijke aanwijzingen geven naar de daders.

Het is duidelijk dat in vele gevallen het gebruik van standaardprocedures niet zullen volstaan: zoals reeds aangehaald is de mechanische destructie van het ontstekingsmechanisme niet altijd de beste neutralisatiemethode voor CBRN-tuigen. Om dit probleem aan te pakken zal men moeten terugvallen op manuele ontminnings- en neutralisatiemethodes. Hiervoor neemt men natuurlijk risico's voor het ingezette personeel. Men dient a priori af te wegen wat de voor- en nadelen zullen zijn bij het gebruik van standaardtechnieken (disruptor vs. manuele inzet) voor ieder scenario dat bekend is. Bovendien moeten de actuele robots voorzien kunnen worden met zowel chemische als radiologische detectoren. In de huidige context zal men niet altijd verwittigd worden over de mogelijkheid dat er een CBRN-scenario aan de gang is. Een routineopdracht kan uitdraaien op de verspreiding van een CBRN-agens door de ontmanteling van een pakket met een onconventionele samenstelling. De aanwezigheid van deze detectoren zou in dat geval een vooralarm kunnen geven alvorens het onherroepelijke gebeurd is. Dit zou in de huidige procedures standaard voorzien moeten worden. Desnoods kunnen, als noodoplossing, detectoren aangehecht worden aan de robot en de aflezing kan gebeuren via de camera's (aangezien datatransmissie van sensoren niet voorzien is). Toch moet men EOD en IEDD-ploegen kunnen uitrusten met ontsmetbare robots. Indien dit niet het geval is zal men, geval per geval moeten afwegen of men een robot, met het gekende prijskaartje, wil prijsgeven in elk CBRN incident omwille van dit mankement, dan wel a priori deze capaciteit wil voorzien om menselijke inzet een stuk veiliger te maken. Ook hier zullen zich beleidsmatig keuzes opdringen: men kan a priori materiaal voorzien dat volledig ontsmetbaar is, voorzien van alle noodzakelijke detectoren, inzetbaar zowel nationaal als geprojecteerd. Alternatief kan men kiezen voor een goedkopere oplossing nl. robots zonder alle of slechts gedeeltelijk voormelde capaciteiten. Dit zal de ploegen de facto verplichten om manuele inzet van mensen te voorzien of een besmette robot op te geven. Kosten/baten analyse enerzijds en risicoanalyse voor inzet van personeel anderzijds, zouden het antwoord moeten geven.

2.1.5. INPERKING VAN BESMETTING EN DECONTAMINATIE (HAZARD MANAGEMENT)

Het beheer van het gevaar omhelst meerdere elementen nl. inperking van het gevaar en decontaminatie. Inperking van het gevaar is vooral gericht op de plaats waar het incident zich voordoet (containment) door bijvoorbeeld ramen en deuren te sluiten en ventilatiesystemen uit te schakelen om verdere verspreiding te vermijden. Deze methode kan eveneens gebruikt worden om de situatie op de plaats van het incident te "bevriezen" nl. door de afscherming van het gevaar¹⁴¹ voor de omgeving,

¹⁴¹ Dergelijke systemen om een CBRN(E)-pakket in een explosie-resistente massa te isoleren bestaan op de markt, maar hebben het nadeel dat de behandeling nadien (detectie en staalname) moeilijker wordt. Dit kan wel een oplossing zijn indien transport van het pakket op korte termijn voorzien is naar een andere locatie.

terwijl het hele dispositief van hulpverlening in plaats kan gesteld worden. Het kan immers enkele uren duren vooraleer alle actoren ter plaatse zijn en de noodzakelijke tijdelijke infrastructuur hebben opgebouwd om het incident te beheren. Inperking geldt echter ook voor de eerste lijn hulpverleners en andere hulpdiensten. Adequate individuele en collectieve beschermingsmiddelen moeten toelaten een degelijke afscherming van eender welk CBRNE gevaar te garanderen. Decontaminatie is een essentieel element in de behandeling van CBRNE incidenten: het garandeert de veilige terugkeer van gekwetsten en personeel uit de gevarezone. Bovendien is het noodzakelijk dat de voertuigen, de tijdelijke infrastructuur en de site zelf, na ontruiming van de zone, een volledige en grondige ontsmetting ondergaat. Naar gelang het gebruikte CBRN agens, zal men eventueel verschillende middelen inzetten. Zeker naar personeel en materieel toe, zal een verschillende procedure gehanteerd worden wat de decontaminatie betreft. Deze stap wordt gedurende trainingen vaak over het hoofd gezien: een CBRN oefening in militair milieu kan gemakkelijk een dag in beslag nemen. Decontaminatie en de daaropvolgende ontkleding is dan meestal het einde van de oefening en wordt niet altijd ernstig uitgevoerd of zelfs helemaal niet: de oefening stopt vaak na de detectie en de staalname. Men moet er zich echter rekenschap van geven dat decontaminatie de cruciale schakel is om het incident op een veilige manier achter zich te laten. Niet het vergaren van bewijsmateriaal is het belangrijkste maar de recuperatie van de slachtoffers (gekwetst en overleden) en eigen personeel (medische hulpverleners, brandweer, Civiele Veiligheid) krijgen de hoogste prioriteit. Als daarbij het nodige bewijsmateriaal intact kan geïncollateerd worden dan is dat een pluspunt. In ieder geval en bijzonder bij een groot aantal slachtoffers (“massive casualties” MASCAL) zullen de meeste middelen ingezet worden in het kader van die slachtofferhulp. Een correct beheer van de site volgens standaardprocedures zal toelaten om na de evacuatie van de slachtoffers en voor decontaminatie van de site, rustig de tijd te nemen om forensisch materiaal te verzamelen.

Men moet ook rekening houden met het pre-advies dat nodig zal zijn om een decontaminatieketen ter plaatse te krijgen: indien plaats en tijd van een kritische manifestatie bekend zijn, kunnen reeds middelen in stand-by gezet worden in de nabijheid van het evenement. Indien echter gebeurtenissen onverwacht en simultaan op verschillende plaatsen plaatsgrijpen, kan de oproeptijd voor het verkrijgen van decontaminatiemiddelen snel oplopen tot enkele uren. Geen enkele actie kan echter gestart worden zonder decontaminatieuitrusting. Eerste hulpverleners, betrokken in een CBRN incident moeten dus aangespoord worden om een minimum aan middelen (voor eigen gebruik) bij zich te hebben.

Een laatste aspect dat hier in beschouwing moet genomen worden is het afvalbeheer: interventieploegen zullen grote hoeveelheden gebruikt (besmet) materieel overhouden na zo'n incident (kledij, uitrusting, staalnamemateriaal, etc). Dit alles moet onderwerp uitmaken van een plan “recuperatie van besmet afval” eventueel onder de vorm van tijdelijke beveiligde opslag om later door een gespecialiseerde firma opgehaald te worden. Ook het afvalwater, afkomstig van decontaminatie (personeel en voertuigen), zal moeten gerecupereerd worden alvorens in de riolering terecht komt. Deze capaciteit van “Waste Management” door recuperatie van afvalwater is een prioriteit voor de nabije toekomst binnen Defensie. Voor wat vast materiaal en uitrusting betreft, wordt deze procedure reeds toegepast (ook in geprojecteerd scenario's).

2.1.6. DETECTIE EN STAALNAME (DETECTION & SAMPLING)

Detectie en staalname zijn van cruciaal belang in het verloop van de activiteiten binnen de gevarezone. Detectie zal immers (in het beste geval) toelaten een categorisatie van het betrokken agens toelaten: metingen kunnen uitgevoerd worden die minstens een categorie van agentia zal weergeven. Hiermee kunnen de medische hulpverleners hun behandelingen beter richten. Biologische detectie is tot op vandaag niet mogelijk. De commerciële toestellen, actueel op de markt verkrijgbaar, zijn gebaseerd op detectie van deeltjes, wat in stedelijke omgeving altijd tot twijfelachtige resultaten zal leiden. Het is dus zeer goed mogelijk dat op de plaats van het incident geen enkele detector indicatie kan geven van het agens dat oorzaak was van wat zal volgen, maar dat de eerste zieken zich enkele uren tot dagen na het incident zullen aanmelden op verschillende plaatsen: daarom zal iedere persoon van wie men vermoedt dat hij/zij mogelijk blootgesteld is geweest moeten geregistreerd worden. In dat geval kan men de mogelijke slachtoffers sneller traceren bij het opduiken van de eerste ziektebeelden. Een alternatief kan gevonden worden in het invoeren van een quarantaineperiode voor deze mensen tot wanneer men uitsluitel heeft van de biologische analyses op de genomen stalen. Belangrijk om weten is dat in alle gevallen, een detectie ten velde altijd zal moeten bevestigd worden door een identificatie in een erkend laboratorium. Deze identificatie zal moeten gebeuren aan de hand van stalen die op de plaats van het incident werden genomen. Het is dus van cruciaal belang dat alle stalen met uiterste zorg worden genomen en dat de behandeling ervan gedekt wordt door de traceerbaarheid vanaf staalname tot rapportering van de analysesresultaten. De resultaten van de analyses zullen natuurlijk moeten doorgegeven worden aan de medische hulpverleners, het beleid ter plaatse (Dir CP-Ops) en naar het hoger echelon (CGCCR). Hierna is het werk nog niet beëindigd: de zone zal mogelijk besmet zijn en decontaminatie zal mogelijk dagen of weken in beslag nemen. Het is dus noodzakelijk dat na evacuatie van alle slachtoffers, de controle op de restbesmetting wordt uitgevoerd. Zolang er geen aanvaardbaar lage concentraties agentia gemeten worden, zal de zone afgebakend en gecontroleerd moeten worden. Het probleem is dat detectoren ten velde in vele gevallen niet alleen beperkt zijn voor de correcte identificatie (enkel categorieën van chemische agentia worden weergegeven zoals zenuwgassen of blaartrekkers), maar dat ook de concentratie in vele gevallen niet aangegeven kan worden: deze toestellen zijn voornamelijk geconcentreerd om aan te geven of er een besmetting is, niet om te bepalen hoeveel agens er rest. Dat is precies het werk van een laboratorium. Om die reden zou het ook aangewezen zijn dat in de opstelling van de hulpverleners op de plaats van het incident een mobiel identificatielaboratorium wordt opgenomen in het dispositief. Dit zou kunnen opgesteld worden in de oranje zone (zie schema bijlage 7), dicht bij de CP-Ops.

Het is evident dat deze sequentie en opstelling eveneens kan toegepast worden in een scenario van geprojecteerde troepen. Bovendien moet men, voor wat de staalname betreft, kunnen berusten op mensen die opleiding hebben genoten en die het gewoon zijn in beschermuitrusting te werken in besmette omgeving. Opleidingen in die zin dienen gegeven te worden aan iedereen die een besmet gebied moet betreden omwille van zijn/haar taken. Deze opleiding moet gevolgd worden door regelmatige oefeningen door alle actoren die ter plaatse zullen werken, met gebruik van reële communicatiemiddelen. Lessen moeten getrokken worden uit iedere oefening en opgenomen worden in herhalingslessen die op regelmatige tijdstippen moeten gebeuren.

2.1.7. SPORENONDERZOEK (IDENTIFICATION FORENSICS)

In deze categorie vallen zowel het sporenonderzoek ter identificatie van de dader(s) als ook het werk ter identificatie van de slachtoffers. Het sporenonderzoek zal voornamelijk door NICC moeten gebeuren. Deze analyses zullen echter plaats grijpen in laatste instantie (na uitsluiting van alle mogelijke CBRNE gevaren). Het is zelfs mogelijk dat bruikbare sporen niet kunnen bewaard worden omwille van de ontsmettingsactiviteiten. DNA materiaal op overtuigingsstukken bijvoorbeeld zal vernietigd worden door decontaminatievloeistof. Men moet er zich echter rekenschap van geven dat de veiligheid van de bevolking en de terugkeer naar een normale situatie de voorrang zal krijgen. Het zou onaanvaardbaar zijn mensenlevens op het spel te zetten voor de vrijwaring van stalen. Dit geldt zowel voor de scenario's in het thuisland als in geprojecteerde scenario's.

Wat de identificatie van de slachtoffers betreft, moet men onderscheid maken tussen de gekwetsten en de dodelijke slachtoffers. Gekwetsten zullen in principe op vrij korte termijn geïdentificeerd kunnen worden (door vraagstelling indien mogelijk). Het grootste probleem zal zich stellen voor identificatie van overleden slachtoffers. De omzendbrief van de Minister van Binnenlandse Zaken is duidelijk in dit verband: deze taak wordt toegewezen aan het Disaster Victim Identification Team (DVI) van de Federale Politie (althans in het Nationale scenario). Hier rijst het probleem dat alle slachtoffers besmet zullen zijn. Bovendien zal het DVI pas op het terrein verschijnen wanneer alle andere actoren (DOVO, Civiele Veiligheid, Staalnameploegen, Ambulanciers) reeds van het toneel zijn verdwenen. Na navraag bij het DVI¹⁴² werd duidelijk dat de planning van dergelijke scenario's nog in kinderschoenen staat. In principe vereist identificatie van overleden slachtoffers dat een post-mortem onderzoek plaatsgrijpt waarbij een aantal gegevens worden verzameld met onder meer:

- Identificatiedocumenten.
- DNA-materiaal (buccale staalname).
- Tandheeskundige gegevens.
- Intern onderzoek (autopsie door een wetsgeneesheer).
- Extern onderzoek (tatouages of andere kenmerken).
- Fotografie.
- Vingerafdrukken.
- Radiografie.

Men moet er zich echter rekenschap van geven dat het slachtoffer volgens de gangbare procedures eerst ontkleedt moet worden: in normale omstandigheden kan dit reeds een lastige en tijdrovende klus zijn. Bijzonder indien reeds lijkstijfheid is ingetreden. In CBRN-omstandigheden kan dit een onoverkomelijke hindernis vormen. Betrokken personeel moet in ieder geval in beschermkledij werken. Indien ontkleding en decontaminatie van het slachtoffer niet mogelijk zijn op het terrein, moet een andere oplossing gevonden worden. Hierbij moet men bovendien rekening houden met het feit dat de inzetijd van de werkende ploegen zo kort mogelijk gehouden wordt. Voorstel is om de identificatie in twee fasen te laten gebeuren. Men zou in eerste instantie essentiële sporen ter plaatse kunnen nemen (vb identificatiedocumenten, buccale DNA-staalname, haarfollicels en foto's van het slachtoffer). Deze gegevens kan men dan bewaren in een afgesloten doos (post-

¹⁴² Interview op datum van 02 juni 2008.

morten CBRN identification kit¹⁴³) die extern ontsmet kan worden zonder de sporen te vernietigen. Pas na identificatie van het betrokken CBRN-agens kan men dan overgaan tot heropening van de kit in gepaste omgeving (in een laboratorium, onder een trekkast met individueel beschermingsuitrusting). Het slachtoffer zelf dient niet meer ter plaatse ontkleedt te worden. De omslachtige decontaminatie kan men ook vereenvoudigen: door gebruik te maken van body-bags met kijkvenster kan men het slachtoffer met kledij bergen en de buitenzijde van de zak laten ontsmetten. In hospitalen kan men dan het intern onderzoek initieel vervangen door een Rx of een CT-scan, zonder opnieuw toegang te moeten krijgen tot de besmette inhoud van de zak (lichaam en kledij). Indien hoger vermelde gegevens nog géén antwoord kunnen bieden met betrekking tot de identiteit van het slachtoffer, kan men in een latere fase overgaan tot heropening van de body-bag in gecontroleerde omgeving met beschermkledij: autopsie zou dan laatste invulling kunnen geven omtrent de identiteit van het slachtoffer. Men dient er rekening mee te houden dat deze procedures slechts voorstellen zijn, en getraind zullen moeten worden op hun haalbaarheid. Ook de ingezette ploegen zullen deze werkwijze in CBRN-uitrusting moeten testen. Gegevens omtrent het te gebruiken materieel en de procedures worden in de huidige stand van zaken bestudeerd. Het is duidelijk dat ook hier enkel de uitgeteste procedures zullen moeten toegepast worden en dat samenwerking met andere FODs en Defensie noodzakelijk is. In het kader van oefeningen zou het nuttig zijn om in de toekomst ook het DVI-team te betrekken: het is immers pas na het vertrek van DVI en de berging van alle slachtoffers dat men zal kunnen overgaan tot de decontaminatie van de site.

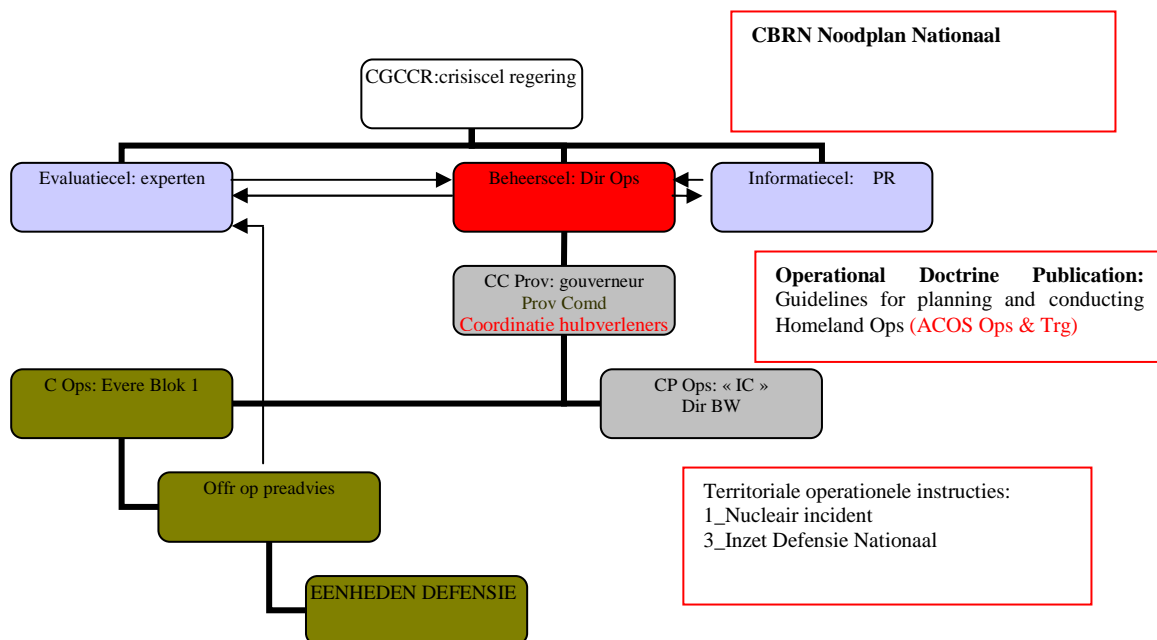
Ook deze procedure kan men toepassen zowel in het Noodplan CBRN Nationaal, als in geprojecteerde scenario's: of DVI wordt uitgestuurd bij incidenten in het buitenland is een beslissing van de regering. In principe kan dit gebeuren, zelfs indien militairen slachtoffer zijn. Men zal wel rekening moeten houden of de slachtoffers gevallen zijn in oorlogsgebied: in dat geval kan men beslissen de lichamen te repatriëren naar België. Desgevallend zullen de militairen ter plaatse ook de toe te passen procedures aanleren die gevolgd moeten worden indien identificatie niet meer onmiddellijk mogelijk blijkt.

2.1.8. NABESCHOUWINGEN EN BESTAANDE PLANNEN

Al de vermelde vereisten dienen voorzien te worden in doctrines en procedures. Bovendien moeten de nodige investeringen gebeuren voor het organiseren van oefeningen op het terrein: voorlopig ontbreekt echter een nationaal noodplan CBRN, of zelfs een inter-FOD protocolakkoord dat een voorlopig kader kan scheppen om gestandaardiseerde procedures toe te passen. In de schoot van Defensie echter, werd reeds een doctrine afgetekend. Deze zal ingevuld moeten worden door de capaciteiten van de eenheden om vertaald te kunnen worden naar Territoriale Operationele Instructies. Als men de structuur van CGCCR en de integratie van Defensie vergelijkt met bestaande procedures komt men tot volgend schema (zie schema 2):

¹⁴³ Dit materiaal is nog niet als dusdanig aanschafbaar. De hier voorgestelde benaming zal gelden voor een kit die vermelde standaarduitrusting bevat voor staalname op de plaats van het delict.

Schema 2 : noodplanning



Het Nationaal Noodplan CBRN wordt uitgewerkt door het CGCCR. Op Militair niveau is een operationele Doctrine uitgewerkt door ACOS Ops &Trg. Deze schetst het algemeen kader waarin troepen van Defensie kunnen ingezet worden als steun aan de Natie. Naar de eenheden toe wordt deze doctrine vertaald in Territoriale Operationele Instructies met voor de eenheden bruikbare procedures voor operationele inzet. Het is duidelijk dat militaire eenheden steeds onder militair commando zullen blijven: daarom zijn contactpunten tussen burgers en militairen vereist: via de Provinciecommandant zal een officier van permanentie kunnen opgevorderd worden om te zetelen in de evaluatiecel van het CGCCR (deze oproeping zal gebeuren via COps Evere). In de praktijk stelde Kol SBH DE KIMPE reeds vast dat de Prov Comd OPCON of Ops Ctl¹⁴⁴ te hebben over de ingezette eenheden. Reden waarvoor een nieuwe structuur werd voorgesteld waarbij de Prov Comdo's ook liaison kunnen uitvoeren met de gemeentelijke crisiscentra (CP Ops). Hierbij werden voorstellen geformuleerd voor een nieuwe structuur en de creatie van een cel "Counter Terrorism and National Operations (CT & NatOps)". Welke ook de invulling die men aan deze cel wil geven, moet men hierbij opmerken dat de voorafgaande in plaats stelling van een cel risicoanalyse (in de schoot van CGCCR) een absolute noodzaak is. Praktisch zou men voor de bemanning van deze cel bijvoorbeeld beroep kunnen doen op het militair personeel van CNVV bij CGCCR. Het bestaande voorstel laat toe om op nationaal niveau een liaison te houden vanuit de evaluatiecel van de CGCCR, aangevuld met de officier van permanentie die opgeroepen wordt door COps om de evaluatiecel te verwoegen in geval van dreigende crisis. Bovendien kan op lokaal niveau, tactische controle uitgevoerd worden over de ingezette eenheden van Defensie. In die zin zal de IC rechtsreeks contact hebben met

¹⁴⁴ Kol SBH DE KIMPE, J., Bescherming van vitale infrastructuur. Welke rol voor Defensie? Kabinet Defensie, 2007, p.71.

de eenheden op de plaats van het delict door de inzet van CC Prov op lokaal niveau: in geval van incident is het dus inderdaad nodig om CC Prov in permanente wisselwerking te laten opereren met de CP Ops.

Tot slot dient men nog rekening te houden met het feit dat dergelijke incidenten zich kunnen voordoen op verschillende plaatsen tegelijkertijd. Voorbeelden uit het verleden tonen meer en meer deze trend aan: bedoeling is om de hulpverlening zodanig te belasten dat de capaciteiten uitgeput raken. Reden te meer om in bestaande plannen of nog op te stellen plannen, rekening te houden met de multipliciteit van simultane incidenten. Voldoende logistieke capaciteit moet dus voorzien worden om ervoor te zorgen dat inzet van middelen op verschillende plaatsen mogelijk blijft, met voldoende opvangcapaciteit voor slachtoffers in omringende ziekenhuizen.

Ook de wetgever kan hier zijn bijdrage leveren om voornoemde scenario's te vermijden. Terrorisme en sabotage van vitale infrastructuur kan ernstige gevolgen hebben voor de samenleving. De adequate aanpak van incidenten van dit type vergt heel wat inzet van personeel en materieel. Bijgevolg is het beter dergelijke incidenten te kunnen voorkomen. Hiervoor moet men meer aandacht schenken aan de bescherming van bestaande infrastructuur, transport van goederen die onder de ADR-normen vallen, opslagcapaciteit en kerncentrales. Alle betrokken partners, FODs en Defensie moeten in deze problematiek betrokken worden. Een illustratie van de moeilijkheidsgraad om alle betrokken organen i.v.m. noodplanning zowel op nationaal als op internationaal vlak te betrekken, wordt weergegeven in bijlage 8: een bijkomende hindernis wordt geïllustreerd door de interacties tussen de verschillende organen. Deze komt soms tot stand via individuele contactpersonen (verbindingspijlen tussen persoonsnamen) of tussen organisaties (groene pijlen voor nationale contacten, rode pijlen voor internationale contacten).

Bedreiging vanuit criminele organisaties, individuen op voornoemde infrastructuur enerzijds en de invloed van georganiseerde misdaad, witteboordencriminaliteit in de organisatie van WMD-transfers anderzijds, kunnen leiden tot indirecte CBRN dreiging. Globalisatie drijft bovendien niet-staatsactoren op het pad van de proliferatie en bedreiging van kritische infrastructuur. De nodige middelen moeten dus voorzien worden om ook op dit terrein weerstand te kunnen bieden.

2.2. Initiatieven voor preventie van en strijd tegen proliferatie

Zowel internationale als nationale instanties hebben verdragen, werkgroepen en praktische richtlijnen opgesteld die de nodige middelen moet verschaffen om de strijd tegen proliferatie vorm te geven. In deze paragraaf belichten we de verschillende internationale beleidsniveaus en de respectievelijke initiatieven die moeten uitmonden in concrete maatregelen op nationaal niveau.

2.2.1. VERENIGDE NATIES

In het kader van de strijd tegen proliferatie, wordt in de schoot van de Verenigde Naties de naleving van meerdere verdragen nagegaan, die afgesloten werden om de proliferatie van WMD en hun vectoren in te dijken en zelfs bestaande stocks af te bouwen. Naast deze verdragen werden ook een aantal “export controle mechanismen” geactiveerd die tot op de dag van vandaag nagaan of aan de voorwaarden wordt voldaan om technologie van tweeërlei aard en ander gevoelig materieel aan strikte banden te leggen. Deze kunnen slechts het voorwerp uitmaken van verkoop indien aan strenge voorwaarden wordt voldaan¹⁴⁵.

Vestigen we eerst onze aandacht op de geldende verdragen. Het “Non-Proliferation Treaty” (Non-Proliferatieverdrag of NPT) werd van kracht in 1970: door dit verdrag verbonden de vijf kernmachten zich ertoe hun arsenaal af te bouwen. De overige ondertekenaars verbonden zich ertoe om de ontwikkeling of de aanschaffing van kernwapens af te zweren. Uitvoer naar niet-kernmachten werd verboden behalve indien, onder toezicht van het internationaal atoomagentschap (IAEA) gelegen in Wenen, de controlemechanismen (“safeguards”) en traceerbaarheid gegarandeerd werden. Deze instantie (IAEA) zag haar mandaat bovendien uitgebreid door het “Additional Protocol to the NPT Safeguards Agreement” (toegevoegd protocol voor garantiemaatregelen). Dit protocol, goedgekeurd sinds 1997, laat meer stringente controles toe door het agentschap: ondertekenaars worden verplicht hun activiteiten i.v.m. kernenergie bekend te maken naar aanleiding van de omzeiling van de initiële garantiemaatregelen door Irak. Inspecties door het atoomagentschap hebben de toelating om zowel aangegeven als niet aangegeven sites te controleren op hun activiteiten. Sinds 1995 werd het NPT impliciet uitgebreid tot alle landen (zie bijlage 2). Artikel IV van het verdrag erkent de vreedzame toepassing van kernenergie: men kan zich echter vragen stellen bij het bilateraal verdrag tussen de VS en India omtrent levering van kernbrandstof dat in 2008 definitief vorm kreeg. India is een kernmacht de facto, maar heeft nooit een verdrag hieromtrent ondertekend. Bovendien is buurland Pakistan eveneens een kernmacht de facto. Beide landen hebben reeds enkele oorlogen achter de rug en zijn nog steeds sinds jaren verwickeld in een bloedige strijd omtrent de regio Kashmir. Hoewel kernbrandstof, vandaag meer dan ooit, van cruciaal belang is voor een land in volle economische groei als India, moet men enkele bedenkingen maken:

¹⁴⁵ Integrale teksten van de vermelde verdragen, data van ondertekening en ratificatie kunnen teruggevonden worden op de site van de Verenigde Naties:
<http://disarmament.un.org/wmd/ctbt/index.html>

- De VS heeft reeds een gelijkaardige overeenkomst afgesloten met Rusland (op 6 Mei 2008) voor de levering van kernbrandstof voor vreedzaam gebruik. Het akkoord met India voorziet echter een specifiek luik dat het land toelaat zelf te bepalen welke sites worden onderworpen aan inspectie door het internationaal atoomagentschap. Hoewel de initiële bedoeling om aanrijking van kernbrandstof aan banden te leggen lovenswaardig lijkt, kan men zich niet van de indruk ontdoen dat een nieuw energetisch monopolie vorm krijgt, dit maal op het domein van de kernenergie. Het zou niet onbelangrijk zijn om het toezicht van alle aanrijkings- en leveringscapaciteiten onder toezicht van de Verenigde Naties te plaatsen. In dit kader zouden ook billijke prijzen kunnen afgesproken worden.
- De aan Iran opgelegde sancties geven een indruk van partijdigheid in het licht van dit nieuw akkoord met India. Alle betrokken instanties - het Congres, het IAEA (nucleaire waakhond van de VN) en de Nuclear Suppliers Group (exportcontrole regime-zie verder) - hebben hun fiat gegeven voor deze op maat geschreven overeenkomst. Hoe kan men Iran in deze omstandigheden verplichten om haar eigen aanrijkingcapaciteit op te geven terwijl India zelf heeft mogen beslissen welke nucleaire sites een militair karakter hebben en verboden terrein blijven voor inspecties door het IAEA? Geen enkele verplichting wordt opgelegd aan India om het NPT na te leven. Buurland Pakistan zoekt ondertussen toevlucht in mogelijke leveringen vanuit China om het economisch en militair evenwicht in de regio te bewaren.
- Ook Rusland gaat niet vrijuit: de voorziene levering van een kernonderzeeër van de Akula-klasse aan India heeft vertraging opgelopen door het incident tijdens de laatste controles voor levering. Men kan enkel vaststellen dat economische belangen voor alle actoren primeren boven het nastreven van de stabiliteit in een regio onder permanente druk.

De tweeslachtige houding van de permanente leden van de VN Veiligheidsraad kan men verklaren door economische doeleinden die bovendien de geopolitieke invloedssfeer uitbreiden door nieuwe economische banden te creëren. Deze problematiek zal een ernstige uitdaging vormen voor de legitimiteit van het NPT tijdens de herzieningsconferentie van 2010. Artikel VI van het NPT is specifiek gericht op de afbouw van kernwapenarsenalen: in dat kader werd het START I¹⁴⁶ verdrag afgesloten tussen de VS en de Sovjet-Unie. Dit verdrag zal aflopen op 5 december 2009. Een verdere vermindering van het bestaande arsenaal werd voorzien in het verdrag van Moskou dat op 1 juni 2003 van kracht werd: doel is tegen 31 december 2012 het aantal kernkoppen te verlagen (tussen 1700 en 2200 aan beide zijden). Er zijn in het kader van dit verdrag echter geen tussenstappen in de afbouw noch bilaterale afspraken tot controle gepland, wat te betreuren valt. Nieuwe gesprekken tussen de VS en Rusland, zouden in de loop van 2009 een hernieuwing van de inspanningen tot ontwapening moeten materialiseren.

In 1996 werd het “Comprehensive Test Ban Treaty” ondertekend: het voorziet de stopzetting van alle type kernontploffingen met een grondig controlesysteem. Pas na de ratificatie door alle kernwapenstaten zal dit verdrag in voege treden.

De chemische wapenconventie (“Chemical Weapon Convention”) werd van kracht op 29 april 1997: ze verbiedt de productie, opslag, aankoop en transfer van chemische wapens. Het organisme dat toezicht moet houden op de correcte uitvoering van dit verdrag is de organisatie voor verbod op chemische wapens (OPCW) gelegen in Den Haag.

¹⁴⁶ Strategic Arms Reduction Treaty trad in werking op 5 december 1994 na het uiteenvallen van de Sovjet-Unie.

De biologische wapenconventie (“Biological and Toxin Weapons Convention”) verbiedt sinds 1975 de ontwikkeling, productie, opslag, aankoop en transfer van pathogenen en daartoe ontwikkelde wapensystemen of andere vectoren. Het gebrek aan een controleorganisme verbonden aan dit verdrag (zoals het IAEA voor het NPT, OPCW voor CWC) om naleving af te dwingen, heeft de efficiëntie van dit verdrag ernstig ondermijnd. Mogelijk ware het een (tijdelijke) oplossing geweest om de wereldgezondheidsorganisatie (WHO), eventueel onder de vorm van een specifieke “task force” de bevoegdheid te geven die de controleorganismen genieten in het kader van de andere verdragen.

Wat de vectoren betreft, is er géén echte resolutie of verdrag: de toegenomen onrust onder de lidstaten omtrent de proliferatie van raketten deed de druk toenemen om een initiatief te starten ter zake. Dit gebeurde vanaf 2000. Herhaalde pogingen en tussentijdse jaarlijkse rapporten van 2000 tot 2007, hebben de problematiek van de proliferatie van vectoren in de schijnwerpers geplaatst. Resolutie A/59/91 (2004) van de Algemene Vergadering van de VN heeft uiteindelijk een gedragscode opgeleverd: de Hague Code of Conduct against Ballistic Missile Proliferation (HCoC). In de praktijk blijken de besprekingen in het kader van deze gedragscode muurvast te lopen zonder enige vorm van naleving of controle. Staten worden aangemoedigd om zich aan te sluiten en nieuwe wegen te ontwaren om op efficiënte wijze de proliferatie van ballistische raketten aan te pakken die in staat zijn om massavernietigingswapens af te leveren. Tot op de dag van vandaag zijn er geen internationale aanvaarde normen voor de controle op ballistische raketten. Ook hier zullen de grote kernmogendheden hun bereidwilligheid moeten tonen, vooraleer in deze materie vooruitgang te kunnen boeken. Ballistische raketten en andere vectoren zijn, vanuit geopolitiek en strategisch oogpunt, een gevoelige materie: niet alleen is het een probleem dat nauw verbonden is aan WMD-capaciteit, maar ook onderdeel uitmaakt van de conventionele slagkracht. Het zal dus zowel politieke moed als een gunstig (lees rustig) militair klimaat vergen vooraleer enige vooruitgang in dit kader kan geboekt worden. De polemiek omtrent het strategisch raketterschild is een bijkomende hindernis om in deze materie tot een vergelijk te kunnen komen.

Naast voornoemde internationale verdragen, zijn er exportcontroles voorzien voor export van materiaal gevoelig voor proliferatie: men dient in gedachte te houden dat toetreding tot deze regimes op vrijwillige basis gebeurt. Belangrijk om weten bij het beschouwen van de volgende export regimes is dat de vrijwillige deelname multilateraal wordt vastgelegd. Dit neemt niet weg dat op bilaterale basis overeenkomsten kunnen gesloten worden die totaal in strijd zijn met de overeenkomsten die vastgelegd werden in volgende comités.

Nuclear Suppliers Group (NSG): deze organisatie werd in 1975 in het leven geroepen na de Indiase kernwapentesten en telt actueel 45 leden. Deze zijn op informele basis overeengekomen om uitvoercontrole van nucleair materiaal toe te passen en aanrijking en verwerking van kernbrandstof aan grondige controles te onderwerpen. Bedoeling is te vermijden dat de technologie omtrent kernenergie misbruikt zou kunnen worden in een militair onderzoeksprogramma. Goedkeuring voor handel vereist eenparigheid van stemmen: deze periode lijkt cruciaal om de praktische uitvoering van de overeenkomst tussen de VS en India voor uitvoer van kernbrandstof al dan niet goed te keuren binnen NSG. Met de verplichtingen die voortvloeien uit het NPT in het achterhoofd, zou NSG wel eens de laatste garantie kunnen zijn om naleving van het NPT in de toekomst af te dwingen. In het kader van het akkoord tussen de VS en India is deze gelegenheid niet uitgebaat.

ZANGER Committee (ZC) ontwierp een lijst met materiaal dat door NPT-ondertekenaars enkel zou geëxporteerd worden onder toezicht van het IAEA en met strikte toepassing van beveiligingsmaatregelen.

Australia Group (AG) is een organisatie die gebaseerd is op vrijwillige deelname. Deze organisatie, opgericht in 1984, heeft zich specifiek toegelegd op de verbetering en harmonisatie van controle op export van chemische precursoren, micro-organismen en materiaal van tweeërlei aard dat gebruikt zou kunnen worden in chemische en biologische wapens.

Missile Technology Control Regime (MTCR) is eveneens gebaseerd op vrijwillige toetreding vanaf 1987. Het accent in deze organisatie is gelegd op de inperking van de verspreiding van vectoren: raketten en UAVs die een nuttige lading kunnen dragen van 500 kg of meer over een afstand van 300 km of meer. Twee categorieën worden in het kader van de ontwikkeling, productie en gebruik van deze technologie nagegaan. Een eerste categorie (Cat I) met volledige subsystemen zoals geleiding en propulsie. Een tweede categorie (Cat II) behelst de technologie van lading, propulsie, geleiding en propulsie voor systemen die een kleiner bereik hebben dan 300 km.

Voor de volledigheid vermelden we hier nog de Wassenaar Arrangement (WA), maar deze organisatie is opgericht in 1993 om ook op het vlak van conventionele en kleine wapens een exportcontrole tot stand te brengen.

Naast de verdragen en de exportcontroleregimes moeten volledigheidshalve specifieke initiatieven vermeld worden zoals:

- Het Proliferation Security Initiative (PSI) is een initiatief van de BUSH-administratie: het project werd gelanceerd op 31 mei 2003 en is gericht op het indijken van de proliferatie (door o.m. smokkel) van WMD en daaraan gerelateerd materiaal. Men kan hier niet echt over een organisatie of resolutie spreken, maar eerder over een engagement van alle (vrijwillig) deelnemende staten om hun eigen wetten in zake non-proliferatie te verstrengen en actief deel te nemen aan interdictieoperaties om transport van WMD materiaal en hun vectoren te onderscheppen. Deze (hoofdzakelijk) maritieme opdrachten worden uitgevoerd in samenspraak met de landen waar de schepen aan wal worden doorzocht. Een probleem blijkt te rijzen indien men de onderschepping van schepen wil uitvoeren in internationale wateren. De UN Convention on the Law of the Sea (UNCLOS) voorziet namelijk vrije doorgang van schepen. Deze doorgang mag enkel verhinderd worden door militaire schepen en schepen van de kustwacht in geval van vermoedelijke slavenhandel, piraterij, drugsmokkel of niet toegestane radio-uitzendingen m.a.w. zal men een schip dat inspectie weigert en niet onder de vlag vaart van een aan PSI-deelnemende natie ongestoord moeten laten¹⁴⁷. In de praktijk blijkt bovendien inspectie van gestapelde containers op volle zee een moeilijke en risicovolle onderneming. Interdictie in nationale wateren van een schip onder de vlag van een deelnemende natie blijkt dus wel mogelijk. Een legitieme vraag is of deze activiteiten relevante resultaten opleveren en of de kosten/baten analyse positief uitvalt. Het antwoord op deze vraag zal voor alle deelnemers slechts deels bekend zijn. Het geheime karakter van deze interdictieopdrachten levert géén overzichtelijke of duidelijke gegevens of verslagen. Resultaten werden ongetwijfeld geboekt om bijvoorbeeld leveringen naar Libië te verhinderen: men kan enkel raden naar het aantal succesvolle onderscheppingen van gevoelig materiaal. Misschien hebben inlichtingendiensten hier een beter zicht op. Men kan zich echter niet van de indruk ontdoen dat betrokken operaties slechts een klein gedeelte van alle illegale wapenhandel zou onderscheppen: alternatieven op zeetransport kunnen snel

¹⁴⁷ UNCLOS, Deel II, sectie 3, art 19 lijst de uitzonderingen die vrije toegang aan banden leggen. WMD worden hier niet in vermeld.

gevonden worden. In het verleden werden die reeds gebruikt: een deel van de transporten van het KHAN-netwerk werden per land of luchttransport ongehinderd tot bestemming gebracht. Een duidelijk wettelijk kader, bijvoorbeeld onder toezicht van de VN, met internationale samenwerking die zich niet enkel beperkt tot maritieme operaties zou hier misschien (nog) meer resultaat kunnen opleveren. Vooral met betrekking op alle ongeregistreerde radiologische bronnen uit Centraal-Azië zou een gecoördineerde actie in die richting moeten gevonden worden.

- VN-resolutie 1540 (S/RES/1540): deze resolutie werd gestemd op 28 april 2004 en is bindend voor alle lidstaten van de VN. Door deze resolutie verbinden de Staten zich ertoe om alles in het werk te stellen om proliferatie van WMD te verhinderen door strengere grenscontroles, export controles en toegespitste nationale wetgeving in dit kader. De resolutie is vooral gericht om niet-staatsactoren de toegang tot WMD materiaal te ontzeggen. Als praktisch hulpmiddel, werd door het IAEA een aantal technische brochures uitgegeven met betrekking tot de organisatie van controle op radiologisch materiaal in internationale transit (post, transport via weg of lucht)¹⁴⁸. Men dient er zich rekenschap van te geven dat sommige controlemiddelen zware investeringen vergen van landen die er niet altijd de mogelijkheid toe hebben. Bovendien kan men zich vragen stellen bij dergelijke opstellingen in de voormelde Centraal-Aziatische gebieden waar tal van omwegen het mogelijk maken om eventuele controles te omzeilen (gaande van fysieke afscherming van radiologische bronnen tot keuze van alternatieve transportroutes).

Na de basis, gelegd door resolutie 1540, werden nieuwe stappen gezet om een globale strategie en actieplan tegen terrorisme en CBRN-smokkel te ontwikkelen: het belang van indirecte CBRN-dreiging werd reeds aangehaald in een vorig gedeelte van dit werk. De resolutie 1540 liet toe om illegale smokkel van CBRN wapens officieel te erkennen als een nieuw risico voor proliferatie. In april 2005 stemde de VN de Internationale Conventie voor het verhinderen van Nucleaire Terroristische activiteiten. In dit kader worden lidstaten aangemoedigd om de technische aanbevelingen van het IAEA na te leven om radiologisch materiaal beter te beveiligen. Voor het eerst werd in dit opzicht de dreiging door de “vuile bom” naar voren geschoven. Een internationale structuur en een gecoördineerd actieplan waren dus noodzakelijk. Daarom werd op 8 september 2006 de Globale Anti-Terrorisme Strategie, onder de vorm van resolutie A/RES/60/288, met eenparigheid van stemmen goedgekeurd. In de aanloop van deze resolutie was reeds een tijdelijke structuur opgericht, die erkend werd door deze resolutie. Het organogram van vermelde structuur is terug te vinden in bijlage 9. Opmerkelijk is dat alle controleorganen van de VN opgenomen zijn in dit organogram. Centraal staat het Counter-Terrorism Implementation Task Force (CTITF) dat van WMD smokkel een centraal thema heeft gemaakt: ook UNICRI (het VN orgaan dat toezicht houdt op de bestrijding van criminele activiteiten op VN-niveau - hoofdkwartier in Turijn), is in dit orgaan vertegenwoordigd. Nationale contactpersonen van de Federale Politie zijn in beide organen actief. Voor UNICRI gebeuren de contacten zowel vanuit EUROPOL (Wenen) als INTERPOL (Lyon). Voor het CTITF gebeurt de uitwisseling door de Directie Criminaliteit tegen Personen-Centrale Dienst Terrorisme en Secten. De algemene trend ging meer en meer naar een toegespitste samenwerking tegen het gebruik van CBRN materiaal in criminele activiteiten. Concreet werd de nadruk gelegd op:

- informatieuitwisseling tussen naties en internationale organisaties.

¹⁴⁸ IAEA Nuclear Security Series N°2 t.e.m. 6 (Technical guidance reference manuals). Zie bibliografie.

- de ontwikkeling van een gestandaardiseerde analysemethode voor gebruik van CBRN materiaal zoals dat reeds gebeurde voor drugs- en wapensmokkel.
- verbetering van kennis en ervaring in de aanpak van smokkel van dit CBRN-materiaal en uitwisseling van ervaring en tactische analyses van de situatie. Een eerste initiatief was een analyse van de situatie aan de grensgebieden van de EU m.n de Euro-Aziatische regio.

Praktisch kan men vaststellen dat er nog hinderpalen zijn. De zo geprezen uitwisseling van informatie loopt niet altijd van een leien dakje: vooral indien een crimineel onderzoek is opgestart, kan de informatie heel traag doorvloeien om het lopende onderzoek niet in gevaar te brengen.

Op nationaal vlak is er het bijkomende probleem van de scheiding van verantwoordelijkheden. De autoriteiten die actief zijn in een onderzoek zijn gespreid over verschillende FOD's: grens- en immigratiecontrole, laboratoria, import en douaneaangelegenheden en beveiliging van kerncentrales zijn hier enkele voorbeelden van. Een coördinatie van alle betrokken diensten is van cruciaal belang om een adequate aanpak van de problematiek te verzekeren op nationaal niveau, laat staan op internationaal vlak. Niet alleen moet de informatie-uitwisseling mogelijk gemaakt worden tussen de verschillende nationale diensten (inter-FOD), maar zeker internationaal (bilateraal of multilateraal) moeten akkoorden afgesloten worden om informatie te laten doorstromen tussen verschillende overheidsdiensten over de landsgrenzen heen. Bijzonder voor een transitland als het onze, dat op het kruispunt ligt van alle lucht-, zee- en autoroutes van Europa, is snelle uitwisseling van informatie van cruciaal belang wanneer men op enkele uren tijd de wereld rond kan reizen. De concentratie aan internationale instellingen in onze hoofdstad vereist bovendien een efficiënte aanpak van deze problematiek. In dit verband kan men merken in het Counter Terrorism organogram van de VN dat zowel het IAEA (voor het radiologische/nucleaire) als de OPCW (voor het chemische) beproefde controlemechanismen in plaats hebben. Het biologische aspect in het CBRN acroniem blijft een probleem omwille van detectieproblemen: vaak wordt een incident ontdekt nadat mogelijke contaminatie is gebeurd. In dit geval biedt epidemiologisch onderzoek de enige oplossing om alle slachtoffers op te sporen en de bron van de besmetting te ontdekken. De wereldgezondheidsorganisatie (WHO) heeft snelle meldingssystemen, maar het fundamentele verschil van de B-problematiek t.o.v. het CRN-gedeelte ligt in het feit dat de ontdekking van een incident kan plaats grijpen, terwijl de besmetting reeds geruime tijd uitbreiding vindt. Dit is niet zo zeer het geval voor chemische/radiologische incidenten die (in het kader van terroristische activiteit) zeer gelokaliseerd zullen voorkomen.

Blikken we nog even terug naar de basis van de samenwerking tegen WMD terrorisme op niveau van de VN met name de UNCR1540, dan merken we dat alle staten aangespoord worden om adequate nationale wetgeving te voorzien om efficiënte aanpak van deze materie te voorzien. In het organogram dat de organen vastlegt in de strijd tegen het terrorisme (bijlage 9) vinden we organisaties zoals o.m. WHO, de Wereldbank, UNICRI, OPCW, IAEA, Dounae organisatie (WCO). In het kader van de aangehaalde moeilijkheden voor informatiestroom en informatieverwerking, zou het nuttig zijn om de nationale wetgeving in elk van de opgesomde domeinen op gestandaardiseerde criteria te laten functioneren die zowel de proactieve fase (informatiestroom, politieel onderzoek) als de gerechtelijke procedure (bewijsvoering en vervolging) zodanig behandeld worden, dat nationale wetgeving of uitzonderingsmaatregelen géén hinderpaal meer vormen voor internationale samenwerking. Dit is mogelijk gebleken in het kader van de vervolging voor oorlogsmisdaden voor het Internationaal Strafhof van Den Haag. Een gelijkaardige aanpak in het kader van terroristische WMD-activiteiten zou zowel de strafvordering als ook de behandeling van beschuldigen in de schijnwerpers plaatsen

van de internationale gemeenschap. Nationale uitzonderingsrechtbanken zonder internationale erkenning, of jarenlange opsluitingen zonder formele aanklacht zouden hierdoor tot het verleden kunnen behoren. Deze aanpak zou bovendien de formele beschuldiging van de internationale gemeenschap uit hoofde van de VN kunnen materialiseren en op die manier de steun doen afnemen die sommige staten geneigd zouden zijn te verlenen aan niet-staatsactoren.

2.2.2. EUROPESE UNIE

Het is niet onbelangrijk na te gaan hoe de strategie van de EU in zake WMD haar definitieve vorm kreeg: sinds 2003 werden diverse initiatieven in die zin opgestart. Op 13 Juni 2003 werd een document van het secretariaat van de Europese raad verspreid met als onderwerp “Action Plan for the Implementation of the Basic Principles for an EU Strategy against Proliferation of Weapons of Mass Destruction”¹⁴⁹. De belangrijkste ankerpunten in dit plan zijn de bestaande VN-verdragen en resoluties met betrekking tot WMD en terrorisme. Het actieplan werd op 20 Juni 2003 ondersteund door een politieke verklaring op initiatief van Javier SOLANA: in dit document¹⁵⁰ worden de dreigingen voor de EU geïdentificeerd (Terrorisme, proliferatie van WMD en vetoren, georganiseerde misdaad) en de strategische objectieven bepaald nl.

- Uitbreiding van een veiligheidszone rond Europa met als voorbeeld de inzet in de beveiliging van de Balkan.
- Versterking van de internationale orde gebaseerd op het charter van de VN en de bestaande verdragen. In het kader van de strijd tegen proliferatie, legt de Raad de nadruk op de universele ratificatie en naleving van ontmantelings- en non-proliferatieverdragen. Indien nodig zal men ijveren naar een strengere toepassing van deze overeenkomsten.
- Het hoofd bieden aan de nieuwe bedreiging (o.m. terrorisme en proliferatie) in de wetenschap dat zuiver militaire actie geen oplossing kan bieden, dat samenwerking met meerdere partners noodzakelijk kan zijn en dat de eerste verdedigingslijn soms ver buiten Europa in plaats gesteld zal moeten worden.

De EU strategie tegen de proliferatie van WMD werd gepubliceerd op 10 december 2003¹⁵¹. De motivatie luidt dat alle vormen van WMD-proliferatie een bedreiging vormen voor de EU, maar ook de proliferatie van vectoren krijgt specifieke aandacht (UAV's inclusief). De beschikbaarheid van deze middelen voor niet-staatsactoren zou een directe bedreiging vormen voor de EU: naast de stoffelijke schade en het massale aantal slachtoffers, zou dit leiden tot de ontwrichting van de samenleving. Als antwoord op deze dreiging moet een doeltreffend multilateralisme als sluitsteen fungeren voor de Europese strategie: deze is gebaseerd op de bestaande verdragen (zoals expliciet vermeld in 14310/03 van de Raad, worden hieronder verstaan het NPT, de bijkomende protocols van het IAEA, de CWC, de BTWC, HCoC en ten slotte CTBT) en de ondersteuning van bestaande controleorganisaties (IAEA, OPCW). De EU stelt voor om politieke, financiële en technische steun te verlenen aan inspectie en export controle. In geval van betwisting, belichaamt de VN, voor de EU, de scheidsrechter die de uiteindelijke accreditatie moet geven omtrent de naleving van de bestaande verdragen. Als randbemerking moeten we hier de aandacht vestigen op het feit dat zelfs de VN, ondanks het feit dat ook vectoren betrokken worden in de EU-strategie, nog niet ver gevorderd is op het vlak van de beheersing

¹⁴⁹ 10354/1/03 REV 1 d .d. 13 June 2003.

¹⁵⁰ SOLANA, J., A secure Europe in a better world. EUROPEAN COUNCIL, Thessaloniki, 20 June 2003.

¹⁵¹ 15708/03 d .d. 10 december 2003

van de proliferatie in dit domein. De Europese strategie beschouwt de bestaande internationale verdragen als startpunt voor verdere actie: in het kader van de proliferatie van raketten (en andere vectoren zoals UAV's) is reeds vermeld dat de onderhandelingen in het kader vastgelopen zijn. De actuele problematiek omtrent het Amerikaans raketschild zal hiervan ongetwijfeld één van de oorzaken zijn. Dat neemt niet weg dat, zoals voor het NPT, géén akkoord ter zake kan bereikt worden indien de kernmachten niet in de eerste plaats overeenkomen: deze situatie geeft een vrijgeleide aan die Staten die, al dan niet ondertekenaar van de verdragen in kwestie, hun weg willen verder zetten op de weg van proliferatie van zowel WMD als hun vectoren.

Hoe de strategie in praktijk dient omgezet te worden komt in hetzelfde document aan de orde. Vooreerst dient multilateralisme efficiënter te worden door een resolute aanpak van proliferatoren. Hiervoor worden zes instrumenten naar voren geschoven:

- Streven naar een universele aanvaarding (en strengere toepassing indien nodig) van bestaande verdragen.
- Bevestiging van de VN-veiligheidsraad in haar rol, met eventuele bijdrage aan expertise teneinde de omzeiling van non-proliferatie in te dijken.
- Politieke, financiële en technische steun verschaffen aan controlesystemen.
- Versterken van exportcontrole in een kader van Europese samenwerking.
- Beveiliging van gevoelig materiaal tegen ongeoorloofde toegang of diefstal.
- Strengere identificatie, controle en interceptie van smokkel in WMD materiaal.

Verder wil men streven naar een stabiele internationale context, samenwerken met de VS en andere bondgenoten. Ten slotte wil de EU de nodige structuren uitwerken om deze doelen te bereiken.

De opvolging van deze strategische doelstellingen wordt nauwgezet toegepast: halfjaarlijkse verslagen peilen naar de uitvoering, mankementen, en noodzakelijke fondsen om de uitgeschreven doelen te bereiken of bij te sturen¹⁵². Hiernaast wordt regelmatig een geactualiseerde lijst met prioriteiten gepubliceerd¹⁵³. De laatste versie van dit verdrag legt de nadruk op de bestaande VN verdragen als basis voor iedere samenwerking in het kader van non-proliferatie. In het vooruitzicht van 2010, zal de aandacht speciaal gevestigd worden op de groeiende belangstelling voor kernenergie als alternatieve energiebron. Zoals uitgelegd in deel I van dit werk kan dit probleem een impliciete bedreiging vormen voor proliferatie. Dit energetisch project moet dus kaderen in een strategie van non proliferatie en nucleaire veiligheid (waaronder zowel de termen “security” als “safety” worden benadrukt, welke in het Nederlands enkel door die ene term “veiligheid” worden omschreven). Ook de horizontale (toenemend aantal bezitters) en verticale proliferatie (toename van het aantal tuigen voor één bezitter) zal een blijvende bezorgdheid zijn voor de EU, welke onder meer in de onderhandelingen met Iran en Noord-Korea, zich zal blijven inzetten om tot een billijk vergelijk te komen. In het kader van de proliferatieactiviteiten van niet-staatsactoren blijft de EU zich scharen achter de standpunten weergegeven in UNSCR 1540¹⁵⁴ om toegang te ontzeggen tot zowel WMD als vectoren: in dit kader blijft de dreiging van illegale smokkel zeer actueel. Specifieke mechanismen zijn vereist om illegale financiële netwerken te ontrafelen en op te doeken in het kader van deze problematiek.

¹⁵² Verslagen 10448/04 van 10 juni 2004, 15246/04 van 03 december 2004, 9898/05 van 08 juni 2005, 14520/05 van 05 december 2005, 10527/06 van 14 juni 2006, 16694/06 van 12 december 2006, 5184/07 van 09 januari 2007, 11024/07 van 19 juni 2007, 16411/07 van 11 december 2007, 10744/08 van 17 juni 2008.

¹⁵³ Laatste in datum is 10747/08 van 17 juni 2008 (prioriteiten van 2008-2010).

¹⁵⁴ Opgevolgd door UNSCR 1673 en 1810.

Bovenop vermelde initiatieven die kaderen binnen de EU WMD-strategie, is de Raad ook actief om initiatieven op te starten ter ondersteuning van VN verdragen, die de pijlers vormen voor de strijd tegen proliferatie van WMD. Door middel van “Joint Actions” worden lidstaten aangemoedigd om zich te scharen achter de waarden en afspraken die in de verdragen afgesproken worden. Concreet worden op EU-niveau de principes geïmplementeerd die men in de VN heeft vastgelegd: kennis, financiering, uitrusting en mankracht worden gemobiliseerd om de doelstellingen te bereiken die de Raad werden vastgelegd. Een bondig overzicht in voetnoot¹⁵⁵ geeft een idee waarin de lidstaten van de EU in dit kader concrete afspraken hebben.

Naast deze concrete inzet zijn er de werkgroepen actief die het voorbereidende werk uitvoeren voor de ministeriële beslissingen in zake ontwapening en non-proliferatie: de voorbereidingsorganen op de vergaderingen in deze materie dragen de namen CODUN en CONOP. Deze vergaderen maandelijks en zijn samengesteld uit vertegenwoordigers van Ministeries van Buitenlandse Zaken van de lidstaten. Hoewel de mandaten van deze werkgroepen overlappen, kan men zeggen dat CODUN (Working Group on Global Arms Control and Disarmament) zich vooral toespitst op de problematiek van de CWC, BTWC, CTBT, kleine wapens en landmijnen. CONOP (Working Group on Non-Proliferation) is meer toegespitst op non-proliferatie, naleving van het NPT en exportcontrole met inbegrip van bijstand aan Rusland voor de vernietiging van chemische wapens. Men dient hier de randbemerking te maken dat deze organen geen beslissende macht hebben: besluiten worden voorgelegd aan de “General Affairs Council” (GAC) dat zich op ministerieel niveau (representatie van buitenlandse zaken) situeert. Het is één van de besluitvormende configuraties van de Raad van de EU. Men dient zich er rekenschap van te geven dat alle beslissingen voorbereidend werk vereisen: alle activiteiten en coördinatie voor beslissingen van de Raad worden uitgevoerd door het “Permanent Representatives Committee” (COREPER), de permanente vertegenwoordiging van de lidstaten.

Naast de vermelde initiatieven en opvolging werd op 12 december 2006 een document gepubliceerd¹⁵⁶ dat de basis moest leggen om een betrouwbare uitvoering van de EU strategie tegen proliferatie van WMD te garanderen: hiervoor werd het WMD-Monitoring Centre (WMD-MC) in het leven geroepen. Belangrijkste einddoelen van dit orgaan in de strijd tegen WMD-proliferatie bestaan erin de efficiëntie en de betrouwbaarheid van de aanpak te verbeteren zonder enige wijziging in de institutionele structuur te induceren. De werkmethode is gebaseerd op samenwerking tussen enerzijds het secretariaat van de secretaris-generaal van de Raad van Ministers en Hoge Vertegenwoordiger voor het Buitenlands- en Veiligheidsbeleid van de EU, en anderzijds de Commissies en Lidstaten. Taken van dit Centrum zijn:

- Dagelijkse opvolging van de WMD strategie.

¹⁵⁵ WHO: [Council Joint Action 2008/307/CFSP of 14 April 2008](#) ;
BTWC: [Council Joint Action 2006/184/CFSP of 27 February 2006](#) ;
CTBTO: [Council Joint Action 2008/588/CFSP of 15 July 2008](#), [Council Joint Action 2007/468/CFSP of 28 June 2007](#), [Council Joint Action 2006/243/CFSP of 20 March 2006](#) ;
IAEA: [Council Joint Action 2008/314/CFSP of 14 April 2008](#), [Council Joint Action 2007/753/CFSP of 19 November 2007](#), [Council Joint Action 2006/418/CFSP of 12 June 2006](#), [Council Joint Action 2005/574/CFSP of 18 July 2005](#), [Council Joint Action 2004/495/CFSP of 17 May 2004](#) ;
OPCW: [Council Joint Action 2007/185/CFSP of 19 March 2007](#), [Council Joint Action 2005/913/CFSP of 12 December 2005](#), [Council Joint Action 2004/797/CFSP of 22 November 2004](#) ;
UNSCR 1540: [Council Joint Action 2008/368/CFSP of 14 May 2008](#), [Council Joint Action 2006/419/CFSP of 12 June 2006](#)

¹⁵⁶ 16694/06 van 12 december 2006.

- Verder ontwikkeling van de WMD non-proliferatie strategie.
- Coherentie ontwikkelen in ondersteuningsprogramma's (Joint Actions).
- Fungeren als contactpunt met derden (Staten en organisaties).

Voor de goede werking is het belangrijk een centraal werkorgaan in dit centrum te voorzien: deze functie wordt voor het ogenblik waargenomen door de Persoonlijke vertegenwoordiger (PR) van de Hoge Vertegenwoordiger voor het Buitenlands- en Veiligheidsbeleid van de EU, Mevr.A.GIANELLA. De eerder vermelde CODUN en CONOP blijven als kader fungeren voor interactie tussen lidstaten en het WMD Center. In het vooruitzicht van herzieningen van non-proliferatieverdragen worden "Ad hoc Task Forces" ingeschakeld om het voorbereidende werk doen (in het vooruitzicht van de NPT herzieningsconferentie van 2010 enerzijds en de BTWC herzieningsconferentie van 2011 anderzijds). Hiernaast moet de structuur aangevuld worden met een pool van deskundigen om coöperatie en bijstandsoperaties te leiden. Informatievergaring kan nog steeds gebeuren door het "EU Joint Situation Centre of the Council (SitCen)". Nauwe samenwerking met de Coördinator Terrorismebestrijding¹⁵⁷ is eveneens van cruciaal belang. In de praktijk worden reeds op regelmatige basis vergaderingen gehouden op twee niveaus:

- Het Secretariaat van de Commissie (maandelijks). Zo heeft de vergadering van 8 juli 2008 o.m. het probleem van multilaterale aanpak van kernbrandstofvoorziening voorbereid alsook de opvolging van het "Joint Actions" programma.
- WMD-Center met lidstaten (per trimester maar op te voeren). In dit kader werden ook nationale vertegenwoordigers aangeduid. De vergadering van 29 februari 2008 behandelde o.m. de problematiek van de functies van de task-force op CBRN niveau. Een document van de Commissie zal deze taken expliciteren. De Belgische contactpersoon in het Centrum werd gekozen uit FOD Buitenlandse Zaken. In deze materie is het echter merkwaardig dat Defensie niet aangesproken wordt om deze taak (eventueel als ondersteuning) uit te voeren. Ervaring van militairen die werkzaam zijn binnen de NAVO-organen in het domein van de CBRN problematiek zouden hier zeker een bijkomende meerwaarde kunnen opleveren. Met betrekking van deze problematiek is het verslag van de vergadering duidelijk: men laat de beslissing over aan de lidstaten om te bepalen wie het best in aanmerking komt om deze functie in te vullen.

Op het vlak van CBRN bescherming werd, in navolging van een CBRN implementatieprogramma¹⁵⁸, strategische objectieven bepaald die geactualiseerd werden na de aanslagen van Madrid op 11 maart 2004. Het groenboek van de Commissie¹⁵⁹ betreffende bioveiligheid werd de aanzet voor de aanpak te volgen in 2008 en 2009: CBRN risico's moeten het aspect veiligheid (safety) omvatten, zowel in het kader van preventie van ongelukken, pandemieën of natuurlijke rampen, als ook in het kader van bescherming tegen opzettelijke acties (security). Ook de strategische doelen werden in deze evolutie aangepast:

- Dreigings- en risicoanalyse: inschatting van het risico blijft een nationale aangelegenheid. Nochtans worden lidstaten aangemoedigd om meer gestructureerd gebruik te maken van de dreigingsanalyses die geleverd worden door SitCen en EUROPOL. In het kader van de biopreventie en de inperking van

¹⁵⁷ Mr.G.de KERCKHOVE

¹⁵⁸ 2002 CBRN Programme met aanpassing in 2004 (15480/04) en 2005 (8988/05).

¹⁵⁹ 11951/07 van juli 2007.

de impact op volksgezondheid werd het European Centre for Disease Prevention and Control (ECDC) te Stockholm opgericht¹⁶⁰.

- Preventie en beperking van risico en kwetsbaarheid: hiermee doelt men op de preventieve ontzegging van WMD materiaal aan terroristen (zoals voorzien in het actieplan terrorisme), maar ook de bescherming van kritische infrastructuur welke hiermee een eigen project krijgt. Teneinde uitwisseling van informatie over dreiging en kwetsbaarheden aan te pakken is een netwerk noodzakelijk: het Critical Infrastructure Warning Information Network (CIWIN) heeft hiervoor vandaag de opdracht.
- Monitoring, identificatie van gebruikte agentia en melding: bestaande snelle waarschuwingssystemen kunnen een waargenomen dreiging onmiddellijk doorgeven¹⁶¹. In dit kader werd door het ECDC te Stockholm een beveiligd IT-netwerk (EWRS- zie voetnoot 161) in gebruik genomen voor de snelle verspreiding van analyse van een sanitaire dreiging voor de volksgezondheid op EU- en op nationaal niveau. Op 4 maart 2008 werd een Emergency Operations Centre (EOC) in gebruik genomen dat de klok rond de nodige middelen inzet om partners op de hoogte te houden van lopende crisissen.
- Operationaliteit en beheer van de respons: onderlinge hulpverlening vereist interoperabiliteit van burgermiddelen voor onmiddellijk inzetbare hulp. Bovendien moeten opleidingen en oefeningen in dit kader voorzien worden. Correcte informatie van de bevolking is hier van essentieel belang en behoort tot de bevoegdheid van de lidstaten.
- Research and development: het onderzoeksprogramma horizon 2013 moet ook in het domein van de gevolgen van een terroristische aanslag een luik “EU Veiligheidsonderzoeksprogramma” omvatten hetgeen tot uiting komt in het lopende ESRP-programma (European Security Research Program: 7th Research Framework Programme). Dit voorziet onderzoek naar bescherming tegen conventionele springladingen en niet-conventionele CBRN aanslagen.
- Internationale samenwerking: dit domein behelst zowel uitwisseling van informatie als rechtstreekse samenwerking met bijvoorbeeld Rusland (EMERCOM) tijdens kernrampen.
- Algemene coördinatie: de uitvoering van vermelde maatregelen wordt opgevolgd door de Commissie en de lidstaat die het voorzitterschap waarneemt.

¹⁶⁰ De reglementering omtrent de werking is beschikbaar op http://ecdc.europa.eu/About_us/Key_Documents/ecdc_regulations.pdf Een waarnemings- en rapporteringsstrategie horizon 2013 is beschikbaar op volgend adres <http://ecdc.europa.eu/>

¹⁶¹ Enkele voorbeelden: MIC (Civil Protection Monitoring and Information Centre: een waarschuwingssysteem om wederzijdse hulp sneller op gang te brengen tussen lidstaten in geval van ernstige noodgevallen); ECURIE (European Community Urgent Radiological Information Exchange: informatienetwerk bij radiologische noodgevallen: nationale POC is FANC); BICHAT (program for cooperation on preparedness and response to Biological and Chemical Attacks: waarschuwingssysteem voor biologische en chemische dreiging en aanval aangevuld met het mondiaal medisch waarschuwingssysteem MedISys); RAPEX (Rapid Exchange of Information of alarmeringssysteem voor consumptiegoederen die niet voedsel gebonden zijn: FOD Economie is nationaal POC); RASFF (Rapid Alert System for Food and Feed databank voor voedselgebonden gezondheidsrisico's: Federaal Agenstchap voor Voedselveiligheid is nationaal POC); EWRS (Early Warning and Response System voor besmettelijke ziekten: FOD Volksgezondheid is nationaal POC); EUROPHYT (phytosanitaire databank: Federaal Agenstchap voor Voedselveiligheid is nationaal POC); SHIFT (databank voor veterinaire gezondheidscontrole met het oog op import: Federaal Agenstchap voor Voedselveiligheid is nationaal POC); ADNS (Animal Disease Notification System: Federaal Agenstchap voor Voedselveiligheid is nationaal POC); ARGUS (General Rapid Alert System: intern netwerk voor verspreiding van informatie binnen de directies en diensten van de Commissie bij het voorkomen van een crisis).

De invulling van de beschikbare middelen om deze opdrachten uit te voeren is terug te vinden in het “CBRN Inventory”¹⁶²: de wettelijke instrumenten voor deze invulling worden per onderdeel hernomen in bijlage 10. Opmerkelijk in dit verband is dat ook hier in de allereerste instantie de nadruk gelegd wordt op dreigings- en kwetsbaarheidsanalyse met daaropvolgende risico-evaluatie zoals werd vastgesteld in het gedeelte indirecte CBRN dreiging (nationale infrastructuur) eerder in dit werk. Het essentiële verschil is dat een lijst van kritische infrastructuur in Europese context opgesteld wordt vanaf een vooraf overeengekomen definitie¹⁶³. Na een eerste ontwerp gepubliceerd in het groenboek betreffende een Europees programma voor de bescherming van kritische infrastructuur¹⁶⁴, werd in december 2006 een voorstel tot richtlijn uitgebracht¹⁶⁵. Hoewel dit document 11 kritische sectoren (waarvan 29 subsectoren) voorzag, met een legale, financiële en logistieke ondersteuning voor wat de bescherming betreft, heeft de uiteindelijke richtlijn¹⁶⁶ een ernstige afslanking ondergaan: slechts twee sectoren (energie en vervoer) blijven overeind. De richtlijn voorziet een leidraad voor de lidstaten om de inventarisatie van de kritische infrastructuur uit te voeren. Bovendien zal een effectbeoordeling uitgevoerd worden, waarna geëvalueerd zal worden of andere sectoren (zoals ICT) onder de richtlijn moeten vallen. In die context is de Anti-Terrorisme Strategie van 2005¹⁶⁷ een belangrijk document: de strategische inzet tegen terroristische activiteit wordt hierin gebaseerd op vier pijlers nl. interdictie, bescherming, vervolging en interventie. Pijler 2 (bescherming), verwijst uitdrukkelijk naar de essentiële noodzaak om de gevoeligheid van de Europese Kritische Infrastructuur ten aanzien van fysische en elektronische aanvallen te beschermen. Ook in dit kader wordt de nadruk gelegd op de non-proliferatie van CBRN materiaal omwille van (in)directe bedreiging. Omwille van de vermelde noodzaak in de relevante documenten, en zoals de praktijk heeft uitgewezen in Estland en meer recent in de conflictgebieden van de Kaukasus, is het duidelijk dat ICT duidelijk in de te beveiligen sectoren dient opgenomen te worden.

Men kan zich vragen stellen rond de grote dispariteit van waarschuwingssystemen (voetnoot 161): de eigenschappen van elke discipline zorgt de facto voor een geëigend transmissiekanaal voor informatieverwerking. Principieel kan men hier weinig aan veranderen. Op het gebied van de integratie van de informatie en de gebruikte hardware voor de verspreiding van de berichten is er echter mogelijkheid tot vereenvoudiging. Het moet zeker mogelijk zijn om één enkel systeem te gebruiken om al de informatie te laten doorstromen naar de voorziene gebruiker. In dit domein kan ook de nationale uitbating van de voorziene transmissiekanaalen zeker verbeterd worden: zo kan men zich de vraag stellen welke systemen principieel integraal deel zouden moeten uitmaken van het CGCCR. Voor het ogenblik zijn dat enkel de systemen Bichat, MIC en ECURIE. Als bemerking moet men hier toevoegen dat enkel ECURIE over een eigen transmissiekanaal beschikt in het kader van radiologische incidenten. Bichat en MIC opereren via Internet, wat het belang onderstreept van de beveiliging van ICT capaciteit. Ook hierdoor is het een vanzelfsprekende noodzaak om ICT toe te voegen aan de domeinen die gedefinieerd worden als kritisch en te beveiligen. Andere vermelde

¹⁶² 10382/08 van 05 juni 2008, Inventory of EU instruments relevant for addressing chemical, biological, radiological and nuclear risks (“CBRN Inventory”).

¹⁶³ In tegenstelling tot de CriViSen-databank.

¹⁶⁴ COM 2005. Uitgangspunten van het European Program for Critical Infrastructure Protection (EPCIP).

¹⁶⁵ COM 2006/0276, Proposal for a directive of the council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

¹⁶⁶ 9403/08 van 22 juni 2008.

¹⁶⁷ 14469/4/05 van 30 november 2005 van de coördinator antiterrorisme.

systemen komen niet rechtstreeks toe in het CGCCR-knooppunt: ECDC alarmering bijvoorbeeld vindt haar weg via de FOD Volksgezondheid. Op zich is dit een logische waarschuwingsketen. Men kan zich echter wel afvragen of de waarschuwing niet in parallel zou kunnen gebeuren om de vertraging van de doorstroom van informatie tegen te gaan. Bovendien zou dit een garantie geven dat bij uitval van één systeem een back-up voorzien is die de centralisatie van de gegevens toch nog toelaat.

Met het oog op het testen van de (CBRN) operationaliteit, worden op regelmatige basis grootschalige oefeningen gehouden in internationale context: EUDREx 2004 (Wiener Neustadt-Oostenrijk), EURATECH 2005 (Portes-lès-Valence-Frankrijk), BIOTECT 2006 (Kopenhagen-Denemarken). Daarnaast worden, in het kader van de Europese defensiepolitiek, nog zuiver militaire oefeningen gehouden (MILEX 2007 en 2008) als ook CME/CMX¹⁶⁸ oefeningen. Dit oefeningenbeleid is merkwaardig in die zin dat men een totaal verschillende aanpak merkt met wat er op nationaal vlak georganiseerd wordt: richten we de aandacht enkel op de CBRN-oefeningen die in realistische scenario's worden uitgevoerd (actieve treinstations, luchthavens, etc.) dan kan men merken dat er tussen 2004 en 2006 reeds drie oefeningen werden georganiseerd bovenop de table-top oefeningen (al dan niet militair van aard).

2.2.3. NAVO

Binnen de NAVO zijn twee elementen die de aandacht trekken met betrekking tot CBRN aangelegenheden. Enerzijds is er de strijd tegen proliferatie en anderzijds de hulpverlening/inzet van operationele capaciteit in CBRN-omgeving (conflicten of incidenten). Alle relevante organen met betrekking tot deze problematiek worden weergegeven in het organogram in bijlage 11. De acroniemen en een korte beschrijving van betrokken groep worden verklaard in bijhorende aanhangsels.

Controle op het vlak van proliferatie gebeurt in de “Senior Defense Group on Proliferation” (DGP): dit is het hoogste NAVO-adviesorgaan met betrekking tot proliferatie van WMD en vectoren. Dit orgaan voorziet beleidsondersteuning (aanbevelingen) voor NAC en volgt de uitvoering van de besluitvorming op in zake respons op proliferatie. Sinds de NAVO-top van Praag (2002), werd een meerwaarde gecreëerd voor alle CBRN-bodies met name diegene voor operationele inzet. Onder meer met het “BRONSON-initiatief” werden concrete voorstellen gedaan om de CBRN-capaciteit aan te vullen. Concreet waren de doelstellingen vastgelegd in een multinationale capaciteit voor:

- Een ontplooibaar analytisch laboratorium ter identificatie van CBRN agentia ten velde.
- Een Assessment Team dat CBRN-incidenten kan evalueren en NAVO-bevelhebbers inlichten en ondersteunen.
- Opdrijven van de CBRN-opleiding.
- NATO Biological and Chemical Defense virtual stockpile beschikbaar voor leden van de Alliantie en bedoeld om snel ingezet te worden in het strijdperk.
- een Disease Surveillance system welk voornamelijk informatie zou vergaren omtrent het uitbreken van onverwachte ziektehaarden.

¹⁶⁸ CME/CMX bedoeld op civiele en militaire samenwerking. Oefeningen werden gehouden van 2002 t.e.m. 2004. De eerste militaire oefening werd gehouden in november 2005 (MILEX 05).

De realisatie van deze doelstellingen is deels uitgevoerd. Wat het analytische laboratorium betreft, is er o.m. Hongaarse capaciteit voor de identificatie van agentia. Men kan echter vaststellen dat hier dezelfde problematiek rijst als voor de behandeling van nationale noodplanning CBRN nl. de ontplooibare labs ofwel chemisch ofwel biologische agentia identificeren, maar dat geïntegreerde aanpak ontbreekt. Ofwel dient men zoals voor de nationale oriëntatielaboratoria, een projecteerbare capaciteit te voorzien, of alternatief is een laboratorium vereist dat het volledige spectrum aan CBRN agentia kan scheiden en identificeren.

In juli 2004 bereikt het “NATO multinational CBRN defence battalion”, waarvoor eveneens in Praag initiatief was gestart, operationele capaciteit. Het werd vervangen door het “Combined Joint CBRN Defence Task Force”. Deze “Task Force” moet NBC-verkenning kunnen uitvoeren, maar ook de identificatie van agentia. Biologische detectie en monitoring is ook één van haar kerntaken. Uiteindelijk moet dit uitmonden in aanbevelingen voor NAVO bevelhebbers. Decontaminatie-opdrachten moeten eveneens kunnen uitgevoerd worden. Normaliter wordt deze eenheid ingebed in de snelle interventiemacht van de NAVO: “NATO Response Force” (NRF) voorziet de snelle ontplooiing in het kader van ontluikende crisissen in opdracht van de Alliantie. De “Task Force” kan echter eveneens ingezet worden ter ondersteuning van burgers in NAVO lidstaten (wat is gebeurd in 2004 voor de Olympische spelen van Athene). Men stelt dus vast dat ook het “Assessment Team” vorm heeft gekregen onder deze benadering. Indien men deze taken overloopt kan men echter niet ongaan aan het feit dat de biologische detectie en monitoring waarover sprake nog in kinderschoenen staat: actueel is geen enkel toestel op de markt beschikbaar dat in “real time” betrouwbare informatie kan verschaffen omtrent de aanwezigheid van biologische agentia. Enkel microscopische deeltjes kunnen een alarm genereren om vervolgens aan analyse onderworpen te worden. Deze procedure geeft aanleiding tot valse meldingen en kan dus nog niet operationeel ingezet worden. Biologische detectie is dus nog de zwakke schakel in het spectrum van de CBRN detectie.

In juli 2007 werd de CBRN opleiding herzien door de oprichting van het “Joint CBRN Defence Centre of Excellence” in Vyskov (Tsjechië). Dit centrum is het forum voor uitwisseling van kennis en informatie omtrent de CBRN-opleiding van de verschillende NAVO-lidstaten: interoperabiliteit, training en oefening in internationale context, ontwikkeling van doctrines en standaardprocedures vormen de kerntaak van dit centrum.

Het NATO Weapons of Mass Destruction Center (WMDC NATO HQ-Evere) werd opgericht in mei 2000. De voornaamste taak van dit orgaan is de coördinatie te verbeteren omtrent WMD gerelateerde activiteiten, overleg in zake non-proliferatie en ontwapening te bevorderen. Bovendien moet het kunnen bijdragen tot militaire CBRN operationaliteit i.e. bijdragen tot de weerbaarheid t.o.v. een CBRN dreiging (voorbereiding) of opereren in CBRN omstandigheden (taken uitvoeren na een aanval). Dit vereist een permanente capaciteit tot aanpassing aan de gegeven omstandigheden. Men kan zich hier de vraag stellen of geen nauwere samenwerking mogelijk is met het EU-WMD Center (zie hoger). Men kan begrijpen dat een afzonderlijk, politiek en militair luik belangrijk blijven, maar gecoördineerde samenwerking met het EU WMD-Centrum lijkt een uitgelezen kans om de verschillende taken beter op elkaar af te stemmen en uitwisseling van informatie te verbeteren. Bovendien zou het toelaten om meer landen te betrekken bij de WMD problematiek vooropgesteld dat deze bilaterale consultaties met betrekking tot WMD tussen EU en NAVO geen eenzijdige vertegenwoordiging blijken van individuen maar een volwaardige en gemandateerde vertegenwoordiging belichamen. In een dergelijk kader zou de samenwerking EU-NAVO, althans wat de WMD problematiek betreft, vlotter kunnen verlopen. Het resultaat moeten officiële en gecoördineerde

standpunten zijn met politieke (EU WMDC) en militaire actiepunten (NAVO WMDC) die op te volgen zijn met vooropgestelde streefdata.

Hoewel voor het vooropgestelde Disease Surveillance system geen officiële NAVO-body de invulling van de verwachting realiseert kan men afleiden, uit wat vooraf werd behandeld, dat er raaklijnen te vinden zijn met de taken van het ECDC. Dit orgaan kan zeker deels de verwachtingen van de vooropgestelde NAVO-doelstellingen invullen. Vraag is of men naar Amerikaans voorbeeld zowel een burgerlijke als een militaire instantie nodig heeft om deze taak in te vullen. Indien de verantwoordelijkheden beperkt blijven zoals nu vastgelegd, lijkt het ECDC ruimschoots voldoende om tegemoet te komen aan de verwachtingen, wat mogelijkheden zou bieden om militaire specialisaties meer te richten naar andere operationele behoeften. In geval van samenwerking zullen duidelijke afspraken en structuren/communicatiekanalen moeten afgestemd worden op elkaar. Liaison van nationale vertegenwoordigers in de materie, militairen en burgers, zullen nodig zijn om de informatiestroom in goede banen te leiden. Daarom is een voorstel om alle bioveiligheidscoördinatoren (zowel burgers als militairen), te laten registreren bij het ECDC met als bijkomende taak de gecoördineerde nationale rapportage naar de centrale cel die het ECDC zal vertegenwoordigen. In dat opzicht lijkt het ECDC de ideale instantie om op het Europees continent als collector te dienen voor alle informatie die van het nationale niveau naar het WHO moet transiteren en omgekeerd. CDC Atlanta kan diezelfde functie waarnemen voor het Amerikaanse continent.

Hulpverlening bij rampen (nood- en interventieplanning), blijft een nationale verantwoordelijkheid, maar de NAVO heeft veel inzet getoond om zich over het probleem “civil emergency planning¹⁶⁹” te buigen om een gecoördineerde aanpak te garanderen: het belangrijkste orgaan (onder NAC) dat de besluitvorming in handen heeft is het Senior Civil Emergency Planning Committee (SCEPC). In de nasleep van de aanslagen van 11 september 2001, werd in Praag een Civil Emergency Action Plan goedgekeurd: hierin wordt voorgesteld om een catalogus van alle beschikbare nationale middelen op te stellen in het kader van hulpverlening. Bovendien werden oefeningen voorzien om de interoperabiliteit in dit domein ook te toetsen en eventueel te verbeteren. In april 2005 werd door SCEPC een aangepast actieplan goedgekeurd om de inspanningen ook te laten gelden tijdens en na terroristische CBRN aanslagen¹⁷⁰. In dit plan wordt o.m. aandacht besteed aan de bescherming van kritische infrastructuur en hulpverlening aan slachtoffers. De operationele entiteiten voor burgerlijke noodtoestanden zijn het Euro-Atlantic Disaster Response Coordination Center (EADRCC) en het Euro-Atlantic Disaster Response Unit (EADRU). Daar waar EADRCC voornamelijk een verzamelpunt voor informatie en een coördinatieorgaan voor de hulpverlening betreft, is het EADRU een multinationale smeltkroes van burgers en militairen die door de NAVO vrijwillig ter beschikking gesteld kan worden in noodgevallen ten gevolge van natuurlijke of terroristische calamiteiten. In afwachting van een officieel rapport van SCEPC betreffende de CBRN respons capaciteit van de NAVO, moet men zich beperken tot een informeel onderzoek van de capaciteiten. De NAVO-top van Boekarest (lente 2008) zou het bewuste rapport uitbrengen: de agenda heeft er anders over beslist. Bedoeling is niet enkel de capaciteiten op een rijtje te zetten, maar ook de mankementen aan het licht te brengen. Meer bepaald zou er nog een tekort zijn aan samenwerking tussen de burgerentiteiten en de militaire instanties. In het

¹⁶⁹ Civil Emergency Planning is binnen NAVO, zoals aangegeven in het document 166 CDS 06 (E)-NATO Parliamentary Assembly, veel ruimer op te vatten dan wat men nationaal met nood-en interventieplanning bedoelt

¹⁷⁰ Updated Action plan for the Improvement of Civil Preparedness for possible CBRN terrorist attacks.

vooropgestelde kader is een gemeenschappelijke planning nodig: deze planning moet gezamenlijk inge oefend worden om gezamenlijk het hoofd te kunnen bieden aan noodsituaties als die zich voordoen.

Men kan opmerken dat we hier tot exact dezelfde conclusie komen als diegene met betrekking tot de hulpverlening op nationaal niveau: ook hier zijn militaire elementen voorzien voor de hulpverlening als steun aan de bestaande burgermiddelen, maar een gebrek aan coördinatie en training op het terrein zorgen voor operationele beperkingen die zich kunnen laten voelen wanneer de nood het hoogst is¹⁷¹. Het essentieel verschil tussen nationale hulpverlening en de assistentie aangeboden door de NAVO is te vinden in het feit dat hulpverlening geen centrale taak van de Alliantie is. Bovendien worden in het kader van de EU meer en meer initiatieven genomen die deze aspecten invullen (oefeningen, CIP, structuren en netwerken-zie hoger). Zoals in het kader van de strijd tegen proliferatie overeenkomsten gevonden werden tussen de NAVO en de EU (WMDC) waarin gevorderde samenwerking mogelijk is, zo moet men ook in het kader van de hulpverlening vaststellen dat parallelle structuren beter met elkaar kunnen samenwerken. Hierdoor kan men in fine parallelle structuren en incoherente taakverdeling vermijden: een illustratie hiervan is de overeenkomst tussen het MIC (EU) en het EADRCC (NAVO). Men mag de Alliantie niet zien als concurrent van de Unie (of andersom): eerder kunnen de verschillende organisaties nauwer samenwerken in overlappende domeinen (zoals proliferatie en noodplanning). Aanvullingen daar waar mankementen vast te stellen zijn bij ene of andere partner kunnen enkel ten goede komen aan de samenwerking en verstandhouding tussen de leden van beide organisaties: de werking van het ECDC is daar een voorbeeld van. Een ander voorbeeld is de “CBRN inventory” van de EU om de militaire middelen te lijsten die men kan gebruiken tijdens noodplanning CBRN.

De eigenheid van de EU als organisatie zonder militaire structuur, heeft er ook voor gezorgd dat op vlak van politie en justitie ver gevorderde samenwerking mogelijk blijkt: dit is essentieel in de proactieve aanpak van terroristische (CBRN) dreiging. In dit kader ziet men een taak weggelegd voor de EU die niet binnen de bevoegdheden van de NAVO ligt, maar die een meerwaarde kan bieden aan de Alliantie. Ook het EPCIP-programma wijst in die richting: men moet hier wel de bemerking maken dat op het vlak van ICT beveiliging, de NAVO, omwille van haar militaire bevoegdheden, verder gevorderd is dan de EU. Meer en meer ziet men zowel in de structuren als in de plannen, dat samenwerking de productiviteit ten goede zou komen: optimalisatie van de inzet van middelen in tijd en ruimte kan ook hier zijn toepassing vinden. Nieuwe structuren dienen niet in het leven geroepen te worden indien bestaande instanties het werk kunnen doen, eventueel in coöperatief verband: zo kan taakverdeling in de ruimte tussen de organisaties ook een optie zijn. Bijvoorbeeld kan de inzet van zware middelen voor hulpverlening in projectie over lange afstand eerder een taak voor de NAVO zijn, terwijl middelen ingezet tussen buurlanden eerder toegewezen zou kunnen worden in EU verband. Een ander initiatief dat op regelmatige basis gebruik maakt van NAVO-middelen, ditmaal in het kader van de VN en de strijd tegen proliferatie, is het PSI. Hinderpalen voor dit initiatief werden reeds vermeld, maar ook hier zou een nauwere samenwerking en overeenstemming van de structuren ervoor kunnen zorgen dat PSI niet enkel een maritieme aangelegenheid blijft, maar ook op land- en luchtroutes systematisch toegepast kan worden. Binnen het NAVO-grondgebied zijn de nodige middelen beschikbaar. De EU (en België in het bijzonder) is een kruispunt voor deze routes. De EU beschikt bovendien over de juridische middelen en informatie (vb. EUROPOL)

¹⁷¹ Hoewel werkdocumenten voor Civ-Mil samenwerking in het CBRN-domein werden opgesteld door DGP en SCEPC in april 2009, moet men er de vertaling nog van vaststellen op het terrein.

om ongeoorloofd transport te verhinderen. Ook op vlak van afzonderlijke initiatieven lijkt het dus aangewezen om nauwere samenwerkingsakkoorden tot stand te brengen om de efficiëntie van het beoogde resultaat te vergroten.

Het is duidelijk dat de aangevoerde analyse enkel haar toepassing vindt binnen het kader van dit werk zijnde proliferatie, passieve (CBRN-)bescherming en bescherming van kritische infrastructuur. Dat nauwere samenwerking tussen vermelde organisaties binnen dit kader nodig is, is duidelijk: CBRN-middelen zijn gespecialiseerd en duur (o.m. personeel en materieel). Een optimale exploitatie van deze middelen vereist dus ook een optimalisatie (lees rationalisatie) van inzet van bestaande structuren binnen de vooropgestelde context. Het is dus geenszins de bedoeling om het bestaan van een conventionele EU-strijdmacht in vraag te stellen: deze problematiek maakt deel uit van een analyse die niet in dit werk zal behandeld worden.

2.2.4. OVSE

De Organisatie voor Veiligheid en Samenwerking in Europa (OVSE) werd opgericht in 1994 te Boedapest. Oorspronkelijk gericht op de inkrimping van conventionele strijdkrachten op basis van “Confidence building measures”, werd het werkterrein grondig uitgebreid na de conferentie van Lissabon (1996): politico-militaire aangelegenheden, economie en milieu, mensenrechten vormen ook een deel van de koek. Belangrijk is het onderscheid te zien tussen de NAVO (een militaire alliantie) en de OVSE die een politieke organisatie is: ze kan enkel advies verlenen tijdens conflicten en bemiddelen waar mogelijk. Het OVSE-hoofdkantoor is gevestigd te Wenen. Voornaamste organen van deze organisatie zijn de OVSE-top, de Ministerraad en de Permanente Raad. De OVSE-top wordt op onregelmatige basis gehouden en is een vergadering van staatshoofden en regeringsleiders. De Ministerraad wordt gehouden tussen de Ministers van Buitenlandse Zaken van de lidstaten. De dagelijkse organisatie is in handen van de vaste vertegenwoordigers die zetelen in de Permanente Raad. Op het einde van de Koude Oorlog werden een aantal initiatieven genomen die het vertrouwen tussen de twee grote allianties moesten herstellen. Eén ervan is het “Open skies” verdrag dat officieel in voege trad in 2002. In het kader van dit verdrag konden een vast aantal aangekondigde observatievluchten over de militaire basissen van de respectievelijke allianties plaatsgrijpen met sensor-uitgeruste toestellen. Het oorspronkelijke doel was het vertrouwen te herstellen tussen de twee militaire blokken. De huidige taken zijn enigszins geëvolueerd. Onder de belangrijkste activiteiten vinden we vandaag o.m. mensensmokkel, wapen- en drugsmokkel als topprioriteit; bijkomende taken zijn de inperking van de wapensmokkel vrijgekomen in het tijdperk na de Koude Oorlog, conflictpreventie, strijd tegen terrorisme met inbegrip van crisisbeheer en tijdige waarschuwingsnetwerken, democratisering, promoten van economische stabiliteit, opleiding, ondersteuning voor de organisatie van verkiezingen, toezicht op de naleving van mensenrechten en persvrijheid, respect voor het milieu en gelijke kansenbeleid. In het kader van de strijd tegen proliferatie en smokkel van WMD materiaal moet men in deze waslijst van taken voornamelijk de aandacht richten naar de acties gericht tegen het terrorisme. Hiervoor is de Action Against Terrorism Unit (ATU) verantwoordelijk. De verschillende verbonden tegen het terrorisme werden op verschillende actiedomeinen benaderd: elk van deze domeinen heeft eigen basisdocumenten. Een bondig overzicht van de verschillende domeinen met de aangepaste referentie is aan de orde:

- Algemene anti-terreur instrumenten: de basis werd gelegd in de ministerraad van 2001 te Boekarest waarin het actieplan werd goedgekeurd dat de krijtlijnen van het Porto-charter van 2002 zou aftekenen (zie bijlage 12). De ministerraad van 20 juni 2005 gaf de nodige impuls om lidstaten de VN Conventie te laten ratificeren tegen nucleair terrorisme. In 2006 (Brussel) werd opnieuw het belang onderstreept voor de goedkeuring van alle internationale verdragen omtrent de strijd tegen het terrorisme, georganiseerde misdaad en corruptie.
- Mensenrechten kregen belangstelling in de Conferentie van Kopenhagen van 1990. Vanaf dan werd de basis gelegd voor wat de fundamentele regelgeving zou worden in zake democratische principes voor de hele OVSE regio: toegespitst op de strijd tegen het terrorisme betekent dit dat alle acties moeten gevoerd worden in respect van internationale mensenrechten.
- Veiligheid in het domein van transportdocumenten: voornamelijk wordt hier de nadruk gelegd op de beperking van beweging van terroristen door efficiënte controle op identiteitsdocumenten¹⁷². Hiertoe wordt het belang aangewezen om biometrische gegevens op te nemen in identiteitsdocumenten¹⁷³. Tegen het frauduleus gebruik van deze documenten wordt samenwerking met Interpol aangemoedigd door middel van het “Automated Search Facility/Stolen Travel Document Database” (ASF-STD). Indien mogelijk, moet een nationaal contactpunt voorzien worden op 24/7 basis¹⁷⁴.
- Wettelijke samenwerking werd vastgelegd in een tekst die de principes van vervolging en uitlevering bepalen in het kader van terrorismebestrijding maar ook in georganiseerde misdaad¹⁷⁵.
- Veiligheid van containertransport wordt overgelaten aan de nationale wetgeving, maar de lidstaten worden aangemoedigd om de veiligheid van dit type transport te garanderen¹⁷⁶. In de praktijk betekent dit dat het transport ook gecontroleerd moet worden op de aanwezigheid van WMD materiaal, nucleair en radiologisch materiaal in het bijzonder. Hiervoor kunnen douaneportieken voorzien worden voor de detectie van straling.
- Internetveiligheid is essentieel in de strijd tegen het terrorisme en voor de beveiliging van kritische infrastructuur in het bijzonder. Bij aanvallen op bestaande structuren moet het beheer van alle systemen mogelijk blijven; bovendien moet de informatie-uitwisseling gegarandeerd worden tussen interveniërende diensten op het terrein met de beheersverantwoordelijken zoals de crisiscellen. Vele systemen werken “wireless” en zijn dus gevoelig voor al dan niet intentionele interferenties, overbelasting, of moedwillige aanvallen. Behalve voor de nucleaire noodplanning, wordt tijdige waarschuwing door onze eigen crisiscel gerealiseerd door middel van internetcommunicatie met buurlanden: meldingen van het MIC of BICHAT transiteren via deze weg die bijzonder kwetsbaar is. Het uitvallen van dit meldingssysteem zou catastrofale gevolgen hebben voor de “situation awareness” in ons eigen crisiscentrum. Acties om het gebruik van Internet voor terroristische doeleinden te ontzeggen worden onderbouwd door OVSE MC Decision 7/06: samenwerking wordt door het ATU gepromoot op basis van de bestaande G8 24/7 Computer Crime Network, dat ook als centraal orgaan kan fungeren voor het detecteren van ongeoorloofde netwerkmisbruiken en cyberterrorisme. Iedere lidstaat heeft een POC in deze

¹⁷² MC Decision No.1/01-Combatting Terrorism.

¹⁷³ MC Decision No.7/03-Travel Document.

¹⁷⁴ MC Decision No.4/04-ASF-STD ; MC Decision No.6/06-Further Measures to Prevent the Criminal Use of Lost/Stolen Passports and Other Travel Documents.

¹⁷⁵ MC Decision No.4/05-Enhancing legal cooperation; MC Decision No.5/06-Combating Organized Crime.

¹⁷⁶ MC Decision No.9/04-Enhancing Container Security; MC Decision No.6/05-Further Measures to enhance container security.

werkgroep: België heeft deze taak toevertrouwd aan het FCCU van de Federale Politie.

- Beslissingen van de Permanente Raad in dit kader hebben voornamelijk betrekking op zelfevaluatie¹⁷⁷, nationale wetgeving omtrent financiering van terrorisme¹⁷⁸, solidariteit met slachtoffers van terrorisme¹⁷⁹ en het aanmoedigen van de maatregelen voorgeschreven door het IAEA met betrekking tot de veiligheid van radioactieve bronnen¹⁸⁰.

Al deze maatregelen passen in een structuur die gericht is om een gunstig klimaat te organiseren voor de samenwerking tussen de lidstaten in het kader van de strijd tegen het terrorisme. Concrete structuren zijn echter onbestaande in deze organisatie: eerder wordt een beroep gedaan op bestaande cellen/structuren binnen een parallelle nationale of internationale organisatie. De verantwoordelijkheid voor de uitvoering van de voorgestelde maatregelen en hun correcte uitvoering blijft de verantwoordelijkheid van de lidstaten. Aan de positieve zijde van de balans kan men vaststellen dat de voorgestelde maatregelen doeltreffend kunnen zijn: voorwaarde is dat ze nageleefd worden door alle lidstaten en voldoen aan uniforme criteria. Naleving van de voorgestelde maatregel kost geld: het is evident dat de landen van de EU bijvoorbeeld technologisch en economisch sterker staan dan landen uit Centraal Azië. Het probleem dat hieruit voortvloeit is dat er geen veilige zones kunnen gecreëerd worden: ofwel worden de maatregelen uitgevoerd door iedereen op dezelfde manier, ofwel zal men in een systeem terecht komen dat veiligheid hanteert naargelang de economische en technologische mogelijkheden m.a.w. met verschillende kwaliteit naargelang het land waarin men komt. Dit is onaanvaardbaar in een situatie waar de samenwerking van iedereen vereist is om de veiligheid van evenveel te garanderen.

2.2.5. NATIONAAL

Men kan zich terecht de vraag stellen wat de concrete impact is van al deze internationale initiatieven op de werking van de nationale instanties: sommige initiatieven hebben onmiddellijke gevolgen voor de lidstaten, andere worden aangemoedigd maar de toepassing ervan blijft een nationale verantwoordelijkheid. We overlopen hier nog even het rijtje en de implicaties voor het beleid op Belgisch niveau.

Zowel de non-proliferatieverdragen als de exportcontroleregimes werden door België geratificeerd. In het kader van het CWC is België zelfs onderhevig aan OPCW inspecties in industrie en binnen Defensie. De resolutie 1540, meer bepaald het gedeelte over toegespitste grenscontroles tegen smokkel van WMD materiaal, biedt enige praktische problemen. In 2008 lieten ambtenaren van Douane nog weten te weinig effectieven te kunnen inzetten met als gevolg dat slechts 1% van alle containertransport grondige controle kon ondergaan. Binnen het kader van de problematiek van de wapenwetgeving i.v.m. doorvoer, kan dit een ernstig risico vormen. Hierbij moet men nog rekening houden met de problematiek van detectie en afscherming van bronnen.

¹⁷⁷ PC Decision No.487- on Financial Action Task Force self assessments on terrorist financing.

¹⁷⁸ PC Decision No.617- on Further measures to suppress terrorist financing.

¹⁷⁹ PC Decision No.618- on Solidarity with victims of terrorism.

¹⁸⁰ PC Decision No.683- on Countering the threat of radioactive sources.

Hoewel het IAEA een technische instructie heeft uitgeschreven voor grenscontrole (Technical guidance N°6), evenals een specifieke instructie voor de behandeling van het probleem van verdachte verzendingen (IAEA technical guidance N°3), moet men toegeven dat een adequate afscherming van radiologische/nucleaire bronnen niet zo moeilijk te realiseren is. Dit kan de detectie natuurlijk in gevaar brengen.

Ook de bescherming van CBRN-sites (specifiek opslag oude/bestaande munitie) en de bescherming van kerncentrales (IAEA technical guidance N°4) of opslagplaatsten van verbruikte nucleaire brandstof moeten een speciaal toezicht krijgen.

Grenscontrole en terrorismebestrijding in het kader van het VN Counter Terrorism Plan vallen binnen de verantwoordelijkheid van de Federale politie: deze wordt op regelmatige basis gevisiteerd naar de controle van actieplannen.

Een groot pijnpunt blijft de coördinatie van de noodplanning en de informatiestroom. De verscheidenheid aan contactpunten binnen de verschillende waarschuwingssystemen maken het er niet gemakkelijke op. Op het vlak van uitwisseling van informatie, zijn nationale contactpunten van internationale organisaties soms moeilijk te vinden (zie bijlage 8). Meeste instanties die in het kader van deze studie werden gecontacteerd bevestigen de indruk dat de meeste organismen ook in afzonderlijke vakjes werken. Dit heeft natuurlijk ernstige gevolgen voor doorstroom van informatie, laat staan de organisatie van gecoördineerde actie. Ook de fundamentele werkwijze van dreigingsanalyse tot bescherming van kritische infrastructuur heeft nog geen generationaliseerde aanpak gezien. Dreigingsanalyse is niet afgestemd op de gelijste kritische infrastructuur (CriViSen), welke op haar beurt niet overeenstemt met de Europese benadering van het probleem. Het incident van IRE heeft aangetoond dat zelfs de meest gekende en getrainde noodplanning spaak loopt indien informatie en gecoördineerde actie inefficiënt blijken of totaal achterwege blijven.



2.3. Deelbesluit

Op vele vlakken kan men vaststellen dat de militaire organisatie, bijvoorbeeld in NAVO verband, beter georganiseerd is: of het nu kadert in militaire operaties of steun aan civiele noodplanning, liggen de structuren en verantwoordelijkheden vast. De nodige middelen zijn voorzien of kunnen naargelang hun beschikbaarheid ingezet worden.

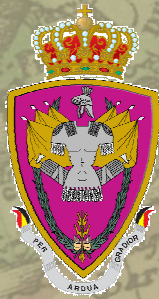
Het probleem dat zich nog steeds acuut stelt, is de militaire samenwerking in de nationale noodplanning. In vele gevallen wordt dit op een ad hoc basis ingevuld. CBRNE-noodplanning kan echter niet op die manier beheerd worden. Hoewel Defensie reeds plannen in aanmaak heeft, hebben we gezien dat ook vele andere departementen betrokken zijn in deze problematiek, al was het maar met betrekking tot de verschillende waarschuwingssystemen en hun respectievelijke contactpunten. De algemene coördinatie m.a.w. de commando, controle en communicatie is blijkbaar nog een vaag begrip binnen de crisiscel die het geheel moet coördineren. De risico-evaluatie heeft voorwerp uitgemaakt van een prioriteitschema dat reeds vijf jaar verouderd is. En indien ook dat buiten beschouwing wordt gelaten, merkt men dat de huidige dreigingsanalyses niet afgestemd zijn op de gelijste doelwitten die gematerialiseerd zouden moeten zijn door CriViSen welke voor geen enkele FOD online beschikbaar is. Erger nog, bewuste lijst is niet bruikbaar omwille van haar samenstelling (te veel inputs; infrastructuur en personen in dezelfde databank; dreigingsanalyse toegespitst op ambassades of personen). Het ontbreken van afdoende definities en een duidelijk concept bij de samenstelling van CriViSen maakt dat bewuste lijst niet bruikbaar is voor uitbating van maatregelen.

Ook de doorstroom van informatie blijkt niet optimaal te gebeuren: tijdens dit onderzoek is meermaals gebleken dat informatie die gevraagd werd, aan verschillende personen moest gericht worden alvorens een correct aanspreekpunt te vinden. Op zich is dit niet zo verwonderlijk als men de verscheidenheid van instanties, en het netwerk daaromtrent voor ogen houdt (zie bijlage 8 en voetnoot 161). Kan men dan nog spreken over een afdoend systeem voor crisisbeheer wanneer een essentieel element van C³ m.n. de communicatie mank loopt? Men mag hopen dat het voorstel dat zal geformuleerd worden in het laatste deel van dit werk meer actoren zal bereiken en aldus een oplossing zal kunnen bieden.

Nog fundamenteeler is de verkeerde hantering van definities en de praktische gevolgen ervan: de wet op de dreigingsanalyse omschrijft duidelijk welke outputs moeten geleverd worden. Refererend naar meldingen op de webpagina van de crisiscel van de regering kan men merken dat terminologie voor dreigingsanalyse en risicoanalyse door elkaar gebruikt worden. Dit kan geen gezonde basis zijn voor een degelijke toepassing van de theoretische begrippen die academici ten voordele van de overheid hebben uitgewerkt. Het probleem stelt zich wanneer men weet dat deze analyse aan het begin van de besluitvormingscyclus ligt: een wankel basis kan immers geen stevig bouwwerk opleveren.

Het volgende hoofdstuk wil mogelijkheden identificeren om zowel praktische als beleidsmatige verbeteringen voor te stellen aan bestaande procedures en/of toepassingen.

Deel 3



Beleidsondersteunende aanbevelingen



3.1. Tactische aanbevelingen

3.1.1. NOODPLANNING C²

Commando en controle impliceert een efficiënt beheer van de site. De sequentie van noodzakelijke activiteiten moet vastliggen en geoefend zijn: procedures moeten klaarliggen en door alle actoren gekend zijn. Bovendien moet CP-Ops permanent kunnen beschikken over een coherent overzicht van de situatie (situation awareness): een voorstel tot ondersteuning zou kunnen zijn dat men visualisatie van de interventie voorziet door camera's. Controle betekent ook dat op de plaats van het delict, alle activiteiten beheerd worden door CP-Ops: dit betekent dat ook de toegang tot de zone aan controle onderhevig is. Het in dit onderzoek aangehaalde voorbeeld van een achtergebleven dader – situatie die men ook uit voorbeelden in het buitenland steeds meer ziet – kan men aanpakken door alle actoren te voorzien met specifieke identificatiebadges. Men zal wel rekening moeten houden met het feit dat een achtergebleven dader zich ook onder de slachtoffers kan verschuilen: de eerste screening en evacuatie van levende slachtoffers zal dus uitermate voorzichtig moeten gebeuren. Voor de evacuatie en identificatie van overleden slachtoffers werd een voorstel gedaan door de invoering van een post-mortem CBRN-kit. Vermelden we voor de volledigheid dat de vastgelegde sequentie van de activiteiten van de verschillende actoren cruciaal zal zijn voor een efficiënte en snelle aanpak van het verloop van de gebeurtenissen. Een strikte naleving hiervan zal ook bijdragen tot het overzicht dat de bevelhebber ter plaatse moet kunnen behouden.

3.1.2. AANKOPEN

De aankoop van uitrusting in het kader van de aanpak van CBRN-incidenten moet aan voorafgaandelijke evaluatie onderhevig zijn. Vragen zoals: moet het materieel enkel ingezet kunnen worden in CBRN-omstandigheden of ook conventioneel, of moet men een conventionele capaciteit aanvullen met een CBRN-capaciteit, moeten vooraf besproken worden. Een voorbeeld hiervan zijn de robots van DOVO die de neutralisatie van geïmproviseerde springtuigen bewerkstelligen. In de literatuur valt men omtrent deze problematiek vaak terug op het volgende standpunt: “don't send a man for what a robot can do!”. Welnu, in dit opzicht moeten robots, a priori uitgerust zijn met alle noodzakelijke detectoren, en moeten ze bovendien ontsmetting kunnen ondergaan. Dit is moeilijk op grondige wijze te realiseren voor robots die uitgerust zijn met rupsbanden. Bovendien is grondige decontaminatie niet compatibel met materiaalvereisten die enkel weerstand tegen stofdeeltjes en lichte regenval voorzien. Dit voorbeeld illustreert hoe een aankoop gevolgen kan hebben op de inzetbaarheid van het materieel: om terug te komen tot ons voorbeeld, heeft men in de huidige configuratie twee opties. Ofwel offert men een robot op voor ieder reëel incident (opnieuw vanuit de optiek dat het aantal werkelijke incidenten zeer beperkt zal zijn), ofwel moet men terugvallen op manuele

neutralisatie met het risico manschappen bloot te stellen. De eerste optie is vanuit militair standpunt uit te sluiten: ook in geprojecteerde scenario's, waar de waarschijnlijkheid van werkelijke incidenten hoger ligt, moet dit type uitrusting inzetbaar zijn! De beslissing ligt bij het beleid: moet men zich niet afvragen waarom operationele vereisten niet a priori kunnen voorzien worden in een nieuw aankoopdossier? Marktvernuwing kan inderdaad het gevolg zijn: niet alle firma's kunnen een volledig uitgerust instrumentarium voorzien. De vraag is of men hierdoor aan operationaliteit moet inboeten en deze achteraf moet invullen door onnodige blootstelling van mankracht omwille van budgettaire redenen.

Het hier besproken voorbeeld is geldig voor ieder uitrusting die aangekocht wordt voor de behandeling van de besproken incidenten. De operationele vereisten zullen de sleutel moeten vormen voor de keuze van het ingezette materieel. Indien budget een beperking vormt, dan kan de uitvoering van de opdracht toevertrouwd worden aan andere partners of moet de invulling van de capaciteit voorzien worden door logistieke ondersteuning van andere partners.

3.1.3. COMMUNICATIE OP DE SITE VAN EEN CBRN INCIDENT

Een essentieel element in de coherentie van de gebeurtenissen wordt tot stand gebracht door efficiënte en robuuste communicatiemiddelen. Werken in een beveiligd pak is niet altijd bevorderlijk voor de elektronica die men meedraagt. Daarboven komt dat lokaal heel wat zenders actief kunnen zijn: afgezien van alle achtergrond (GSM-netwerken bijvoorbeeld), zal de ontmijningsdienst, waar nodig, gebruik maken van stoorzenders om een ontstekingsmechanisme onklaar te maken dat van op afstand kan aangezet worden. Beveiligde communicaties zijn bovendien noodzakelijk om te vermijden dat verkeerde informatie doorgegeven wordt aan de hulpverleners. Een coherent en beveiligd lokaal communicatieplan is dus een absolute noodzaak. Dit zal bovendien toelaten dat verzaaiing van een commercieel netwerk geen weerslag heeft op het correcte verloop van de activiteiten. Een bespreking van de coherentie van de snelle waarschuwingsnetwerken zal besproken worden onder de strategische aanbevelingen.

3.1.4. SENSOREN

Het aanbod aan detectoren is zeer ruim, maar ook zeer verschillend naargelang het agens dat moet gedetecteerd worden. Een universele detector voor het volledige CBRN- spectrum is technisch niet echt realistisch als objectief. Bovendien moet men nog de keuze kunnen maken tussen afstandsdetectoren (stand-off), gerichte detectoren (point detection), vaste en draagbare detectoren. Met afstandsdetectoren bedoelt men vaste of mobiele systemen die grote zones van op afstand kunnen bestrijken. Gerichte detectoren, daarentegen, zijn draagbare systemen bedoeld om een verdachte plaats te controleren. Vaste detectoren zijn meestal grotere installaties voor de controle van een grote stroom bagage, voertuigen of zelfs mensen. Draagbare detectoren worden eerder gebruikt voor de snelle detectie en pre-identificatie van een agens. De vastgelegde operationele taak van iedere actor zal bepalend zijn voor het type detectoren dat men zal willen inzetten. Men kan hierbij echter wel de bedenking maken dat, bijvoorbeeld voor het geval van chemische detectoren, de geleverde output nog vaak te catalogeren valt onder de NBC-taal die dateert uit de koude oorlog: de output valt terug op de grote classificaties van agentia (blaartrekkers, zenuwgassen, stikgassen en

bloedgassen). De industriële toxische agentia reageren vaak niet of verkeerd op dit type detector. Voor reële operaties valt het dus aan te raden dat het spectrum van de verschillende agentia voor één CBRN categorie (in dit geval chemische) zo ruim mogelijk wordt gehouden: dit kan enkel ten goede komen aan de interventiesnelheid en op die manier valse negatieve detecties tot een minimum herleiden.

Om specifiek in te gaan op de problematiek van biodetectoren, kan men enkel vaststellen dat hun ontwikkeling een constante evolutie kent: idealiter zouden deze detectoren bruikbaar moeten zijn door hulpverleners in alle weersomstandigheden. Bovendien moeten ze in staat zijn om een breed spectrum aan pathogenen te detecteren aan een zo laag mogelijke detectiedrempel, in een veelvoud aan matrices; valse positieve en valse negatieve meldingen zouden niet mogen voorkomen en het toestel zou ook een toepassing moeten hebben voor gebruik als stand-off beveiliging (lees detectie voor de beveiliging van installaties of gekampeerde troepen). Het is duidelijk dat deze ideale omstandigheden niet compatibel zijn: ergens zal men een compromis moeten sluiten over welke detector men wil ontwikkelen of aankopen: moet men kiezen tussen een toestel dat detecteert om een aanval af te wenden (detect to protect) of een toestel dat de evolutie van de besmetting als monitor opvolgt (detect to treat). Deze twee benaderingen zijn fundamenteel verschillend en kunnen natuurlijk complementair gebruikt worden. Bovendien moet men rekening houden met de gebruiker: zullen militairen of burgers de monitoring uitvoeren? Antwoorden op deze vraag impliceert dat men geëxperimenteerde mensen moet voorzien die de resultaten kunnen interpreteren: hiervoor is ervaring vereist om verder te kunnen denken dan datgene wat het toestel als resultaat weergeeft. Of moet men eerder hulpverleners met het gebruik van deze toestellen belasten? Dit is een keuze die zowel door doctrines, als door financiële en operationele beperkingen zal moeten vastgelegd worden. De keuze ligt bij het beleid, maar men kan hier wel aanraden verder te gaan in de ontwikkeling/aankoop van complementaire systemen: enerzijds kunnen eenvoudige toestellen een eerste indicatie geven en bijgevolg gebruikt worden door hulpverleners of operatoren ten velde. Men zal moeten aanvaarden dat deze toestellen gevoeliger zullen zijn voor valse meldingen. Anderzijds kan men deze uitrusting aanvullen met detectoren die nauwkeuriger zullen functioneren en minder gevoelig zijn voor deze valse meldingen: in deze fase zal echter interpretatie vereist worden van adequaat gevormd (wetenschappelijk) personeel. Men moet steeds in gedachten houden dat de ideale detector niet bestaat en dat biodetectie steeds zal moeten aangevuld worden met andere middelen. Voorstel is om biodetectie te laten steunen op vijf pijlers: detectie (door bio-detectoren met alle voordelen en beperkingen die aangehaald werden), profylaxie, biologische staalname en identificatie (ter controle van de detectie), klinische rapportage (eventueel met reach-back capaciteit van een erkend laboratorium) en collecte van informatie (voor, tijdens en na het incident). Het is duidelijk dat biodetectoren het werk niet alleen aankunnen: opvolging is noodzakelijk en de voorgestelde pijlers vormen een basis ter ondersteuning en uitbating van de informatie om de beschikbare middelen optimaal te kunnen inzetten.

We stellen vast dat detectoren hun beperkingen hebben wat de output van informatie betreft. Om eenduidige identificatie toe te laten zou het aangewezen zijn op de plaats van het delict over een mobiel identificatielaboratorium te beschikken. Dit type laboratorium is uitgerust met alle toestellen die, in beveiligde omgeving, toelaten om ter plaatse (géén transport vereist naar andere laboratoria), op een tweetal uren tijd, uitsluitel te geven over het gevaar van het betrokken agens. Deze informatie zal CP-Ops toelaten om beslissingen te nemen over de eventuele aanpassing van veiligheidsafstanden en perimeters (en dus ook over de opheffing van evacuatiemaatregelen). Bovendien zal men een eerste evaluatie kunnen voorstellen met betrekking tot de decontaminatie van de site.

Meteorologische informatie is een essentieel element in het kader van CBRN interventies: onderzoek heeft uitgewezen dat voorspellingen van hoge luchtstromen, door het KMI ter beschikking gesteld, niet bruikbaar zijn in stedelijke omgeving. Deze informatie is vooral nuttig tijdens een ramp type Tsjernobyl. Een noodzaak is het beschikken van micrometeo op de plaats van het incident om evoluties in real-time op te volgen. Twee oplossingen, die elkaar niet uitsluiten, dringen zich op. Vooreerst zou men moeten beschikken over studies die rekening houden met de specifieke stedelijke luchtstromen en perturbaties: dergelijke berekeningen kunnen gegenereerd worden voor alle steden, met Brussel als prioriteit. Om een bruikbare output te verkrijgen uit deze berekeningen zal men ook bijvoorbeeld luchtkokers van metro's moeten opnemen als parameter. Dit aspect wordt in het volgende punt aangehaald (beschikbaarheid van informatie). De algoritmes die voortvloeien uit de studie moeten eveneens opgenomen worden in de ondersteunende informatie van de noodplanning. Vervolgens moet men in dezelfde optiek rekening houden met de update van de metingen op de plaats van het delict: dit is een essentiële informatie die de theoretische berekening zal moeten voeden. Een plotse windstoot, of het keren van de wind bij een kruispunt, kunnen het volledige CBRN dispositief in gevaar brengen. Er moet grondig over de in plaats stelling nagedacht worden gezien de tijd nodig om een volledig dispositief aan te passen. Verwijzen we in dit verband en ter illustratie nog even naar bijlage 7. Het is dus essentieel voor de veiligheid van iedere hulpverlener dat plaatselijke meetpunten opgesteld worden, die de evolutie van de meteorologische omstandigheden onmiddellijk kunnen weergeven in het CP-Ops. Een minimale bezetting van dergelijke meetpunten zou uit twee stations moeten bestaan (één vóór het dispositief en één erachter). De informatie waarover men moet kunnen beschikken zijn windrichting en snelheid in prioriteit, eventueel aangevuld met temperatuur en luchtvochtigheid. Ten slotte moet men er zich rekenschap van geven dat ook na afloop van het incident metingen zullen moeten uitgevoerd worden, al was het maar om de efficiëntie van de ontsmetting na te gaan.

3.1.5. BESCHIKBAARHEID VAN DE INFORMATIE

Gebruik en vergaring van de informatie is een fundamenteel element in de nood-en interventieplanning, zoals tijdens elke crisis. Deze informatie kan beschikbaar zijn in vooraf opgestelde plannen, maar kunnen ook vergaard worden door sensoren tijdens een lopend incident. In deze paragraaf zullen, in het kader van de beschikbaarheid van de informatie, verschillende thema's aangehaald worden: bestaande infrastructuurplannen, oefenbeleid, ontruimingsplannen en inlichtingenstroom naar de bevolking toe. Rationalisatie van het informatienetwerk wordt behandeld in het gedeelte "strategische aanbevelingen".

Vooreerst moeten infrastructuurplannen beschikbaar zijn voor kritische infrastructuur. Bovendien moeten de hulpdiensten kunnen beschikken over dezelfde informatie met betrekking tot metro, riolering en verluchtungskokers: deze elementen vormen essentiële informatie die de verspreiding van een CBRN-incident zal helpen in te schatten.

Wat het oefenbeleid betreft, moet men ook de kans grijpen om de praktijk in te oefenen, met alle beschikbare middelen en alle betrokken actoren (alle FODs samen met Defensie): deze praktijk zal toelaten om mankementen aan het daglicht te brengen die nog kunnen rechtgezet worden. Een reëel incident zal die opportuniteit niet geven! Het radiologisch incident te Fleurus in augustus 2008 heeft aangetoond dat, ondanks de beschikbaarheid van een inge oefend noodplan, nog heel wat mis kan gaan op gebied van communicatie naar de bevolking: dit werkt verwarring in de hand.

Voor een plan dat enkel op papier bestaat, zullen de gevolgen nog ernstiger zijn. De budgettaire enveloppe zal bijgevolg middelen moeten voorzien om grootschalige oefeningen te organiseren op regelmatige basis.

Een preventieve inlichtingencampagne naar de bevolking toe (bijvoorbeeld folders in kader van civiele veiligheid: wat te doen in geval van een radiologisch incident, stroomonderbreking, overstroming, aanslagen etc...) kunnen zeker nuttig zijn: ze zouden bovendien vermijden dat er spontaan en massaal paniek uitbreekt. Hoe vaker mensen iets te zien of te horen krijgen, des te meer worden ze de voorgestelde maatregelen gewoon. Vandaag de dag zal niemand meer opkijken wanneer een politiepatrouille aankondigt dat ramen en deuren gesloten moeten worden: laten we deze ervaring ook voorzien voor andere incidenten. Bovendien moet men de mogelijkheid voorzien om, via de GSM-operatoren een SMS-campagne te lanceren tijdens een incident: hierdoor kan men een blijvende stroom van mensen naar de betrokken zone vermijden.

“Network centric capabilities” moeten ook in het kader van noodplanning hun nut bewijzen. Deze capaciteit laat toe om “real-time” informatie uit te wisselen tussen crisiscellen en operatoren op de site. Het implementeren van deze capaciteit veronderstelt dat interoperabiliteit nagestreefd zou worden tussen verschillende FODs en Defensie in domeinen als uitwisseling van informatie, communicaties en ondersteuning. De opportuniteit van dergelijke capaciteit in crisisbeheer heeft haar nut reeds aangetoond tijdens militaire operaties op en rond het slagveld. In de VS wordt het gebruik ervan ook aangemoedigd in Homeland operaties: specifieke toepassingen en mogelijkheden voor gebruik in stedelijke omgeving zullen moeten bestudeerd worden. Uiteindelijk moeten de verschillende informatiekkanalen geïntegreerd kunnen worden in een operationeel systeem: dit laat toe om de horizontale (inter-FOD) en verticale (hiërarchische lijn binnen één FOD of Defensie) uitwisseling van informatie toe te laten.

3.1.6. BESCHERMING VAN HET PERSONEEL

Deze studie heeft aangetoond dat het niet vanzelfsprekend is om coherente beschermingsnormen af te spreken tussen hulpverleners die een CBRN-site zullen betreden. Nochtans zijn valabele normen reeds ter beschikking onder de vorm van NIOSH beschermingsfactoren: een eventuele studie kan deze problematiek verder uitdiepen, maar het lijkt ons aangewezen om nu reeds standaardnormen te hanteren i.p.v. beschermingsmaatregelen aan te passen naar de middelen die men ter beschikking heeft. Ook deze besluitvorming maakt deel uit van een eigen risicoanalyse op niveau hulpverlener/IC: consequente aanpak vereist de analyse van de situatie om de in te zetten middelen te bepalen. Te vaak zet men middelen in die voorhanden zijn zonder voorafgaande besluitvorming. Hetzelfde geldt voor de veiligheidsafstanden: dit onderwerp werd reeds uitvoerig behandeld. Ook hier bestaat een bruikbare norm (ERG) die ingepast moet worden in de administratieve afbakening van zones, voorzien in de Nood- en Interventieplanning.

3.1.7. BEVEILIGING VAN LUCHTHAVENS

Beveiliging van vliegtuigen kan moeilijk nog strenger aangepakt worden dan vandaag het geval is. Hierdoor heeft men mogelijk de bedreiging verplaatst naar de luchthaven zelf: men kan slechts vaststellen dat aanslagen in belangrijke mate plaatsgrijpen op druk bezocht plaatsen. Wat kan er drukker zijn dan de inkomhall van een luchthavencomplex? Mogelijk zouden terroristische activiteiten zich naar deze zone kunnen verschuiven. Het is dus belangrijk om deze zone eveneens te voorzien met snelle screeningsmethodes. Mogelijk ligt hier een domein open voor wetenschappelijk onderzoek gericht naar portieken voor screening van personen op basis van biometrische gegevens vóór de incheckbalie? Men zou het gebruik van betrokken apparatuur zelfs kunnen uitbreiden naar zones als treinstations, metrostations, bushaltes, sportinstallaties en megamanifestaties.

3.1.8. BEVEILIGING VAN OPERATIONELE ZONES, BESCHOTEN MET VERARMD URANIUM (DU): INFORMATIEBERICHTEN OMTRENT HET GEBRUIK VAN DU-MUNITIE

Munitie met verarmd uranium is reeds enkele jaren in gebruik op het slagveld omwille van het penetrerend vermogen. Zowel voor artillerie als voor individuele wapens wordt dit type munitie door sommige troepen gebruikt. Gebruik op zich levert geen risico's op. Het grote probleem met dit type munitie is dat impact vervorming en versplintering veroorzaakt. Naast de vernietiging van doelen, worden dus heel wat stofdeeltjes verspreid die afkomstig zijn van deze munitie. Deze stofdeeltjes bevatten nog steeds kleine hoeveelheden natuurlijk uranium, een α -straler. Munitie van dit type hoort niet in de categorie van massavernietigingswapens. Op zich kan iemand in de aanwezigheid van een α -straler, weze het in de lucht of op de grond, zeer goed beschermd worden: handschoenen en maskers zijn in principe voldoende. Het probleem is dat deze radioactiviteit lange tijd aanwezig kan blijven en enkel verplaatst kan worden door de verplaatsing van de besmette deeltjes. In wezen kan hier dus een probleem reizen van besmetting van de zone, zoals het geval is bij een vuile bom maar dan op kleinere schaal. Dat betekent dat niet alleen geallieerde troepen in dezelfde regio, maar zeker de burgerbevolking een ernstig risico kan lopen op besmetting. Zeker voor deze groep is het gevaar ernstig aangezien de eerste bekommernis van de bevolking vaak gericht is op de hervatting van hun activiteiten. Zonder vermelding van de aanwezigheid van deze dreiging, lopen vele mensen, na het conflict, het risico op ernstige gezondheidsproblemen. Daarom is het aangewezen dat een bescherming geboden wordt voor troepen in de regio: door verspreiding van informatieberichten "gebruik van DU-munitie" kan men bevriende troepen waarschuwen voor de gevaren. Deze kunnen de betrokken zones vermijden of de gepaste individuele beschermingsmaatregelen nemen en wrakken in de zone vermijden. Naar de lokale bevolking toe zijn deze berichten misschien nog belangrijker. Mijnevelden worden gemerkt terwijl zones waar DU werd ingezet niet worden gemerkt: deze houden echter een ernstig latent gezondheidsrisico in. Idealiter zou men zones ook tijdelijk kunnen afbakenen met nieuwe pictogrammen eigen aan het gebruik van DU-munitie. Na controle van de zone op α -straling, kan deze dan opnieuw vrijgegeven worden. We moeten ons geen illusies maken door te hopen dat op korte termijn dit type munitie verboden zal worden, laat staan effectief uit gebruik zal worden genomen. Aangepaste markering zou dus echt niet overbodig zijn.



3.2. Strategische aanbevelingen

3.2.1. WAPENWET

Zowel de uitvoer als de doorvoer van militair materieel werden besproken in deel 1 van dit werk als toelichting op de gebreken die in het kader van de bestaande wapenwetgeving nog vastgesteld kunnen worden op het gebied van proliferatie. Europese verordeningen moeten in dit verband klaarheid scheppen. Nochtans hebben we kunnen vaststellen dat de wapenhandel onderhevig is aan nationale en soms zelfs regionale bevoegdheden. Meer bijzonder voor wat het materieel voor tweërlei gebruik betreft, heeft men kunnen vaststellen dat een beperking is ingebouwd voor goederen die opgenomen zijn in bijlage van de Europese verordening EG 1334/2000 en dat de bevoegdheid ter zake gedeeld wordt door de Ministers van Buitenlandse Zaken en Economie. Men zou hier het initiatief kunnen vragen van de wetgever om ook een wettelijk kader te scheppen voor de behandeling van de eerder vernoemde “soft proliferatie”. Dit wettelijk kader zou praktische uitvoering vinden in cellen, gericht op de bestrijding van de activiteiten in het domein van de proliferatie (zie verder 3.2.5).

Doorvoer wordt geregeld op gewestelijk niveau omwille van de regionalisering: ter herinnering kan men vermelden dat voor goederen voor tweërlei gebruik de vergunningsplicht vervalt indien reeds (elders) een communautaire uitvoervergunning werd verleend. Bovendien is er zelfs geen meldingsplicht voor doorvoer die niet onderworpen is aan een vergunning. Het resultaat is dat er bitter weinig overzicht, laat staan rapportering in deze materie mogelijk blijkt. Daarenboven blijkt dat voor die rapportage, zowel op nationaal, als ook op regionaal vlak verschillende maatstaven gehanteerd worden. In eerste instantie zou men, om de transparantie te garanderen, nationale maatstaven moeten hanteren in dit domein, die ook van toepassing moeten zijn voor de gewestelijke jaarverslagen. Bovendien zouden deze jaarverslagen ook een weergave moeten inhouden van de doorvoer van materiaal voor tweërlei gebruik. Het is duidelijk dat doorvoer een kwetsbaar onderdeel vormt van de bestaande wetgeving. Om de controle op dit vlak te verbeteren moeten meer middelen vrijgemaakt worden voor de controlerende organisaties ter zake zijnde de douane: economische druk en geautomatiseerde procedures in wereldhavens vergemakkelijken de taak van deze dienst niet. Zowel op het gebied van materieel als voor het personeel zal versterking van het dispositief en de middelen moeten voorzien worden indien men naar een efficiënte en adequate controle en registratie van doorvoer van proliferatiegevoelig materiaal wil evolueren. België is in deze zeker geen alleenstaand geval: vanuit Singapore, Japan, Maleisië, Australië en waarschijnlijk nog meerdere havens, werd onrechtmatige uitvoer vastgesteld, ondanks automatisering en intensief gebruik van sensoren en scanners. Om die reden zouden internationale standaarden op punt gesteld moeten worden voor de uitvoering van de administratieve- en controletaken van de douane. Bij gebrek hieraan, kan men in de EU reeds het voorbeeld geven door het gebruik van gestandaardiseerde procedures voor melding, controle en registratie te regelen.

Bovendien moet dit aanleiding kunnen geven tot de vorming en instandhouding van een databank die internationaal geraadpleegd kan worden (door de bevoegde diensten) teneinde trends aan het licht te kunnen brengen. Hierdoor kunnen eventueel tijdig efficiënte (re)acties op punt gesteld worden.

Een eerste stap in de goede richting zou kunnen gezet worden door de oprichting van een nieuwe nationale cel en de invoering van de meldingsplicht. Deze cel zou doorvoer kunnen traceren en doorgeven naar een hoger echelon (EU). Bovendien kan op die manier een databank bijgehouden worden (op nationaal niveau) die zowel de aard van materieel, de bestemming en de gevolgde route bijhoudt. Alle regio's van ons land vormen door waterwegen, zee- en luchthavens een ideaal doorstroomgebied voor goederen voor tweeeërlei gebruik.

3.2.2. NUCLEAR FUEL CYCLE MANAGEMENT

De kernbrandstofcyclus vormt, zoals uiteengezet, een proliferatierisico op zich. Nochtans voorziet artikel IV van het NPT de toelating tot vreedzaam gebruik van kernenergie. Deze tegenstelling wordt noch ingewikkelder in de wetenschap dat de kernbrandstofcyclus meerdere disciplines omvat: van mijnbouw, over ertswinning, tot aanrijking van grondstof en opslag van verbruikte brandstof. Aan het einde van de cyclus werd tot voor kort een afwachtende houding ondernomen. De standaard leek de opslag van verbruikte brandstof. Deze opslag moet echter tientallen jaren in veilige omstandigheden gegarandeerd kunnen worden. In 1980 werd in Mol het project HADES opgestart: het uitgangspunt was om de haalbaarheid na te gaan om stabiele geologische lagen te gebruiken als basis voor decennia durende opslag. Vanaf 2009 zal ook de thermische invloed op de opslagcapaciteit bestudeerd en in kaart gebracht worden. Onlangs werden echter alternatieven onderzocht voor de opslag van verbruikte kernbrandstof, mede omwille van het groeiende belang van duurzame ontwikkeling: indien recyclage van gebruikte kernbrandstof een haalbare optie zou blijken, kan de brandstofcyclus gesloten worden. Als rechtsreeks gevolg zou heel wat nieuwe ertswinning overbodig zijn en zouden bestaande reserves langer gebruikt kunnen worden. Bovendien zou de nodige opslagcapaciteit voor afval aan het einde van de cyclus drastisch naar beneden gehaald kunnen worden. Het gebruik van een "gesloten" brandstofcyclus impliceert dat gebruikte brandstof opnieuw aangerijkt kan worden voor hergebruik in de energiecentrales. Op zich is het instrumentarium dat hiervoor vereist wordt zeer gevoelig voor proliferatie: het betreft materiaal van tweeeërlei aard en kan dus ook gebruikt worden in militaire programma's. We hebben reeds kunnen vaststellen dat een aantal initiatieven (waaronder GNEP van de VS) bedoeld waren om het geheel van de activiteiten, gericht op herconditionering van verbruikte brandstof, uitgevoerd zouden worden in de landen die daar VANDAAG de capaciteit voor hebben m.a.w. nieuwkomers of vragende partijen naar kernbrandstof zouden geleverd worden door landen met bestaande capaciteit om hierdoor de proliferatie van de technologie te verhinderen. Op zich is dit ook een lovenswaardig initiatief, ware het niet dat een aantal commerciële belangen de overhand kunnen halen en een monopoliepositie in de hand kunnen werken: er is vandaag geen erkende of vastgelegde prijsafpraak voor gerecycleerde brandstof. Voor bestaande kernbrandstof kon men vaststellen dat de prijs evolueerde van 11,00USD/lb in 2003 naar 40,00USD/lb in 2006¹⁸¹. Binnen het bestaande kader kan men bijgevolg een aantal voorstellen doen om elk land de toegang te garanderen tot het vreedzaam

¹⁸¹ IAEA TECDOC 1529, Management of reprocessed Uranium, International Atomic Energy Agency, Vienna, 2007, p.86.

gebruik van kernenergie. In eerste instantie dient hiervoor de hele kernbrandstofcyclus onder toezicht geplaatst te worden van de Verenigde Naties en meer bepaald het IAEA of een aanverwant organisme dat specifiek hiervoor opgericht kan worden. Alle bestaande verwerkingscapaciteit moet onder toezicht van dit organisme komen, welk ook zou moeten instaan voor het vastleggen van een billijke marktprijs. Bovendien moet de terugname van kernafval in dit kader gegarandeerd worden m.a.w. er moet een controle tot stand kunnen gebracht worden “from cradle to grave” voor elke vorm van brandstof ongeacht de oorsprong, commercieel of militair. Hiervoor kunnen zowel mechanische als chemische merkers aangebracht worden en zullen inspecties en registraties georganiseerd moeten worden. Deze manier van werken zou toelaten dat de capaciteit niet meer afhankelijk is van bilaterale akkoorden zoals onlangs afgesloten tussen India en de VS. Hierdoor zal de internationale gemeenschap de finale scheidsrechter kunnen worden voor het verstrekken van de brandstof zonder daarom een nieuw proliferatierisico in het leven te roepen. De bestaande reserves kunnen bovendien aangevuld worden met materiaal afkomstig van de ontmanteling van kernkoppen (impliciet voorzien in artikel VI van het NPT). Aan hergebruik van dit materiaal kan bovendien een output opgelegd worden met welbepaalde standaarden die het onmogelijk maakt om opnieuw geïntegreerd te worden in bewapeningsprogramma’s (van HEU naar LEU bijvoorbeeld). Intensief wetenschappelijk onderzoek werd reeds uitgevoerd in het domein van recyclage van kernwapensplijtstoffen naar brandstof dat reeds bruikbaar is voor kerncentrales. In dit domein heeft o.m. het Belgische Studiecentrum voor Kernenergie te MOL (SCK-CEN) zich in het verleden reeds onderscheiden¹⁸². Een vaak aangehaald tegenargument in het kader van de recyclage van kernbrandstof, is dat het weinig rendabel zou zijn: men dient hier voor ogen te houden dat alle ontmantelingsactiviteiten van voormalige munitie, al dan niet van het conventionele type, zonder meer een grote kost met zich meebrengen. Deze nieuwe aanpak zou echter toelaten om systematisch energie terug te winnen uit gestapelde kernwapenarsenalen en afgedankte maritieme propulsiesystemen. In deze zware economische tijden is dit een niet te verwaarlozen factor die toelaat om de ontwapening toch op de agenda te laten staan i.p.v. bestaande situatie te laten voor wat ze is, of te verwijzen naar latere datum, met alle inherente risico’s voor de internationale veiligheid. De bestaande persoonlijke expertise van kernwapenexperten zal bovendien niet wegvallen: buitenlandse wetenschappers, werkzaam in de kernwapenindustrie, kunnen zeer goed omgeschoold worden naar de toepassingen van het vreedzaam gebruik van kernenergie. Bovendien heeft dit personeel reeds een gedegen achtergrond wat betreft het werken met hoog radioactieve bestanddelen, hetgeen een niet te verwaarlozen meerwaarde geeft aan het voorgestelde project.

3.2.3. INTERNATIONALE VERDRAGEN: CONSOLIDATIE EN UITBREIDING

In het vooruitzicht van de NPT herzieningsconferentie van 2010¹⁸³, worden jaarlijks voorbereidende vergaderingen georganiseerd¹⁸⁴. Het voortbestaan van het verdrag zal afhangen van de verdere ondersteuning van de drie pijlers van het verdrag met name de voortzetting van de nucleaire ontwapening, de preventie van de nucleaire proliferatie en het oplossen van de problematiek omtrent de voorzieningen voor kernenergie.

¹⁸² Door de verwerking van plutonium tot MOX-fuel bijvoorbeeld.

¹⁸³ Van 26 april tot 21 mei 2010 in New-York.

¹⁸⁴ De PrepCom van 4 tot 15 Mei 2009 in New-York was de laatste voor de herzieningsconferentie van 2010

Ter ondersteuning van de eerste pijler van dit verdrag, zouden de kernwapenstaten zich moeten engageren rond een agenda voor de ratificatie van “NPT ondersteunende verdragen” als het CTBT, HCoC en FMCT. Daar waar het NPT vooral de verwerving van kernwapens aan banden wil leggen, is het CTBT eerder gericht op het inperken van de uitbouw van eigen kernwapenarsenalen, HCoC op de beperking van proliferatie van vectoren en FMCT op de beperking van productie van splijtstoffen voor militaire doeleinden in het algemeen. Niet alleen moeten in het kader van deze verdragen controlemechanismen ingebouwd worden, maar waarschijnlijk gevoeliger is de mentaliteitswijziging die de huidige kernwapenstaten moeten ondergaan om te beseffen dat ook zonder kernwapenarsenaal de vitale belangen van de betrokken Naties gevrijwaard kunnen worden.

De problematiek van de controles is een technische aangelegenheid die zeer nauwgezet kan uitgebouwd worden in afwachting van de ratificatie van een verdrag: het CTBT is hier een illustratie van. Het verdrag wacht nog steeds op ratificatie door China, Noord-Korea, Egypte, India, Indonesië, Iran, Israël, Pakistan en de VS alvorens het officieel van kracht wordt¹⁸⁵. Het controlesysteem van dit verdrag is ondertussen al grondig uitgebouwd: bij ratificatie zal het bestaande technisch secretariaat van het voorbereidend comité (PrepCom) omgevormd worden tot het Comprehensive Nuclear Test Ban Treaty Organization (CTBTO), gelegen te Wenen. Als ondersteuning van het CTBTO is nu reeds een monitoringsysteem (International Monitoring System) uitgebouwd over de hele planeet. Dit is gebaseerd op metingen van zowel seismologische activiteit, hydro-akoustische activiteit, meting van laagfrequentie geluidsgolven en radionuclide metingen. Gecollecteerde data worden doorgezonden naar het International Data Centre (IDC) te Wenen. Dit netwerk heeft zijn nut reeds bewezen door de detectie van het incident met de kernduikboot Koersk (12 augustus 2000) evenals de ondergrondse kernexplosie van Noord-Korea (9 oktober 2006). Bovendien kan het diensten bewijzen voor de vroege aankondiging van tsunami-alarmen en vulkanische activiteit. Meer nog, bij het in voege treden van het Verdrag, zal het systeem verbonden aan het CTBTO onmiddellijk operationeel zijn als controleorgaan. Dergelijke controleorganen kunnen ook in het kader van andere verdragen uitgebouwd worden: ondanks de universaliteit van het NPT, moeten in dit kader nog steeds waarborgovereenkomsten (“safeguards agreements”) en bijkomende protocols (“additional protocols”) afgesloten worden met meerdere staten. Dit systeem, dat een uitgebreide controle door het IAEA toelaat heeft reeds zijn meerwaarde bewezen en laat bovendien toe vertrouwen te wekken (“confidence building”) rond de werking van dit verdrag. De activering van dergelijke mechanismen in het kader van andere verdragen zal bovendien toelaten om kinderziektes uit het systeem te weren alvorens betrokken verdragen effectief operationeel moeten kunnen functioneren.

Veel moeilijker is het gesteld met de veiligheidsproblematiek en haar perceptie: het behelst hier niet enkel een technische benadering maar voornamelijk een mentaliteitswijziging. Het NPT is geschreven in het kader van het streven naar nucleaire ontwapening m.a.w. de inperking van gebruik van kernenergie in militaire programma's. Dit is niet zozeer naar de zin van de huidige kernwapenstaten die (al is het geen uitbreiding van hun arsenaal) de vernieuwing van bestaande middelen (kernkoppen en vectoren) en C² blijven organiseren. Bijkomende problemen die vanuit dit oogpunt vroeg of laat op tafel zullen worden gegooid zijn de tactische

¹⁸⁵ Het verdrag telt 180 leden, waarvan 148 het verdrag hebben geratificeerd. Het verdrag zal slechts van kracht worden 180 dagen nadat 44 staten, die in bijlage 2 van het verdrag zijn hernomen, het verdrag hebben geratificeerd. Negen daarvan hebben dat nog niet gedaan (waaronder de VS, China, India, Pakistan, Israël en Noord-Korea).

kernwapens (bijvoorbeeld gelokaliseerd in NAVO-lidstaten) en het raketterschild van de VS. Een consequente benadering van het NPT impliceert dat ook de tactische wapens geïnventariseerd moeten worden. Het raketterschild daarentegen schept vooral een probleem voor Rusland en China. In principe gericht op de verdediging tegen “schurkenstaten”, zien zowel Rusland als China het raketterschild en het gebruik van de ruimte voor bewapening, als een gevaarlijke uitbreiding die kan leiden tot nieuwe wapenwedlopen en zelfs een nieuwe poort zou kunnen openen voor proliferatie: dit brengt meteen de tweede pijler in gevaar nl. de preventie van de nucleaire proliferatie. Het is dus uitermate aangewezen dat omzichtig wordt omgesprongen met de implementatie van het “ruimtelijk” aspect van het raketterschild. Binnen de NAVO-structuur wordt sinds geruime tijd onderzoek gedaan naar de integratie van tactische middelen¹⁸⁶ voor de bescherming van troepen tegen korte en middellange afstandsrocketten, met inbegrip van sensorplatformen van diverse oorsprong, maar het grote probleem wordt gevormd door het Amerikaans luik van het raketterschild. De officiële standpunten, de technische aspecten en de haalbaarheid van dit project werden bestudeerd in de aanloop van de NAVO conferentie van staats- en regeringsleiders te Kehl-Straatsburg ter gelegenheid van het 60 jarig bestaan van de Alliantie in mei 2009: ongetwijfeld wordt de verdere behandeling van dit project een belangrijke factor voor de toekomst van het NPT en aanverwante verdragen.

De derde pijler die van belang is voor het voortbestaan van het NPT nl. de voorzieningen van kernenergie voor vreedzame doeleinden draagt eveneens een proliferatierisico in zich (zie deel 1 van dit werk). Een mogelijke oplossing van deze problematiek werd voorgesteld in de bespreking van de “nuclear fuel cycle management”. Het gevaar voor de ondermijning van de derde pijler ligt eerder in bilaterale overeenkomsten voor het leveren van kernbrandstof aan de facto kernwapenstaten die het NPT niet hebben geratificeerd. De VS hebben een gevaarlijk precedent gecreëerd door het sluiten van de commerciële overeenkomst met India. De reactie van Pakistan kon niet lang op zich laten wachten: China heeft reeds steun toegezegd om een gelijkaardig akkoord te zullen ondersteunen met Pakistan. Een gelijkaardig akkoord zou volgens de Libische autoriteiten besproken zijn met de Russische leiders op 01 november 2008¹⁸⁷. Het is duidelijk dat deze bilaterale akkoorden de globale perceptie van de geloofwaardigheid van het NPT kunnen ondermijnen. Men kan stellen dat het akkoord tussen India en de VS een gevaarlijk precedent vormt dat nu reeds voor opschudding zorgt omwille van commerciële en geostrategische belangen. Om deze trend te keren moet de voorziening van kernenergie op internationaal niveau geregeld worden, bijvoorbeeld onder de auspiciën van de Verenigde Naties als regulerend orgaan enerzijds en anderzijds het Internationaal Atoomagentschap, haar nucleaire waakhond, als uitvoerend orgaan. Een te onderzoeken piste is de handel in kernbrandstof te beperken tot materiaal dat lage concentraties splijtstof bevat (LEU) dat niet gebruikt kan worden in militaire programma's, vooropgesteld dat het geleverde land niet over aanrijningscapaciteit beschikt. In dit opzicht moeten de kerncentrales in aanbouw voorzien zijn om met dit type brandstof te kunnen functioneren: nieuwe licenties uitgaande van het IAEA kunnen zich hierop richten. In dit kader kan men ook voor de maritieme propulsie normen opleggen die gebruik van LEU i.p.v. HEU bevoordelen. Behalve de verlaagde risico's in geval van incidenten met schepen die geladen zijn met dit type brandstof, wordt het proliferatierisico drastisch verlaagd aan het einde van de levenscyclus: LEU

¹⁸⁶ Active Layered Theatre Ballistic Missile Defence (ALTBMD) zou operationeel moeten zijn tegen 2010.

¹⁸⁷ Agence France Presse report d.d. 01 November 2008 en Carnegie Proliferation News d.d. 04 november 2008.

is inderdaad weinig aantrekkelijk als basis voor kandidaat-proliferatoren gezien de verplichte aanrijningscyclus die de brandstof opnieuw zou moeten doorlopen.

We merken op dat we hier ook het domein van de commerciële belangen van landen betreden: in de huidige economische crisis zullen commerciële belangen van firma's eerder de overhand krijgen op de morele verplichting tot naleving van een verdrag dat door een Natie moet worden nageleefd. De meeste Naties hebben in het kader van het NPT een bijkomende waarborgovereenkomst afgesloten met het IAEA. Dit neemt niet weg dat de eerste controle van commerciële activiteiten een nationale aangelegenheid blijft. Een piste om ook op dit niveau de naleving van verdragen af te dwingen, kan men bekomen door een internationaal accreditatielabel toe te kennen (uitgevaardigd door het IAEA) aan bedrijven die voldoen aan de eisen van alle verdragen in verband met non-proliferatie. Zoals het ISO-label, zou een "compliance certificate" kunnen toegekend worden aan een bedrijf dat alle geatificeerde verdragen op het gebied van non-proliferatie naleeft. De invulling van eventuele sancties of embargo's ten opzicht van bedrijven die niet over dit label beschikken, zou dan ingevuld moeten worden door instanties die toezien op het correct verloop van commerciële activiteiten in dit domein met coherente en systematische rapportage naar het IAEA en de VN-veiligheidsraad: in dit kader is het mogelijk dat de meldingsplicht van de NSG-leden gekoppeld wordt aan een afdwingbaar actieplan.

Een andere mogelijkheid kan men vinden in het "markeren" van agentia, bronnen en materiaal van tweeërlei aard en het inventariseren van bestaande radiologische bronnen. Het land van oorsprong kan op die wijze steeds nagetrokken worden voor zover een internationale databank van merkers wordt aangelegd. Tot hier toe was de ondertekening van het FMCT (Fissile Material Cut-off Treaty) een hindernis omwille van de moeilijke controle en de onzekerheid over de geërfde stock uit de periode van de koude oorlog en de clandestiene productie: in de praktijk lijken vele controlemechanismen bruikbaar die reeds bestaan in het kader van het NPT¹⁸⁸. Het gebruik van "tracers" in nieuwe splijtstof is een te onderzoeken piste om ook dit verdrag nieuw leven in te blazen.

De chemische wapenconventie (CWC) is een efficiënt gecontroleerde conventie door de OPCW. Echter, de voorziene deadline voor vernietiging van alle chemische wapens tegen 29 april 2012, zoals goedgekeurd door de Conferentie van deelnemende Staten, lijkt moeilijker realiseerbaar dan initieel voorzien. De VS bijvoorbeeld, hebben nog 71000 ton chemische agentia te vernietigen tegen de vooropgestelde datum. Ook in dit aspect zal de economische crisis een rol spelen: ontmanteling kost immers geld zonder immers grote economische compensaties. Het is echter noodzakelijk voor de geloofwaardigheid van het systeem dat de vooropgestelde termijnen worden gerespecteerd: een eerste deadline was immers reeds voorzien in 2007. De faling van een verdrag in uitvoering zou immers ook andere verdragen (NPT e.a.) in het gedrang kunnen brengen. Meer nog dan het naleven van deadlines is de uitbreiding van het verdrag, naar het voorbeeld van het NPT (zie bijlage 2), een onontbeerlijk onderdeel van het werkschema. De universele uitbreiding van het CWC zou ook de laatste weerstand uit het Midden-Oosten kunnen breken om zich te engageren in het verdrag: in deze regio moeten Egypte, Irak en Libanon nog toetreden tot het verdrag. Op gebied van proliferatie is alles echter verbonden: zo lang Israël geen duidelijkheid zal verschaffen over haar kernwapenarsenaal, zal het moeilijk zijn deze landen over de streep te trekken om de chemische wapenconventie te ondertekenen. We weten ook dat het

¹⁸⁸ « A verifiable Fissile-Material Treaty as a Foundation for Nuclear Disarmament », transcript of a presentation held on 11 April 2007 at United Nations Headquarters, in *Disarmament 2007: Critical Disarmament Issues*, United Nations 2008, pp.1-26.

kernwapenarsenaal van Israël een existentiële kwestie is zolang het bestaansrecht van deze Staat niet wordt erkend door landen in de regio. Daarom is het zo belangrijk dat de universaliteit van deze verdragen wordt afgedwongen voor iedereen. Vandaar ook dat de kernwapenstaten meer terughoudendheid aan de dag zouden moeten leggen voor de levering van proliferatie gevoelig materiaal ook al worden hiermee economische belangen gediend. Ook het CWC is in zeker zin op die manier verbonden met het NPT. Ook in deze materie zal de herzieningsconferentie (gepland voor 2013) een belangrijke mijlpaal zijn, ware het maar om vooropgestelde doelstellingen te evalueren in het globaal kader van het non-proliferatie regime.

Wat de biologische wapenconventie (BTWC) betreft is er het blijvend probleem van het ontbreken aan controlemechanismen, zoals een aanvaard protocol voor de uitvoering van inspecties en opvolging van biologische activiteiten. Bovendien ontbreekt de politieke wil die noodzakelijk is om de naleving ervan te respecteren. Zowel in de biotechnologie als in de farmacologie rijst bovendien het probleem dat vele processen beschermd worden door patenten: inspecties, zo vreest men, zouden dus economische belangen kunnen ondermijnen door het blootleggen van productiegeheimen. Hierdoor krijgt het verdrag in de praktijk geen afdwingbare waarde. Nochtans werd een werkzaam controleapparaat opgebouwd in het kader van de UN Special Commission¹⁸⁹(UNSCOM), opgevolgd door de United Nations Monitoring Verification Commission¹⁹⁰ (UNMOVIC). Deze commissie heeft heel wat ervaring kunnen opbouwen: zowel in het kader van staalname, kwaliteitscontrole als het opbouwen van een internationaal netwerk van biologische laboratoria werd een schat van informatie verzameld¹⁹¹. Deelnemers aan deze commissies bevestigen dat niet de volledige productielijnen geïnspecteerd dienen te worden om te weten of een biologisch programma al dan niet van militaire aard is: staalname aan het einde van de productieketen of op het terrein kunnen volstaan om jaren na de activiteiten nog exploitierbare sporen te vinden. De opdracht van betrokken commissie is echter afgelopen en de opgebouwde structuur is grotendeels ontmanteld. Indien nog een toekomst weggelegd is voor dit verdrag, zal dit moeten aangemoedigd worden door vertrouwenwekkende maatregelen: hierin kan de EU een voortrekkersrol spelen door vrijwillige inspecties toe te staan en door middel van het ECDC op Europees vlak een netwerk uit te bouwen van experts en controlelaboratoria. Dit zou als voorbeeld kunnen dienen om een vernieuwde permanente structuur in het leven te roepen op niveau van de VN, evenwaardig aan het IAEA en OPCW. Het gezamenlijk standpunt van de EU uitgebracht op 20 maart 2006 voor de praktische uitvoeringsmodaliteiten van het verdrag en het voorgestelde programma voor de concrete aanpak van agendapunten in het vooruitzicht van de zevende opvolgingsconferentie van 2011 zijn hier een illustratie van. Deze aanpak moet ook in de nationale wetgeving terug te vinden zijn: een voorstel in die richting is hieronder terug te vinden onder de bespreking van ECDC en bioveiligheid: een internationale databank van incidenten, structurele rapportage en snelle waarschuwingsnetwerken en de rechtspersoonlijkheid van bioveiligheidscoördinatoren zijn slechts enkel mogelijke voorbeelden. Nochtans zullen deze initiatieven geen resultaat hebben zonder de medewerking van de grootmachten. De administratie BUSH is steeds tegenstander geweest voor een meer uitgesproken rol van een controleorgaan. De nieuwe VS-administratie heeft sinds januari 2009 reeds een wijziging van koers aangetoond in haar houding ten opzichte van kernwapenprogramma's. Indien dit zich ook voortzet naar de BTWC, kan de

¹⁸⁹ Actief van 1991 tot 1998 op basis van UNSCR 687 van 1991 in het kader van de crisis in Irak.

¹⁹⁰ Actief van 1999 tot 2008 op basis van UNSCR 1284 van 1999 als opvolging van UNSCOM.

¹⁹¹ Een uitgezuiverde publieke versie van hun bevindingen is beschikbaar onder de vorm van een Compendium op <http://www.un.org/Depts/unmovic/new/pages/compendium.asp>

aanzet van de EU en het voorgestelde mechanisme meer slagkracht geven in dit domein.

3.2.4. WMDC SAMENWERKING EN NATIONALE VERTEGENWOORDIGING

Zowel de NAVO als de EU hebben een WMD Centre in het leven geroepen. Het zou een onschatbare meerwaarde creëren indien deze beide instanties samen zouden vergaderen en hun actieplannen op elkaar afstemmen. Op die manier kan men het militaire luik van de NAVO aanvullen met een ruimer politiek luik dankzij de samenwerking met de EU. Bovendien zou de uitwisseling van informatie gemakkelijker tot stand kunnen komen. Idealiter zou men beide centra kunnen fusioneren om duplicatie te vermijden in verschillende organisaties. Bij een gebrek aan deze mogelijkheid kan men er alleszins voor zorgen dat permanente vertegenwoordigers in deze cellen dienst doen als liaisonofficier om de communicatiekanalen op permanente wijze open te houden. Een bijkomend voordeel dat men kan vinden in deze samenwerking is dat de het aantal deelnemende landen toeneemt (NAVO en EU samen vertegenwoordigen meer naties dan elke organisatie afzonderlijk). Men kan deze samenwerking nog verder doortrekken naar andere toepassingen: in de organisatie van de EU, werken de persoonlijke vertegenwoordiger van Mr.SOLANA (EU WMD Center) samen met de vertegenwoordiger “Counter Terrorism” van de EU: parallel zou men ook in het kader van de NAVO een gelijkaardige samenwerkingsstructuur antiterrorisme en WMD-bestrijding kunnen uitwerken. De NAVO heeft immers, samen met haar partners, sinds 2002 het “Partnership Action Plan on Terrorism” (PAP-T) opgestart: een multidisciplinaire aanpak tegen terrorisme wordt in dit kader nagestreefd. Lidstaten hebben zich geëngageerd om, zowel als lid van de Alliantie als van de VN en de OVSE, op lange termijn, politieke, economische, diplomatieke en militaire actie te coördineren in de strijd tegen het terrorisme. Zonder dat het expliciet wordt vernoemd in de doelstellingen van het actieplan dat tijdens de NAVO-top van Praag werd voorgesteld, past dit ook in het kader van de strijd tegen WMD-proliferatie. De realisatie van dergelijke samenwerking zal voorbereiding vereisen, maar de structuren bestaan: idealiter zouden principiële afspraken gemaakt kunnen worden tussen de secretaris-generaal van de NAVO en de Hoge Vertegenwoordiger voor buitenlandse politiek van de EU. Een eerste werkgroep zou vervolgens de harmonisatie van beide cellen kunnen uitwerken om op het gebied van proliferatie, terrorismebestrijding, tijdige waarschuwingsnetwerken, bescherming van kritische infrastructuur en noodplanning concrete samenwerking en verantwoordelijkheden af te lijnen. Het spreekt vanzelf dat ook nationale vertegenwoordigers in deze Centra vertegenwoordigd zullen moeten worden. Deze zullen idealiter de functie van liaisonofficier moeten kunnen invullen naar de nationale overheden.

3.2.5. “SOFT PROLIFERATION”

Het is duidelijk dat Internet gezorgd heeft voor de snelle verspreiding van informatie, maar ook toelaat om plannen, blauwdrukken en financiële transacties snel te laten verlopen. Deze vorm van “soft proliferatie” kan op zich verscheidene vormen aannemen. Buiten het Internet kunnen dezelfde transacties door koeriers uitgevoerd worden. Bovendien kan men zelfs ervaring in het vakgebied transfereren naar verschillende landen door fysieke personen zoals (ex-)medewerkers van

kernwapenprogramma's. Indien deze vorm van transfers gecontroleerd en ingeperkt moet worden, moeten ook hiervoor de middelen voorzien worden. In het kader van dit werk werd noch op nationaal, noch op internationaal niveau enige instantie gevonden die dit type activiteiten in kaart brengt, laat staan aan banden legt. Praktische voorbeelden van effectieve transfers van blauwdrukken werden echter meermaals vastgesteld (in mei 2008 werden nog blauwdrukken afkomstig van het KHAN netwerk vernietigd door de Zwitserse overheid). Een structuur zou deze activiteiten kunnen controleren: hiervoor moeten nationale cellen de informatie kunnen doorgeven naar een daartoe in het leven geroepen internationale instantie. Op nationaal niveau zou men deze "soft proliferation cel" kunnen laten kaderen in de activiteiten die aansluiten bij de Federale politie. In België kunnen zowel het FCCU als de cel terrorismebestrijding samenwerken om deze politionele activiteit uit te voeren. Het FCCU is enkel gericht op technische aspecten van Internetgebruik, maar zou gemandateerd kunnen worden om geselecteerde toegangen en informatiestromen langs het net te verhinderen. De cel Terrorismebestrijding zou in hetzelfde kader informatie- en geldtransfers in kaart kunnen brengen om zo eventuele netwerken bloot te leggen. Centralisatie en verwerking van gegevens kan vervolgens zorgen voor uitbating en rapportage op nationaal (bijvoorbeeld via een Nationale magistraat naar het CGCCR en het OCAD) alsook op internationaal vlak (naar het IAEA of een daartoe aangehechte cel). Het spreekt voor zich dat ook deze bijkomende taak nieuwe middelen aan personeel en materieel zal vereisen, maar dat bovendien een wettelijk kader zal moeten gecreëerd worden waarin zowel de definitie als de aanpak van "soft proliferatie" worden omschreven. De beste structurele benadering tot deze realisatie moet men zoeken op basis van een eenvormig internationaal kader, welk nationaal ingevuld kan worden.

3.2.6. NAAR EEN CEL RISICOANALYSE EN BESCHERMING KRITISCHE INFRASTRUCTUUR (CIP)

Dit onderzoek heeft aangetoond dat het uitermate belangrijk is om te vertrekken van eenduidige definities met betrekking tot risicoanalyse. Op nationaal vlak ligt hier een grote verantwoordelijkheid bij de CGCCR. De dreigingsanalyse wordt door OCAD regelmatig herzien. De mogelijke doelwitten zijn echter niet aangepast aan de databank CriViSen, noch aan de EPCIP-criteria. Bovendien is er geen regelmatige herziening van de impactanalyse hetgeen de risico-evaluatie hopeloos verouderd. Voorstel is om een nieuwe cel risicoanalyse samen te stellen: deze kan deel uitmaken van het CGCCR. Vertrekkende van een herziene versie van CriViSen die overeenkomt met de EPCIP-vereisten, dient men deze gegevens te koppelen aan de dreigingsanalyse van OCAD. Dit impliceert dat OCAD toegang heeft tot deze databank en bijgevolg gerichte analyses kan voorstellen. Hieruit kan de nieuwe cel risicoanalyse zowel de impactanalyse als het risico evalueren, telkens wanneer de bedreiging wordt herzien. De gebruikte methode werd hiervoor reeds vastgelegd in het FRISK-rapport. Aan de geëvalueerde risico's moeten maatregelen voor beveiliging gebonden worden, specifiek voor de betrokken infrastructuur welke van militaire of burgerlijke aard zal zijn. Mogelijkheden voor bemanning van voorgestelde cel zouden bijgevolg bij het militair- en politie-personeel gevonden kunnen worden: het personeel CNVV zou in dit verband vanaf de input van de dreigingsanalyse tot het eindresultaat betrokken kunnen worden bij de evaluatie van de risico's. Op die manier kan er ook eenvoudig terugkoppeling bestaan naar de militaire keten voor gebeurtenissen met zuiver militaire impact. Bovendien kan de cel aangevuld worden door politiemensen voor evaluatie van politionele maatregelen (ordehandhaving bijvoorbeeld).

Nog een laatste opmerking met betrekking tot CriViSen en EPCIP: logischerwijze zou men de bestaande nationale databank moeten aanpassen aan de EPCIP-criteria. Het zou best kunnen dat een beperkt aantal bijkomende punten in de databank, nationaal van belang blijken. Zonder daarom opnieuw tot een lijst van meer dan 13000 punten te komen, kan men de databank uitbreiden met de vermelding dat het betrokken punt omwille van nationale vereisten of EPCIP-criteria opgenomen is in de lijst. Een aangepaste cel, toegespitst op de bescherming van kritische infrastructuur (CIP) lijkt dus zeer aangewezen: deze kan op regelmatige basis de beschermingsmaatregelen aanpassen door het opvolgen van nieuwe technieken en toepassingen ervan.

3.2.7. WELKE CELLEN IN DE CGCCR?

In vorige punten werden voorstellen gedaan om nieuwe cellen te creëren en bestaande systemen aan te passen. De vraag dringt zich op welke cellen bijkomend opgenomen moeten worden in CGCCR. De cel « soft proliferation » heeft eerder een politionele bevoegdheid en hoeft niet noodzakelijk opgenomen worden in het Crisiscentrum. De bescherming van eigen ICT in het Crisiscentrum moet echter wel intern gegarandeerd worden. Hiervoor kan hulp gezocht worden bij FCCU. Het voorstel om ook de verantwoordelijke aanpak van « soft proliferation » bij FCCU te leggen, impliceert dat de informatie doorstroomt naar het Crisiscentrum en OCAD met betrekking tot dreigingsanalyse en risico-evaluatie.

De voorgestelde samenwerking tussen EU WMD Center en NATO WMDC veronderstelt eveneens een nationale vertegenwoordiging die verslag kan uitbrengen bij het Crisiscentrum.

Ten slotte hebben we nog de taken van het CNVV uitgebreid door de risico-evaluatie. Deze cel maakt reeds deel uit van het Crisiscentrum. De cel CIP is echter een nieuwe cel die ook in het CGCCR haar plaats vindt.

De gevolgen van deze bijkomende taken hebben vooral implicaties voor de informatiestroom, waarvan we reeds weten dat deze een zwakke schakel kan vormen gezien het enorm aantal gesprekspartners op verschillende niveaus: verwijzen we ter illustratie nogmaals naar bijlage 8. In dit kader zou het dus nuttig zijn om de communicatiecel van CGCCR te herstructureren: niet enkel de PR tijdens incidenten is belangrijk maar een efficiënte doorstroom van informatie door netwerking is even belangrijk voor de goede werking en “situation awareness” in het Crisiscentrum. Een rationalisatie van bestaande systemen voor snelle waarschuwing wordt verder nog behandeld, maar men moet zich bewust zijn dat correcte informatie van cruciaal belang is in alle aspecten van de besluitvorming, en des te meer in een Centrum dat verondersteld wordt een crisis te beheersen: het kan dus nuttig zijn om de structuur en de werking van de communicatiecel te herzien. Uiteindelijk is CGCCR de collector voor de verwerking van informatie en de besluitvorming ten voordele van de politieke verantwoordelijken. Communicatie is dus een centrale functie voor de verwerking van de inputs uit de verschillende cellen en kan niet beperkt worden tot een PR machine die voorgekauwde berichten moet bekend maken aan de bevolking.

3.2.8. NOODPLANNING CBRN

Het is vanzelfsprekend dat de middelen moeten gebruikt worden die beschikbaar zijn in de verschillende diensten die een CBRN-competentie bezitten. Voor Defensie betekent dit dat een ondersteunende rol weggelegd zal zijn ter zake, weze het voor de inzet van specifieke middelen die niet beschikbaar zijn in andere overheidsdiensten of voor de ondersteuning van logistieke capaciteit. Bovendien betekent dit dat Defensie pas ingezet kan worden “op aanvraag”. De uitvoering van deze opdracht is binnen Defensie reeds gepland. De invulling voor de uitvoering van deze opdracht is terug te vinden, zowel op strategisch niveau (een algemene politiek voor civiele-militaire wisselwerking) als op tactisch niveau (operationele richtlijnen voor “Homeland operations”¹⁹²). Dit betekent niet dat de omschrijving van de rol van eenheden van Defensie onduidelijk mag zijn in de noodplanning CBRN: deze mag zich niet beperken tot een opsomming van middelen waarop beroep gedaan kan worden, maar moet een gedetailleerde omschrijving van interdepartementele verantwoordelijkheden en middelen omvatten. Bovendien moeten specifieke incidentgerichte communicatieplannen voorafgaand aan (aanvraagprocedures), tijdens (middelen) en na interventies (rapportage) voorzien worden. Een interministerieel protocolakkoord tussen alle betrokken FODs en Defensie zal de symbolische hoeksteen vormen van de samenwerking tussen verschillende diensten. De invulling ervan dient echter volledig terug te vinden te zijn in het Noodplan CBRN, opgesteld door CGCCR.

3.2.9. ECDC EN BIOVEILIGHEID

Bioveiligheid, zoals deze studie heeft aangetoond, omvat zowel het aspect biosafety (veiligheid voor de werknemers, gebruikers in de dagelijkse manipulatie van bioagentia) als biosecurity (veiligheid tegen diefstal of het ongecontroleerd vrijkomen van bioagentia). Terwijl hevige discussies nog volop aan de gang zijn om de controle ervan volledig in handen te geven van de VN, dan wel daartoe nieuwe internationale structuren te creëren, kan men in deze materie een nieuwe rol zien voor het ECDC. Naar het voorbeeld van het CDC (Atlanta) zou het, specifiek voor Europa, de registratie en verspreiding kunnen verzorgen van alle besmettingshaarden: naast de “early-warning” naar andere landen, kan een “ad hoc task force” ter plaatse opereren om de nodige bewijzen van besmetting te vinden. Op die manier kunnen adequate behandelingsmethoden en gerichte profylaxie opgestart worden. Bovendien zou het ECDC ook kunnen zorgen voor de registratie van alle bioveiligheidscoördinatoren i.e. alle verantwoordelijke personen die op Europees grondgebied toezicht moeten houden op biologische activiteit (al dan niet commercieel). Dit impliceert dat elke lidstaat een rechtspersoonlijkheid zou moeten inbouwen in de taakomschrijving van deze functie. Het gevolg hiervan is dat aan elke biologische activiteit een juridische verantwoordelijkheid verbonden is in de persoon van de bioveiligheidscoördinator, die moet toezien op de problematiek van bioveiligheid in de volledige betekenis van het woord (biosafety en biosecurity). Deze deskundigen kunnen als officiële aanspreekpunten fungeren en als dusdanig opgenomen worden in een databank: doet zich een probleem voor binnen een lidstaat van de EU, dan kan men onmiddellijk alle bioveiligheidscoördinatoren, samen met de overkoepelende nationale instanties van het probleemgebied samenroepen om duidelijkheid te scheppen met betrekking tot het

¹⁹² Operaties die kaderen in de steun aan de Natie.

incident. Als het ECDC deze taak kan uitvoeren (in de veronderstelling dat de nodige middelen aan materieel en personeel worden verschaft), kan het een relais vormen naar de WHO. CDC Atlanta kan dit ook voor haar rekening nemen op het grondgebied van de VS. Beide instanties kunnen dus een schat aan informatie aanbrengen voor het WHO om de taak van waakhond in zake bioveiligheid op zich te nemen onder overkoepelend toezicht van de VN. Op die manier verkrijgt de WHO een met het IAEA gelijkaardig statuut dat in zake biologische toepassingen en incidenten volwaardige rapportering ten opzichte van de VN kan uitvoeren. De taak is hiermee niet rond: Azië, Afrika en Australië/Oceanië ontbreken nog aan dergelijke structuren. In een volgende fase zou per continent een dergelijke organisatie in het leven geroepen kunnen worden met dezelfde verantwoordelijkheden. Samen kunnen alle continenten met de nodige CDC-expertise deelnemen aan een commissie die vanuit biosanitair oogpunt toezicht houdt. Pas dan kan men op niveau van de WHO echt spreken over een gecentraliseerd toezicht dat antennes heeft over de hele wereld. Dit impliceert dat de rijkere landen eventueel zullen moeten bijdragen voor de opbouw van dergelijke centra elders in de wereld (bijvoorbeeld Afrika). Bioveiligheid is immers eenieders bekommernis en infectiehaarden kennen geen grenzen meer in deze globaliserende maatschappij. Investeren in o.m. een Afrikaans centrum is een inspanning die ook onze (bio-)veiligheid ten goede zal komen.

Dit voorstel houdt in dat geen nieuwe structuren uit de grond moeten “getoverd” worden met gedeeltelijke of overlappende bevoegdheden: de basis bestaat en is reeds in permanent contact met het WHO. Dit is de organisatie bij uitstek om deze informatie te beheren en beschikbaar te houden voor de VN, “het” forum bij uitstek voor snelle en universele verspreiding van crisisinformatie. De Algemene Vergadering van de VN is trouwens ook het officiële aanspreekpunt voor organisaties als IAEA, OPCW en CTBTO: het zou niet verstandig zijn om bioveiligheid los te koppelen van de vermelde problematiek die een universele aanpak vereist. Een afzonderlijke structuur creëren zou de garantie weghalen om alle Naties te kunnen bereiken met materiële, logistieke of intellectuele bijstand. In dit voorstel van coördinatie en controle kan men ook nieuwe initiatieven nemen om het BTWC nieuw leven in te blazen: in de plaats van de discussie te beperken tot de periodieke werkgroepvergaderingen zonder gevolg, kan voorgestelde structuur de basis vormen voor het uitwerken van controlesystemen binnen het verdrag. Deze hebben dan automatisch een structureel kader dat reeds in plaats is gesteld om ervoor te zorgen dat de genomen engagementen wordt nageleefd.

3.2.10. TIJDIGE WAARSCHUWINGSNETWERKEN: RATIONALISATIE EN INTEGRATIE VAN VERSCHILLENDE KETENS

Op Internationaal vlak hebben de VN inspanningen geleverd om de smokkel in WMD materiaal in kaart te brengen o.m. aan de grenzen van de EU. In dat opzicht werd door UNICRI het “Knowledge Management System” uitgebouwd: sinds 2003 heeft deze organisatie haar aandacht gericht op de smokkel van chemische, biologische, radiologische en nucleaire wapens en materialen. 25 landen werden zo onder het licht van de schijnwerpers gehouden om de dreiging te evalueren, die o.m. uitgaat van criminele groeperingen, en de betrokken activiteiten in de bestudeerde landen in kaart te brengen. Dit heeft geleid tot de redactie van rapporten die ernstige lacunes blootgelegd hebben in de gebruikte standaarden voor het vergaren en de uitwisseling van informatie. Samenwerking van de Europese Commissie, met technische ondersteuning van het IAEA, OPCW, EUROPOL, en Interpol, zou ervoor moeten zorgen dat zowel het vergaren van informatie, als de uitwisseling en

de uitbating vlotter gebeuren. Tijdens deze studie is gebleken dat de informatie die beschikbaar was in dit type verslagen helemaal niet tot bij het OCAD raakte.

Het “Knowledge Management System” werd in het leven geroepen om zowel de uitwisseling van informatie als de wisselwerking tussen nationale experts met betrekking tot CBRN incidenten te vereenvoudigen. In dit kader moeten een aantal standaarden vastgelegd worden in de fase “vroeg detectie” van dit type incidenten (liefst in hun voorbereidingsfase). Daarom is het nog merkwaardiger dat een nationale instantie als het OCAD niet systematische op de hoogte wordt gehouden van de activiteiten van deze groep. Men kan dus voorstellen om nationale vertegenwoordigers van EUROPOL/Interpol aan te stellen als nationale POC binnen de werkgroep. Op hun beurt kunnen zij dan de informatie doorgeven naar het OCAD: deze informatie is essentieel voor een goede evaluatie op nationaal vlak. Zonder een correct gestructureerd informatienetwerk is een adequate dreigingsanalyse onbestaand. In dit werk werd besproken waarom dit een essentiële eerste stap is in de globale risico-evaluatie die moet uitgevoerd worden in de schoot van het CGCCR. We moeten ons geen illusies maken over de communicatie tussen de internationale gesprekspartners: ook hier zijn tekorten vast te stellen. In de schoot van de EU blijkt de communicatie niet steeds door te stromen tussen de Commissie en het Secretariaat-generaal. Tijdens dit onderzoek werd hier niet verder op ingegaan, maar het is duidelijk dat de verbindingen tussen de verschillende partners, geïllustreerd aan de hand van bijlage 8, ingewikkeld is: daarbovenop komen eventuele interne communicatieproblemen binnen de voorgestelde afdelingen. Dit maakt het onmogelijk om een efficiënt netwerk tot stand brengen.

Ook op nationaal vlak kan er nog rationeler omgesprongen worden met de doorstroom aan informatie. De verschillende waarschuwingkanalen alsook hun verschillende internationale en nationale aanspreekpunten werden vermeld in deel 2 van dit werk. Meer in het bijzonder werden de verschillende Europese initiatieven voor de uitbouw van snelle waarschuwingketens besproken onder de initiatieven voor preventie en strijd tegen proliferatie (zie ook voetnoot 161). Een reëel radiologisch incident in augustus 2008 heeft aangetoond dat zelfs voor wat de radiologische informatie betreft, geen tijdige en duidelijke communicatie kon gegarandeerd worden op nationaal niveau. Voorstel hier is om het probleem aan te pakken in twee fasen: in eerste instantie zouden voor alle bestaande EU-informatienetwerken en databanken POCs moeten aangeduid worden per verantwoordelijke FOD. Deze zullen automatisch verslag moeten uitbrengen aan het CGCCR. Ondertussen zou het CGCCR werk kunnen maken van een coherent plan met betrekking tot de doorstroom van de informatie tussen de verschillende POCs (lees FODs): dit is onontbeerlijk voor de goede werking van het CGCCR. Vervolgens kan de informatie vormelijk gerationaliseerd worden: de informatie is soms onder de vorm van databanken, soms als internetberichtgeving beschikbaar. Zowel de keuze van de vorm als de bescherming van de informatieketen (ICT bescherming of andere vormen van informatieverwerking) zijn belangrijk voor de correcte en snelle verwerking van de gegevens: enerzijds kan men er voor zorgen dat een uniforme manier voor weergave van informatie zal toelaten om sneller de juiste contactpunten te kunnen aanspreken. Anderzijds zal de bescherming van de keten ervoor zorgen dat de informatie niet verloren gaat en dat de juiste instanties onmiddellijk en op adequate wijze kunnen reageren op een incident.

3.2.11. NAAR EEN EUROPEES “DEPARTMENT OF HOMELAND SECURITY” (EDHS)?

In de VS hebben de aanslagen van 9/11 aangetoond dat een interdepartementale aanpak noodzakelijk was voor het slagen van opdrachten in zake veiligheid van personen en diensten op nationaal grondgebied, hetzij defensief, hetzij proactief. Een voorstel tot de realisatie van deze structuur werd ingediend in juni 2002. Het U.S. Department of Homeland Security (USDHS¹⁹³) werd officieel in het leven geroepen op 1 maart 2003. In een klein land als België is een dergelijke structuur niet haalbaar, maar de benadering van het probleem en de initiatieven zijn op Europees niveau op vele vlakken gelijklopend. Men kan zich bijgevolg terecht de vraag stellen of een structuur voor een “Europees DHS” niet nuttig zou kunnen zijn in de coördinatie van de verschillende inspanningen voor het verbeteren van de Europese en bijgevolg ook de nationale veiligheid. De structuur van de Europese commissie die het beste aanleunt bij het USDHS kan men vinden in het “Directorate General Justice, Freedom and Security”¹⁹⁴ opgericht in oktober 1999. Integratie van de douanediens ten op Europees niveau zou de bestaande structuur kunnen verstevigen. Bovendien zou de cel die het programma beheert omtrent “bescherming van Europese kritische infrastructuur” bijgevoegd moeten worden in het organogram. Een beter uitwisseling tussen de inlichtingendiensten en een gemeenschappelijke Europese buitenlandse politiek, zouden de positie van een EDHS enkel ten goede kunnen komen.

Hoe ver men wil gaan in de hervorming tot voorgestelde structuur, moet vanuit een gemeenschappelijk standpunt ingevuld kunnen worden door de lidstaten: nationale vertegenwoordigers spelen hierin een cruciale rol om hun taken niet enkel op Europees niveau te spelen maar ook een relaisfunctie uit te oefenen naar het nationale niveau. Zo kan men Europese coördinatie op nationaal vlak in de praktijk te brengen. De belangrijkste taak van dit directoraat bestaat erin een wettelijke basis te creëren om van de EU-zone vrijheid, veiligheid en justitie tot hun recht te laten komen. Om dit doel te bereiken werden specifieke taken vastgelegd in de verdragen van Rome, Amsterdam, en Maastricht. Men kan echter aan iedere sectie van het organogram een uitvoerende rol toekennen die gericht is op internationale coördinatie in de verschillende directoraten. Nationale actoren zijn in elk van deze domeinen reeds actief voor de praktische uitvoering van deze taken op hun respectievelijke grondgebieden: het volstaat het geheel te integreren in de voorgestelde structuur met een degelijke wettelijk kader dat ook de praktische uitvoering van de supranationale samenwerking vastlegt. Men mag echter niet uit het oog verliezen dat een aangepaste structuur niet het wondermiddel bij uitstek zal zijn om het hoofd te kunnen bieden aan dreiging op eigen grondgebied: de persoonlijke ervaringen spelen hierin een complementaire rol. In deel twee werden verschillende aspecten van deze problematiek uiteengezet. Ook in de VS blijkt dat lang na de invoering van het US DHS men in januari 2009 nog moet vaststellen dat¹⁹⁵: “Custom officials understand how to screen and control people and things transiting borders. Emergency managers are well schooled in natural disasters but lack familiarity with terrorists’ capabilities. And law enforcement officers understand investigations but are not trained to manage events using the Incident Command System, which is the system first responders use to command and control response assets during a disaster.”

¹⁹³ Organogram beschikbaar op http://www.dhs.gov/xabout/structure/editorial_0644.shtm

¹⁹⁴ Organogram beschikbaar op http://ec.europa.eu/dgs/justice_home/organigramme_en.pdf

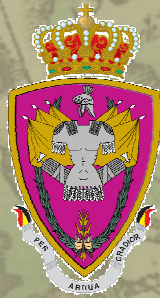
¹⁹⁵ WORMUTH, C., « The Next Catastrophe: Ready or Not? », in *The Washington Quarterly*, January 2009, p.102.

Het is duidelijk dat de capaciteiten van de individuen en de structuren elkaar zullen moeten aanvullen om een valabele meerwaarde te creëren in de geïntegreerde aanpak van een incident, zoals die werd voorgesteld in deel 2 van dit werk: het heeft geen enkele zin nieuwe structuren in het leven te roepen die geen meerwaarde hebben bij de uitvoering van de opdracht. De bedoeling moet nog steeds gericht zijn op een betere coördinatie van de voorbereiding en de uitvoering ten einde de nodige weerstand en veerkracht te kunnen bieden tijdens een incident.



3.3. Deelbesluit

In dit deel hebben we mogelijke pistes willen identificeren om zowel praktijkgerichte (tactische) als beleidsmatige (strategische) verbeteringen voor te stellen aan bestaande procedures, toepassingen, wetgeving en werking van internationale structuren. Sommige voorstellen zijn onderhevig aan beschikbaarheid van personeel en middelen: in de huidige context van financiële crisis zal het niet eenvoudig zijn om prioriteiten te leggen. Een verlaagde inspanning in de tactische en strategische veiligheidsmaatregelen omwille van budgettaire redenen zou echter een gevaarlijke keuze zijn: veiligheid is een essentieel onderdeel van de samenleving. Het wegvallen van waakzaamheid en middelen kan bijvoorbeeld de energiebevoorrading treffen, of de voedselketen. Een onmiddellijke weerslag op ons dagelijks leven is dus niet uitgesloten. Non-prolifерatie en actie tegen niet-staatsactoren is geen agendapunt dat opzij geschoven kan worden in barre tijden, maar is een werk van lange adem en ononderbroken inzet.



Algemeen Besluit





4. Algemeen Besluit

Op internationaal vlak is men verplicht in te zien dat op korte termijn (2009-2011) cruciale hindernissen zullen moeten genomen worden om het voortbestaan van het non-proliferatieregime te garanderen. Verder moet men vertrouwenwekkende maatregelen blijven koesteren door van ontwapening een prioriteit te maken. Het non-proliferatieregime houdt verdere ontwapening trouwens niet tegen: ontmanteling van bestaande stocks is een principe dat inherent is aan elk wapenverdrag. Indien de nakende herzieningsconferenties zonder resultaat worden afgesloten, kunnen op korte termijn tal van nieuwe kernwapenstaten opduiken: hiermee verhoogt het risico dat niet-staatsactoren onconventionele capaciteit bemachtigen. Regionale spanningen kunnen hierdoor uitmonden in ongeziene catastrofes met inzet van non-conventionele middelen.

Nationaal gezien heeft België geen eigen waardevolle grondstoffen. Meer dan andere landen is het economisch afhankelijk van import, export, dienstverlening, verwerkingscapaciteit en innovatie. Als gevolg daarvan, moet het land zich kunnen profileren als logistiek knooppunt in het licht van de wereldeconomie. Bovendien moeten omstandigheden gecreëerd worden die ervoor kunnen zorgen dat ons potentieel aan wetenschappelijke kennis en expertise niet kiest voor uitstroom. Om die reden is de infrastructuur zo belangrijk en moet ze permanent, op rationele wijze, vernieuwd en beveiligd worden. Bovendien moeten diensten gegarandeerd worden die het vertrouwen van de bevolking ten aanzien van de Staat bevestigen: het wegvallen van deze diensten of infrastructuur, zou, naast de fysische ontmanteling van de samenleving, een ernstige psychologische impact hebben op de bevolking. Deze studie heeft aangetoond hoe broos de bescherming van infrastructuur en de garantie van dienstbedeling nog is: pistes werden aangewezen om deze te verbeteren. Ook in het kader van militaire operaties in het buitenland, zal bescherming van vitale infrastructuur steeds een van de hoofdbekommernissen zijn. Behoud van aanvoer- en communicatielijnen is essentieel voor het welslagen van een opdracht voor expeditionaire troepen. Nationale vitale infrastructuur moet op dezelfde wijze behandeld worden om de continuïteit van de samenleving te garanderen. Bestaande nationale en internationale organisaties zijn in tal van domeinen actief om proliferatie in te dijken en noodplanning te organiseren. Men zal echter prioriteiten moeten leggen om duplicatie te vermijden tussen de verschillende structuren. Hiervoor zijn, buiten de nodige middelen, een coherente organisatie en doeltreffende communicatiekanalen van cruciaal belang. De invulling van de te volgen strategie moet niet beperkt worden tot één organisatie of één Natie.

Beleidsondersteunende maatregelen werden in het laatste deel van dit werk toegelicht. Exhaustiviteit was niet de hoofdbekommernis in de bespreking van deze maatregelen: bedoeling was om voor de gebreken die in deze studie naar voren zijn gekomen, een bruikbaar alternatief te formuleren zowel op tactisch als op strategisch gebied.

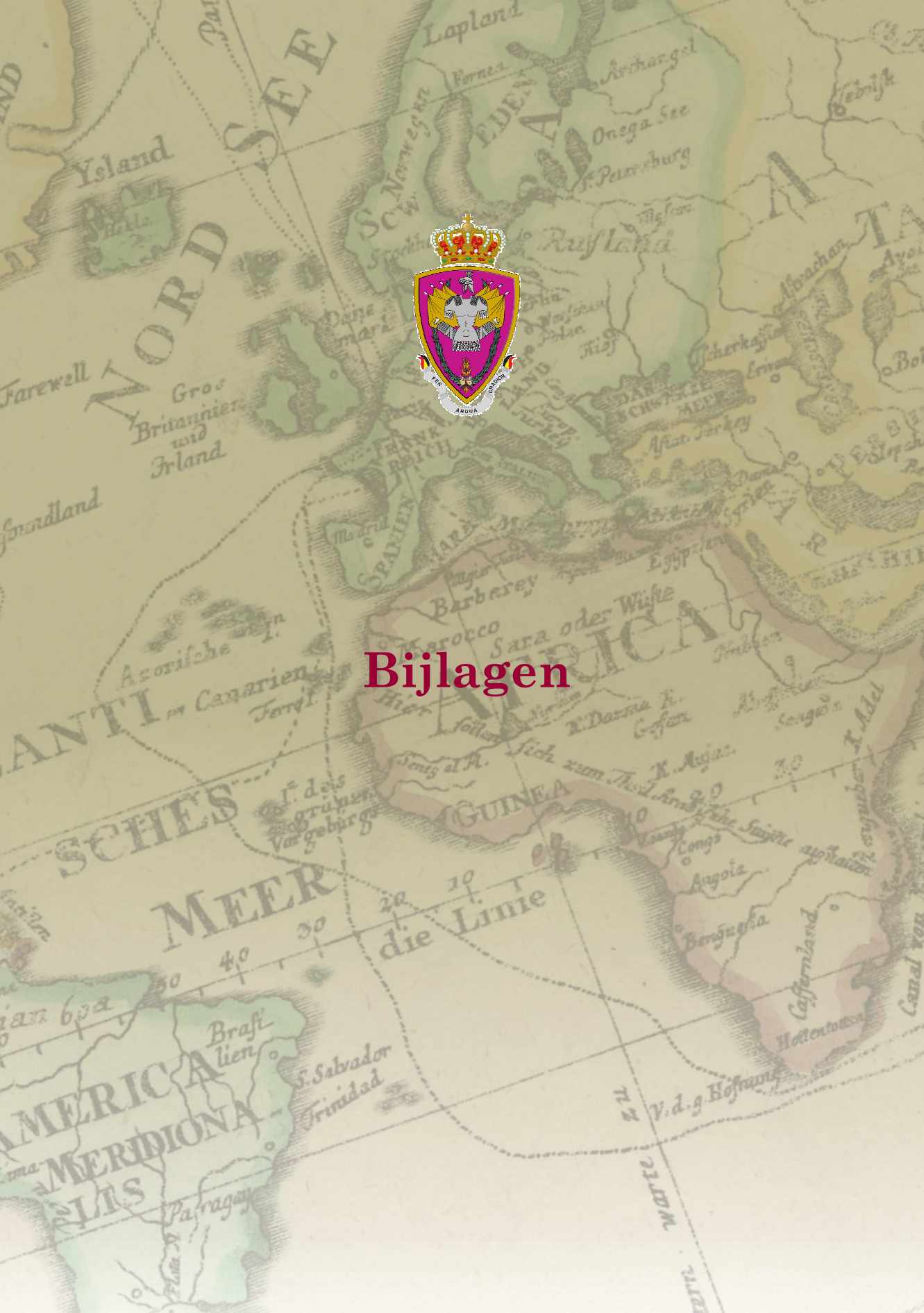
Deze studie heeft ook een aantal onontgonnen gebieden benaderd: zo is de problematiek van het raketterschild ter sprake gekomen zonder verder analyse. De nieuwe VS administratie zal in deze materie op korte termijn een strategie moeten uittekenen. In het verlengde hiervan is de bewapening van de ruimte niet uitvoerig ter

sprake gekomen. Ook dit aspect zal zijn weerslag hebben op het non-proliferatieregime. Op het vlak van energie, zeker in crisisperiodes, begint men zich, terecht, meer en meer zorgen te maken over de (on)afhankelijkheid van energievoorziening – zowel voor grondstoffen als infrastructuur - en mogelijke alternatieven: ook dit aspect is slechts raketings benaderd in het kader van het hergebruik van splijtstoffen. Niet alleen in het geval van splijtstoffen, maar in alle andere energiesectoren bestaat er een inherent veiligheidsrisico: mede om die reden zal men in de toekomst moeten toezicht houden op de globale controle van de keten op gebied van veiligheid, beschikbaarheid en prijs. De identiteit van allianties en unies ten slotte, is even ter sprake gekomen voor het deelgebied dat besproken werd. De aangeraden rationalisering van communicatiekanalen houdt ook hiermee verband: een herdefinitie van de eigen positie van supranationale instellingen dringt zich op. Op die manier kan duplicatie van inspanningen en verdunning van beschikbare middelen tegengaan worden. Op die manier kan men gecoördineerde samenwerking bevoordelen tussen verschillende organisaties om krachtlijnen af te tekenen en actieplannen op elkaar af te stemmen.

Wetenschappelijke studies, die oplossingen zouden kunnen brengen in deelgebieden van deze studie zijn tijdens dit onderzoek opgedoken. Zo is gebleken dat een specifiek algoritme vereist is voor de berekening van micro-meteorologische gegevens: in dit kader, moet men de stromingsdynamiek in kaart kunnen brengen, rekening houdend met het fenomeen “street channeling” en alle mogelijke metrokokers. Op het gebied van biodetectoren is nog werk te verrichten: hoewel analyses wel op punt staan, zijn bewakings- en detectiesystemen nog niet betrouwbaar in de huidige configuratie. De haalbaarheid voor een screening op biometrische gegevens vóór de betreding van druk bezochte zones is ook een piste die onderzocht zou moeten worden. Verschillende mogelijkheden bieden zich aan die in het kader van politionele activiteiten reeds gebruikt werden (oorbiometrie, irisscanning, handafdruk, antropomorfe gegevensverwerking, e.a.). Ten slotte zou men in de militair-civiele samenwerking in het kader van noodplanning beroep kunnen doen op de ervaring van “network centric capabilities” in operationele zones: hierdoor kan men enerzijds de communicatie beter beveiligen, maar eveneens de “situation awareness” bevorderen.



Bijlagen



Bijlage 1 : Tabel WMD-capaciteiten van landen

LAND	Kernkoppen^{5,6}	Biologisch⁴	Chemisch⁴	Raketten⁴
Rusland ¹	5000-10000	Wapens	Wapens in ontmanteling	ICBM
China ¹	145-240	Wapens	Wapens	ICBM
Verenigde Staten ¹	5000-10000	Wapens	Wapens in ontmanteling	ICBM
Frankrijk ¹	348	Wapens	Wapens	ICBM
Verenigd Koninkrijk ¹	160	Wapens	Wapens	ICBM
Israël ²	100-200	Programma (Non-BWC)	Wapens (Non-CWC)	SRBM
India ²	50-70	Programma	Wapens in ontmanteling	MRBM
Pakistan ²	60	Programma?	Programma?	MRBM
Noord-Korea ³	5-6?	Programma	Wapens (Non-CWC)	IRBM
Iran ³	Programma	Programma	Wapens?	MRBM
Egypte		Programma (Non-BWC)	Wapens (Non-CWC)	SRBM
Syrië		Programma	Wapens	SRBM
Zuid-Korea			Wapens in ontmanteling	
Lybië		?	Wapens in ontmanteling	SRBM
Albanië			Wapens in ontmanteling	

1: erkende kernmachten

2: de facto kernmachten niet onderworpen aan het non-proliferatieverdrag

3: landen in overtreding met het non-proliferatieverdrag

4: CIRINCIONE, J., WOLFSTHAL, J., RAJKUMAR, M., Deadly Arsenals: nuclear, biological

and chemical threats. Carnegie Endowment for International Peace, 2005, p.20.

5: Stockholm International Peace Research Institute, SIPRI Yearbook 2007, Summary. Armaments, Disarmament and International Security, Oxford, Oxford University Press, 2007, p.21 e.v. Ontplooid kernkoppen in januari 2007.

6: Global Fissile Material Report 2008, International Panel on Fissile Materials, Princeton University, September 2008, p.8. Het totaal voor de VS en Rusland is geschat op 10000, met een onzekerheid over het aantal ontplooide tuigen.

Bijlage 2 : Tekst uitbreiding van het NPT

NPT REVIEW AND EXTENSION CONFERENCE DECISION ON EXTENSION OF THE NON-PROLIFERATION TREATY

Adopted at New York on 11 May 1995

The Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear weapons,

Having convened in New York from 17 April to 12 May 1995, in accordance with article VIII, paragraph 3, and article X, paragraph 2, of the Treaty on the Non-Proliferation of Nuclear Weapons,

Having reviewed the operation of the Treaty and affirming that there is a need for full compliance with the Treaty, its extension and its universal adherence, which are essential to international peace and security and the attainment of the ultimate goals of the complete elimination of nuclear weapons and a treaty on general and complete disarmament under strict and effective international control,

Having reaffirmed article VIII, paragraph 3, of the Treaty and the need for its continued implementation in a strengthened manner and, to this end, emphasizing the decision on strengthening the review process for the Treaty and the decision on principles and objectives for nuclear non-proliferation and disarmament, also adopted by the Conference,

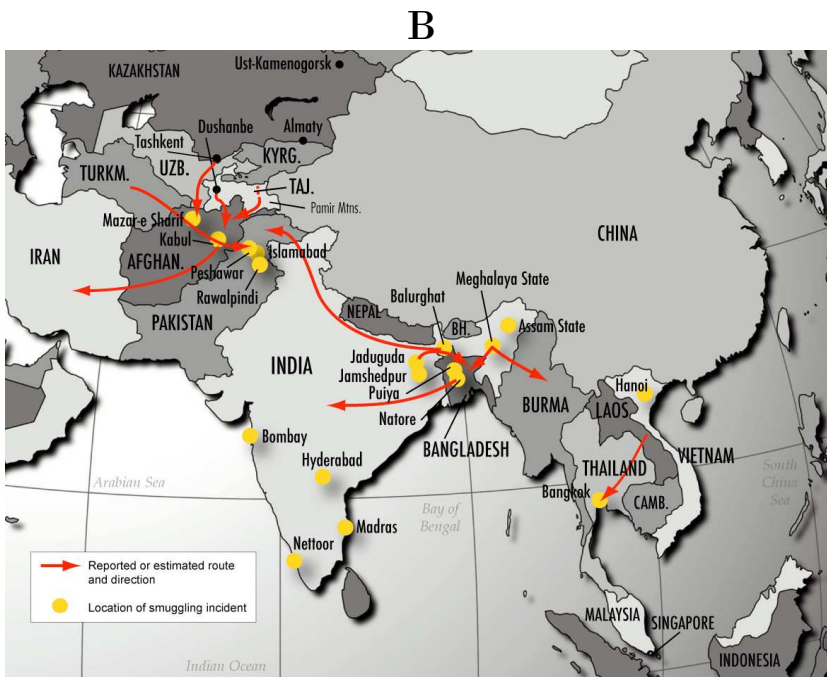
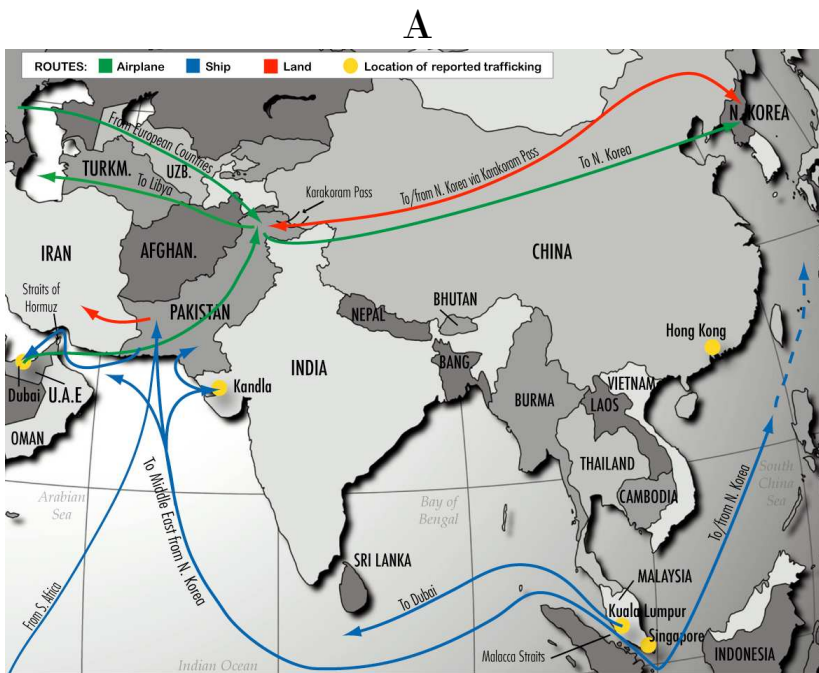
Having established that the Conference is quorate in accordance with article X, paragraph 2, of the Treaty,

Decides that, as a majority exists among States party to the Treaty for its indefinite extension, in accordance with its article X, paragraph 2, the Treaty shall continue in force indefinitely.

Bron:

Review and Extension Conference of the Parties to the Treaty on the Non-Proliferation of Nuclear Weapons, Final Document, NPT/CONF.1995/32 (Part I, decision 3), 1995.

Bijlage 3 : Smokkelroutes “Khan-netwerk”



Bron:

Andrew Prosser, Nuclear Trafficking Routes: Dangerous Trends in Southern Asia Nov. 22, 2004

Biljage 4 : Confirmed incidents involving HEU and Pu (1993-2006)

Incidents involving HEU and Pu confirmed to the ITDB, 1993-2006			
Date	Location	Material Involved	Incident Description
1993-05-24	Vilnius, Lithuania	HEU/ 150 g	4.4 t of beryllium including 140 kg contaminated with HEU were discovered in the storage area of a bank.
1994-03	St.Petersburg, Russian Federation	HEU/ 2.972 kg	An individual was arrested in possession of HEU, which he had previously stolen from a nuclear facility. The material was intended for illegal sale.
1994-05-10	Tengen-Wiechs, Germany	Pu/ 6.2 g	Plutonium was detected in a building during a police search.
1994-06-13	Landshut, Germany	HEU/ 0.795 g	A group of individuals was arrested in illegal possession of HEU.
1994-07-25	Munich, Germany	Pu/ 0.24 g	A small sample of PuO ₂ -UO ₂ mixture was confiscated in an incident related to a larger seizure at Munich Airport on 1994-08-10.
1994-08-10	Munich Airport, Germany	Pu/ 363.4 g	PuO ₂ -UO ₂ mixture was seized at Munich airport.
1994-12-14	Prague, Czech Republic	HEU/ 2.73 kg	HEU was seized by police in Prague. The material was intended for illegal sale.
1995-06	Moscow, Russian Federation	HEU/ 1.7 kg	An individual was arrested in possession of HEU, which he had previously stolen from a nuclear facility. The material was intended for illegal sale.
1995-06-06	Prague, Czech Republic	HEU/ 0.415 g	An HEU sample was seized by police in Prague.
1995-06-08	Ceske Budejovice, Czech Republic	HEU/ 16.9 g	An HEU sample was seized by police in Ceske Budejovice.
1999-05-29	Rousse, Bulgaria	HEU/ 10 g	Customs officials arrested a man trying to smuggle HEU at the Rousse customs border check point.
2000-12	Karlsruhe, Germany	Pu/ 0.001 g	Mixed radioactive materials including a minute quantity of plutonium were stolen from the former pilot reprocessing plant.
2001-07-16	Paris, France	HEU/ 0.5 g	Three individuals trafficking in HEU were arrested in Paris. The perpetrators were seeking buyers for the material.
2003-06-26	Sadahlo, Georgia	HEU/ ~170 g	An individual was arrested in possession of HEU upon attempt to illegally transport the material across the border.
2005-03 to 2005-04	New Jersey, USA	HEU/ 3.3 g	A package containing 3.3 g of HEU was inadvertently disposed of.
2005-06-24	Fukui, Japan	HEU/ 0.0017 g	A neutron flux detector was reported lost at an NPP.
2006-02-01	Tbilisi, Georgia	HEU/ 79.5 g	A group of individuals was arrested trying to illegally sell HEU.
2006-03-30	Hennigsdorf, Germany	HEU/ 47.5 g	Authorities discovered trace amounts of HEU on a piece of tube found amidst scrap metal entering a steel mill.

Bijlage 5: Europese definities kritische infrastructuur.

CIP TERMS AND DEFINITIONS

This indicative list of definitions could be further built upon depending on the individual sectors for the purpose of identification and protection of Critical Infrastructure (CI).

Alert

Notification that a potential disaster situation will occur, exists or has occurred. Direction for recipient to stand by for possible escalation or activation of appropriate measures.

Critical infrastructure protection (CIP)

The ability to prepare for, protect against, mitigate, respond to, and recover from critical infrastructure disruptions or destruction.

Critical Information Infrastructure (CII):

ICT systems that are critical infrastructures for themselves or that are essential for the operation of critical infrastructures (telecommunications, computers/software, Internet, satellites, etc.).

Critical Information Infrastructure Protection (CIIP)

The programs and activities of infrastructure owners, operators, manufacturers, users, and regulatory authorities which aim at keeping the performance of critical information infrastructures in case of failures, attacks or accidents above a defined minimum level of services and aim at minimising the recovery time and damage. CIIP should therefore be viewed as a cross-sector phenomenon rather than being limited to specific sectors. CIIP should be closely coordinated with Critical Infrastructure Protection from a holistic perspective.

Contingency plan

A plan used by a MS and critical infrastructure owner/operator on how to respond to a specific systems failure or disruption of essential service. Contingency plans would typically include the development, coordination, and execution of service- and site-restoration plans; the reconstitution of government operations and services; individual, private-sector, nongovernmental and public-assistance programs to promote restoration; long-term care and treatment of affected persons; additional measures for social, political, environmental, and economic restoration as well as development of initiatives to mitigate the effects of future incidents.

Critical Information

Specific facts about a critical infrastructure asset, vitally needed to plan and act effectively so as to guarantee failure or cause unacceptable consequences for critical infrastructure/installations.

Critical Infrastructure (CI)

Critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of Citizens or the effective functioning of governments.

There are three types of infrastructure assets:

- . Public, private and governmental infrastructure assets and interdependent cyber & physical networks.
- . Procedures and where relevant individuals that exert control over critical infrastructure functions.

- Objects having cultural or political significance as well as “soft targets” which include mass events (i.e. sports, leisure and cultural).

Essential service

Often applied to utilities (water, gas, electricity, etc.) it may also include standby power systems, environmental control systems or communication networks that if interrupted puts at risk public safety and confidence, threatens economic security, or impedes the continuity of a MS government and its services.

European critical infrastructure (ECI)

European critical infrastructure include those physical resources, services, and information technology facilities, networks and infrastructure assets, which, if disrupted or destroyed would have a serious impact on the health, safety, security, economic or social well-being of two or more MS. The definition of what constitutes an EU critical infrastructure is determined by its cross border effect which ascertains whether an incident could have a serious impact beyond two or more MS national territories. This is defined as the loss of a critical infrastructure element and is rated by the:

- extent of the geographic area which could be affected by the loss or unavailability of a critical infrastructure element beyond three or more Member State’s national territories;
- effect of time (i.e. the fact that a for example a radiological cloud might, with time, cross a border);
- level of interdependency (i.e. electricity network failure in one MS effecting another);

Impact

Impacts are the total sum of the different effects of an incident. This needs to take into account at least the following qualitative and quantitative effects:

- Scope - The loss of a critical infrastructure element is rated by the extent of the geographic area which could be affected by its loss or unavailability - international, national, regional or local.
- Severity - The degree of the loss can be assessed as None, Minimal, Moderate or Major.

Among the criteria which can be used to assess impact are:

- Public (number of population affected, loss of life, medical illness, serious injury, evacuation);
 - Economic (GDP effect, significance of economic loss and/or degradation of products or services, interruption of transport or energy services, water or food shortages);
 - Environment (effect on the public and surrounding location);
 - Interdependency (between other critical infrastructure elements).
 - Political effects (confidence in the ability of government);
 - Psychological effects (may escalate otherwise minor events), both during and after the incident and at different spatial levels (e.g. local, regional, national and international)
- Effects of time - This criteria ascertains at what point the loss of an element could have a serious impact (i.e. immediate, 24-48 hours, one week, other).

Interdependency

Identified connections or lack thereof between and within infrastructure sectors with essential systems and assets.

Occurrence

The term “occurrence” in the CIP context is defined as an event (either human caused or by natural phenomena) that requires a serious emergency response to protect life or property or puts at risk public safety and confidence, seriously disrupts the economy, or impedes the continuity of a MS government and its services. Occurrences include negligence, accidents, deliberate acts of terrorism, computer hacking, criminal activity and malicious damage, major disasters, urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, storms, public health and medical emergencies and other occurrences requiring a major emergency response.

Operator Security Plan

The Operator Security Plan (OSP) identifies all of the operator’s critical infrastructure assets and establishes relevant security solutions for their protection. The OSP describes the methods and procedures which are to be followed by the owner/operator.

Prevention

The range of deliberate, critical tasks and activities necessary to build, sustain, and improve the operational capability to prevent, protect against, respond to, and recover from an incident. Prevention involves efforts to identify threats, determine vulnerabilities and identify required resources. Prevention involves actions to protect lives and property. It involves applying intelligence and other information to a range of activities that may include such countermeasures as deterrence operations; heightened inspections; improved surveillance and security operations; investigations to determine the full nature and source of the threat; public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and as appropriate specific law enforcement operations aimed at deterring, pre-empting, interdicting, or disrupting illegal activity, and apprehending potential perpetrators and bringing them to justice. Prevention involves the stopping of an incident before it happens with effective processes, guidelines, standards and certification. Seamless interactive systems, and comprehensive threat- and vulnerability analysis. Prevention is a continuous process of ongoing actions to reduce exposure to, probability of, or potential loss from hazards.

Response

Activities that address the short-term direct effects of an incident. Response includes immediate actions to save lives, protect property, and meet basic human needs. As indicated by the situation, response activities include applying intelligence and other information to lessen the effects or consequences of an incident; increased security operations; continuing investigations into nature and source of the threat; ongoing public health and agricultural surveillance and testing processes; immunizations, isolation, or quarantine; and specific law enforcement operations aimed at pre-empting, interdicting, or disrupting illegal activity, and apprehending actual perpetrators and bringing them to justice.

Risk

The possibility of loss, damage or injury. The level of risk is a condition of two factors: (1) the value placed on the asset by its owner/operator and the impact of loss or change to the asset, and (2) the likelihood that a specific vulnerability will be exploited by a particular threat.

Threat

Any indication, circumstance, or event with the potential to disrupt or destroy critical infrastructure, or any element thereof. An all-hazards approach to threat includes accidents, natural hazards as well as deliberate attacks. It can also be defined as the

intention and capability of an adversary to undertake actions that would be detrimental to critical assets.

Vulnerability

A characteristic of an element of the critical infrastructure's design, implementation, or operation that renders it susceptible to destruction or incapacitation by a threat.

Bron:

Groenboek betreffende een Europees programma voor de bescherming van kritieke infrastructuur, Commissie van de Europese Gemeenschappen, Brussel, 2005, bijlage 1.

Bijlage 6: CBRN-oefeningen in de VS



July 31, 2008

Biohazard drill a 'success'

By *DOROTHY SCHNEIDER*
dschneider@journalandcourier.com

Emergency personnel worked to contain an anthrax contamination and deal with injuries, crowd control and even a woman in labor Wednesday at Lafayette's main post office.

Luckily, it was only a drill.

Emergency responders, firefighters, police officers, post office personnel, and health care and American Red Cross workers spent much of the afternoon simulating their response to a biohazard emergency and the complications that could ensue.

"If this ever happens (for real) it's going to be considered a weapon of mass destruction," said Kim Yates, customer relations coordinator for the U.S. Post Office. "We have to be prepared."

The mock biohazard drill was a success, according to those involved.

Tim Batta, deputy director of Tippecanoe County Emergency Management Agency, said there are a lot of steps involved in a response of this scale and going through the whole drill helps work out the kinks.

When the team goes back to critique the job later, Batta said, everyone will note different areas where improvements can be made.

Jim Eagy of Lafayette, a mail handler at the post office on Indiana 26, volunteered to be one of the people evacuated by emergency teams and put through decontamination. He had to go through a shower system that washed him down head to toe, which was pretty appealing given the hot weather.

But Eagy was more impressed by the response from the local team.

"It's making us feel more comfortable as postal workers to have all this aid that's going to come help us," he said. "It's fantastic."

The post office uses a biohazard detection system to continuously test loose particles in the mail. An alarm would go off in the case of a biohazard detection and calls would go out to local 911 dispatchers.

Cecil Frink, a U.S. Postal inspector, said the alarm systems are reliable and "if they do go off, it's going to be the real thing."

Those evacuated that needed decontamination were run through wash stations. Emergency personnel simulated washing people with injuries and practiced processing uninjured people through a truck shower system. The cleansers: Dawn dish soap and liquid Tide, universal to hazardous materials operations, Batta said.

In a real biohazard emergency, Batta said, workers would have to cut the contaminated clothes off an injured person.

"They'd go down to their birthday suit," he said, adding that curtains would be hung around the

washing stations. On Wednesday, workers scrubbed over clothes and those going through the showers wore bathing suits.

Contaminated clothes would be collected, along with the water used to rinse people off, and the materials would be disposed of by a contracted company after a real emergency.

After decontamination and treatment, antibiotics would be distributed to those exposed to the anthrax environment, said Ron Cripe, administrator of the Tippecanoe County Health Department.

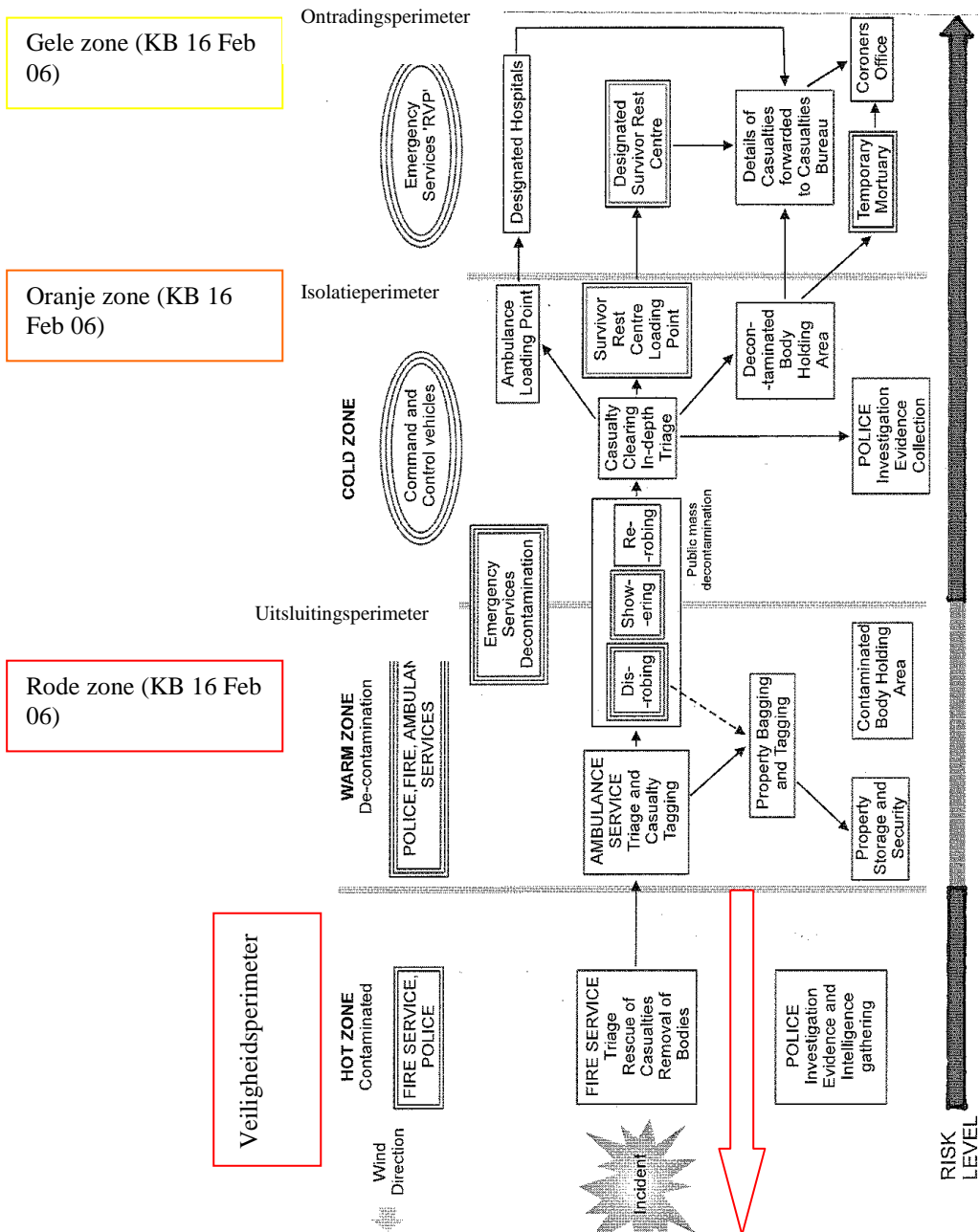
The department keeps limited amounts of anthrax medication on hand at all times, but more would be made available quickly in the event of a real emergency, Cripe said.

Yates said there's no increased concern about anthrax threats, but drills are done routinely at different post office locations to ensure preparedness. Two postal workers died from anthrax exposure in 2001 in Washington, D.C.

Bron:

www.jconline.com

Bijlage 7: Voorbeeld van organisatie van de zone in een CBRN-incident.

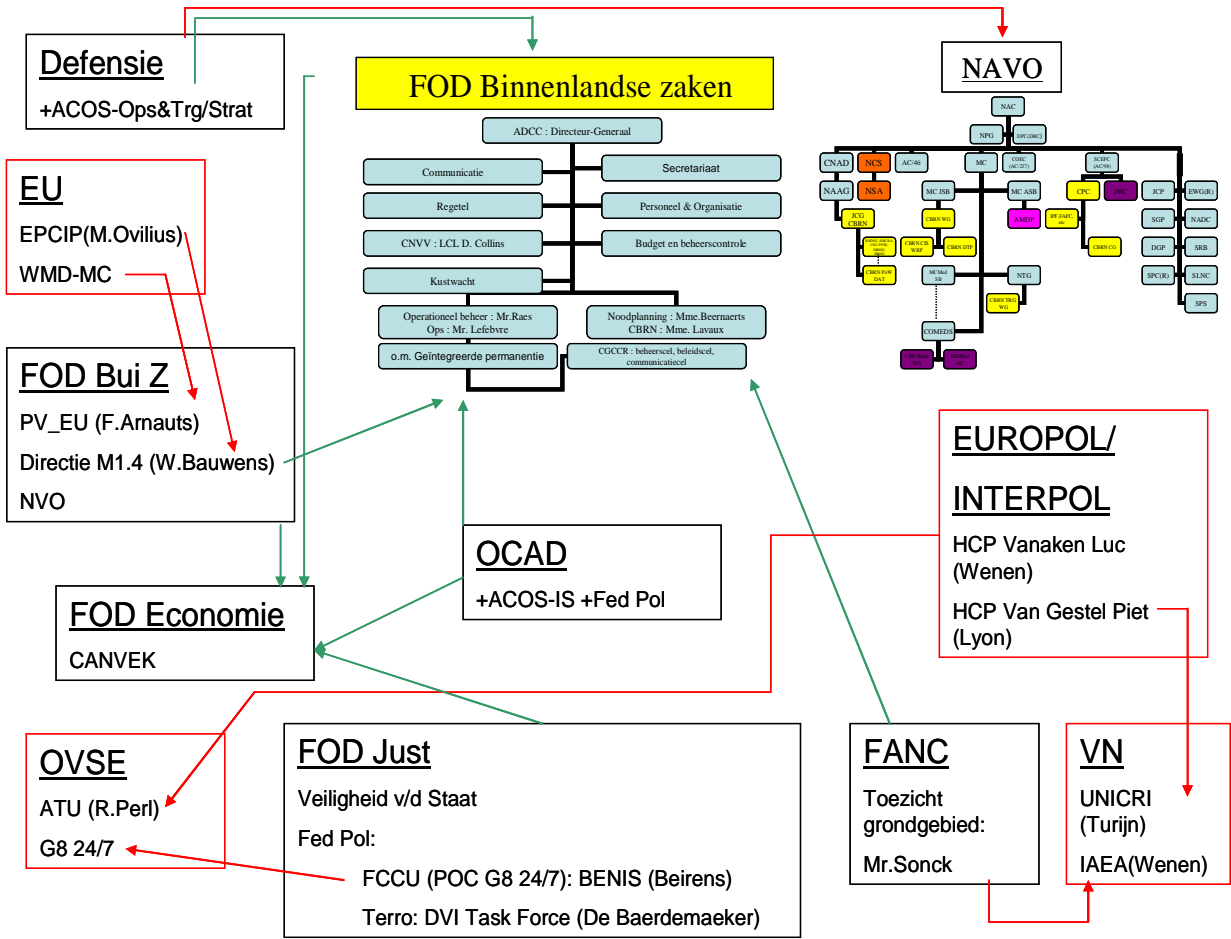


Bron:

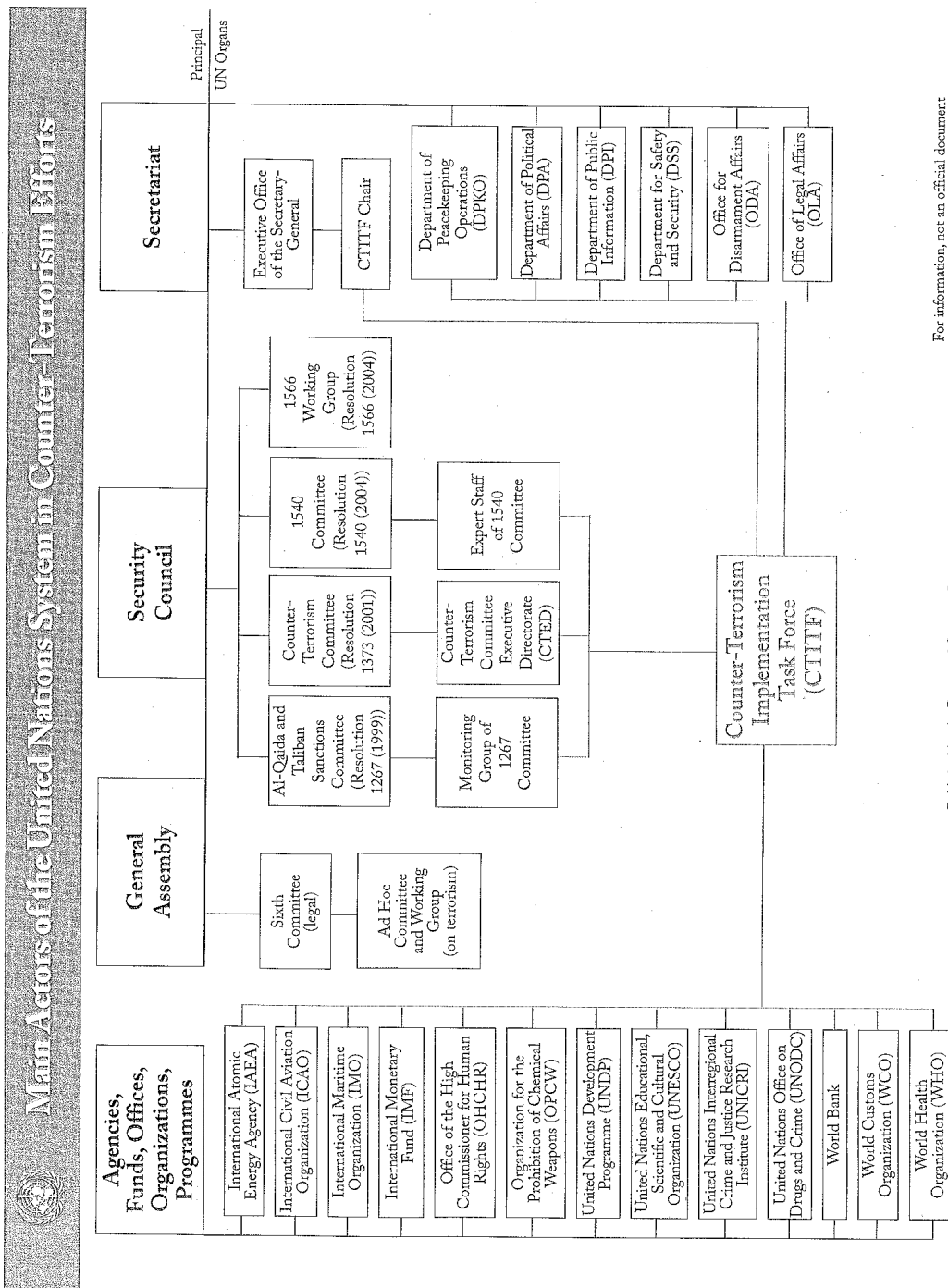
Schema aangepast uit:

Operations in the UK: The Defence Contribution to Resilience. Interim Joint Doctrine Publication 02. Ministry of Defence, December 2004, bijlage 9c en KB van 16 februari 2006; Ministeriële omzendbrief NPU-1 betreffende de nood- en interventieplannen.

Biilage 8: Nationale en internationale organen betrokken in noodplanning en WMD/CBRN aangelegenheden (niet exhaustief).



Bijlage 9: VN structuur « verdediging tegen terrorisme ».



Published by the Peace and Security Section of the United Nations Department of Public Information – December 2007
 For information, not an official document
 For more information, visit: <http://www.un.org/terrorism>

Bijlage 10: Instrumenten van de EU in het « CBRN Inventory ».

LIST OF INSTRUMENTS

In the alphabetical / chronological order:

Animal protection
Chemicals and dangerous substances
Chemical industries
Civil Protection
Customs
Environment protection
Food protection
Genetically Modified Organisms (GMOs)
Human health protection
Horizontal actions and overall coordination
Military support
Non-proliferation, Global disarmament and arms control
Pharmaceuticals for human use
Plant Protection and Plant Health Police
Radiological and nuclear protection
Research
Transport

Animal protection (see p. 45)

1. Council Directive 64/432/EEC of 26 June 1964 on animal health problems affecting intra-Community trade in bovine animals and swine.
2. Council Directive 82/894/EEC of 21 December 1982 on the notification of animal diseases within the Community (OJ L 378, 31.12.1982, p. 58). Directive last amended by Commission Directive 2004/21/EC of 1 March 2004 (OJ L 67, 5.3.2004, p. 27).
3. Council Directive 90/425/EEC of 26 June 1990 concerning veterinary and zootechnical checks applicable in intra-Community trade in certain live animals and products with a view to the completion of the internal market.
4. Council Decision 91/666/EEC of 11 December 1991 establishing Community reserves of foot-and-mouth disease vaccines, as amended by Decision 2001/181.
5. Council Directive 92/35/EEC of 29 April 1992 laying down control rules and measures to combat African horse sickness.
6. Council Directive 92/66/EEC of 14 July 1992 introducing Community measures for the control of Newcastle disease.
7. Council Directive 92/102/EEC of 27 November 1992 on the identification and registration of animals.

8. Council Directive 92/119/EEC of 17 December 1992 introducing general Community measures for the control of certain animal diseases and specific measures relating to swine vesicular disease.
9. Council Directive 93/119/EC of 22 December 1993 on the protection of animals at the time of slaughter or killing.
10. Council Directive 97/78/EC of 18 December 1997 laying down the principles governing the organisation of veterinary checks on products entering the Community from third countries (OJ L 024 , 30.1.1998, p. 9).
11. Council Directive 98/58/EC of 20 July 1998 concerning the protection of animals kept for farming purposes.
12. Regulation (EC) No 1760/2000 of the European Parliament and of the Council of 17 July 2000 establishing a system for the identification and registration of bovine animals and regarding the liability of beef and beef products and repealing Council Regulation (EC) No 820/97.
13. Council Directive 2000/75/EC of 20 November 2000 laying down specific provisions for the control and eradication of bluetongue.
14. Directive 2001/82/EC of the European Parliament and the Council of 6 November 2001 on a Community Code relating to veterinary medicinal products (OJ L 311, 28.11.2001, p. 1), as amended by Directive 2004/28/EC of 31 March 2004 (OJ L 136, 30.4.2004, p. 58).
15. Council Directive 2001/89/EC of 23 October 2001 on Community measures for the control of classical swine fever.
16. Commission Regulation (EC) 466/2001 setting maximum levels for certain contaminants in food.
17. Directive of the European Parliament and the Council 2002/32/EC of 7 May 2002 on undesirable substances in animal feed.
18. Council Directive 2003/85/EC of 29 September 2003 on Community measures for the control of foot-and-mouth disease.
19. Directive 2003/99/EC of the European Parliament and of the Council of 17 November 2003 on the monitoring of zoonoses and zoonotic agents, amending Council Decision 90/424/EEC and repealing Council Directive 92/117/EEC (OJ L 325, 12.12.2003, p. 31).
20. Council Regulation (EC) No 21/2004 of 17 December 2003 establishing a system for the identification and registration of ovine and caprine animals and amending Regulation (EC) No 1782/2003 and Directives 92/102/EEC and 64/432/EEC (OJ L 5, 9.1.2004, p. 8).
21. Council Directive 2005/94/EC of 20 December 2005 on Community measures for the control of avian influenza.

22. Council Regulation (EC) No 1/2005 of 22 December 2004 on the protection of animals during transport and related operations and amending Directives 64/432/EEC and 93/119/EC and Regulation (EC) No 1255/97.

Chemicals and dangerous substances (see p. 55) (*for transport, see at the end*)

23. Council Directive 67/548/EEC of 27 June 1967 on the approximation of the laws, regulations and administrative provisions relating to the classification, packaging and labelling of dangerous substances (OJ L 196, 16.8.1967, p. 1). Directive as last amended by Regulation (EC) No 807/2003 (OJ L 122, 16.5.2003, p. 36).
24. Council Directive 76/769/EEC of 27 July 1976 on the approximation of the laws, regulations and administrative provisions of the Member States relating to restrictions on marketing and use of certain dangerous substances and preparations (OJ L 262, 27.9.1976 p. 201). Directive as last amended by Commission Decision 2006/139/EC (OJ L 384, 29.12.2006, p. 94).
25. Council Directive 96/82/EC of 9 December 1996 on the control of major accident hazards involving dangerous substances (OJ L 10, 14.1.1997, p. 13), as amended by Council Directive 2003/105/EC of 12 December 2003 ("Seveso II Directive") (OJ L 345, 31.12.2003, p. 97).
26. Council Decision 98/685/EC of 23 March 1998 concerning the conclusion of the Convention on the Transboundary Effects of Industrial Accidents (OJ L 326, 3.12.1998, p. 1).
27. **Council Directive 98/24/EC of 7 April 1998 on the protection of the health and safety of workers from the risks related to chemical agents at work (fourteenth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) (OJ L 131, 5.5.1998, p. 11).**
28. Directive 1999/45/EC of the European Parliament and of the Council of 31 May 1999 concerning the approximation of the law, regulations and administrative provisions of the Member States relating to the classification, packaging and labelling of dangerous preparations (OJ L 200, 30.7.1999, p. 1). Directive as amended by Commission Directive 2001/60/EC (OJ L 226, 22.8.2001, p. 5).
29. Regulation (EC) No 304/2003 of the European Parliament and of the Council of 28 January 2003 concerning the export and import of dangerous chemicals (OJ L 63, 6.3.2003, p. 1). Regulation as last amended by Commission Regulation (EC) No 1376/2007 (OJ L 304, 24.11.2007, p. 14).
30. Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC (OJ L 136, 29.5.2007, p. 1).

Civil Protection (see p. 70)

31. Council Decision 91/396/EEC of 29 July 1991 on the introduction of a single European emergency call number OJ L 217, 6.8.1991, p. 31.
32. Exchange of letters between UNOCHA and the Commission concerning their cooperation in the framework of disaster response (in case of simultaneous interventions in a country affected by a disaster) signed, on 28 October 2004, by Commissioners Wallström and Nielson and by Under-Secretary-General of the UN Jan Egeland (16339/04)
33. Council Decision 2007/162/EC, Euratom of 5 March 2007 establishing a Civil Protection Financial Instrument (OJ L 71, 10.3.2007, p. 9).
34. Commission Decision 2007/606/EC, Euratom of 8 August 2007 laying down rules for the implementation of the provisions on transport in Council Decision 2007/162/EC, Euratom, establishing a Civil Protection Financial Instrument (OJ L 241, 14.9.2007, p. 17).
35. Council Decision 779/162/EC, Euratom of 6 December 2007 establishing a Community Civil Protection Mechanism (Recast),(OJ L 314, 1.12.2007, p. 9; declarations for the minutes: 13459/07).
36. Commission Decision 2008/73, EC, Euratom, of 20 December 2007 amending Decision 2004/779/EC, Euratom as regards rules for the implementation of Council Decision 779/EC, Euratom establishing a Community Civil Protection Mechanism (OJ L 20, 24.1.2008, p. 23).

Critical infrastructure protection (see p. 68)

37. p.m.

Environment protection (see p. 54)

38. Council Directive 75/440/EEC of 16 June 1975 concerning the quality required of surface water intended for the abstraction of drinking water in the Member States (OJ L 194, 25.7.1975, p. 26).
39. Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).
40. Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2003 on public access to environmental information and repealing Council Directive 90/313/EEC (OJ L 41 , 14/02/2003, p. 26.)
41. Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE) (OJ L 108, 25.4.2007, p. 1).

Feed and Food protection (see p. 38)

42. Council Directives 76/895/EEC, 86/362/EEC, 86/363/EEC and 90/642/EEC fixing maximum limits for Pesticide Residues on feed and foodstuffs
43. Regulation 178/2002/EC of 28.01.2002 laying down the general principles and requirements of food law, establishing the European Food Safety Authority and laying down procedures in matters of food safety (OJ L 31 of 1.2.2002, p. 1). Regulation as amended by Regulation (EC) No 1642/2003 (OJ L 245, 29.9.2003, p. 4) and by Commission Regulation (EC) No 575/2006 of 7 April 2006 (OJ L 100, 8.4.2006, p. 3).
44. Regulation (EC) No 852/2004 of 29 April 2004 on the hygiene of foodstuffs (OJ L 139, 30.4.2004, p. 1).
45. Regulation (EC) No 853/2004 of 29 April 2004 laying down specific hygiene rules for food of animal origin (OJ L 139, 30.4.2004, p. 55).
46. Regulation (EC) No 854/2004 of 29 April 2004 laying down specific rules for the organisation of official controls on products of animal origin intended for human consumption (OJ L 139, 30.4.2004, p. 206).
47. Regulation (EC) No 882/2004 of the European Parliament and of the Council of 29 April on official controls performed to ensure the verification of compliance with feed and food law, animal health and animal welfare (OJ L 191, 28.5.2004, p. 1).
48. Commission Regulation (EC) No 2230/2004 of 23 December 2004 laying down detailed rules for the implementation of European Parliament and Council Regulation (EC) No 178/2002/EC with regard to the network of organisations operating in the fields within the European Food Safety Authority's mission (OJ L 379, 24.12.2004, p. 64).
49. Regulation (EC) No 183/2005 of 8 February 2005 laying down requirements for feed hygiene (3677/04).
50. Regulation EC No 396/2005 of the European Parliament and of the Council of 23 February 2005 on maximum residue levels of pesticides in or on food and feed or plant and animal origin and amending Council Directive 91/414/EEC (OJ L 70, 16.3.2005, p. 1).
51. Commission Regulation (EC) No 776/2006 of 23 May 2006 amending Annex VII to Regulation (EC) No 882/2004 of the European Parliament and of the Council as regards Community reference laboratories (OJ L 136, 24.5.2006, p. 3).
52. Commission Regulation (EC) 1881/2006 setting maximum levels for certain contaminants in food.

Genetically Modified Organisms (GMOs) and biological agents (see p. 51)

53. Council Directive 90/219/EEC of 23 April 1990 on the contained use of genetically modified micro-organisms (OJ L 117, 8.5.1990, p. 1). Directive as last amended by Regulation (EC) No 1882/2003 of the European Parliament and of the Council (OJ L 284, 31.10.2003, p. 1).

54. **Directive 2000/54/EC of the European Parliament and of the Council of 18 September 2000 on the protection of workers from the risks related to exposure to biological agents at work (OJ L 262, 17.10.2000, p. 21).**
55. Directive 2001/18/EC of the European Parliament and of the Council on the Deliberate Release into the Environment of Genetically Modified Organisms and repealing Council Directive 90/220/EEC (OJ L 106, 17.4.2001, p. 1).
56. Council Decision 2002/628/EC of 25 June 2002 concerning the conclusion, on behalf of the European Community, of the Cartagena Protocol on Biosafety (OJ L 201, 31.7.2002, p. 48).
57. Regulation(EC) No 1946/2003 of the European Parliament and of the Council of 15 July 2003 on transboundary movements of genetically modified organisms (OJ L 287, 5.11.2003, p. 1).
58. Regulation (EC) No 1830/2003 of the European Parliament and of the Council, of 22 September 2003 concerning the traceability and labelling of genetically modified organisms and the traceability of food and feed products from genetically modified organisms and amending Directive 2001/18/EC (OJ L 268, 18.10.32003, p. 24).
59. Regulation (EC) No 1829/2003 of the European Parliament and of the Council of 22 September 2003 on genetically modified food and feed (OJ L 268, 18.10.2003, p. 1).
60. Commission Regulation (EC) No 65/2004 establishing a system for the development and assignment of unique identifiers for genetically modified organisms (OJ L 10, 16.1.2004, p. 5).

Human health protection (see p. 23)

(including occupational health and safety)

61. **Council Directive 89/391/EEC of 12 June 1989 on the introduction of measures to encourage improvements in the safety and health of workers at work (OJ L 183, 29.6.1989, p. 1).**
62. **Council Directive 98/24/EC of 7 April 1998 on the protection of the health and safety of workers from the risks related to chemical agents at work (fourteenth individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) (OJ L 131, 5.5.1998, p. 11).**
63. Decision 2119/98/EC of the European Parliament and of the Council of 24 September 1998 setting up a network for the epidemiological surveillance and control of communicable diseases in the Community (OJ L 268, 3.10.1988, p. 1). Decision at last amended by Commission Decision 2007/875/EC (OJ L 344, 28.12.2007, p. 48)
64. Commission Decision 2000/57/EC of 22 December 1999 on the early warning and response system for the prevention and control of communicable diseases under Decision 2119/98/EC of the European Parliament and of the Council, OJ L 21 (26.1.2000, p. 32). Decision as amended by Commission Decision 2008/351/EC of 28 April 2008 (OJ L 117, 1.5.2008, p. 40).

65. Commission Decision 2000/96/EC of 22 December 1999 on the communicable diseases to be progressively covered by the Community network under Decision 2119/98/EC (OJ L 28, 3.2.2000, p. 50). Decision as last amended by Commission Decision 2007/875/EC (OJ L 344, 28.12.2007, p. 48).
66. **Directive 2000/54/EC of the European Parliament and of the Council of 18 September 2000 on the protection of workers from the risks related to exposure to biological agents at work (OJ L 262, 17.10.2000, p. 21).**
67. Council conclusions of 15 November 2001 on bioterrorism (13826/01, p. 12).
68. Programme of the Health Security Committee (HSC) of 17 December 2001 on cooperation on preparedness and response to biological and chemical agent attacks (health security).
69. Commission Decision 2002/253/EC of 19 March 2002 laying down case definitions for reporting communicable diseases to the Community network under Decision No 2119/98/EC (OJ L 86, 3.4.2002, p. 44). Decision as last amended by Commission Decision 2003/534/EC of 17 July 2003, OJ L 184, 23.7.2003, p. 35 and Commission Decision 2008/.../EC of 28 April 2008 (OJ L ..., p. ..).
70. Decision 1786/2002/EC of the European Parliament and of the Council, of 23 September 2002, establishing a programme of Community action in the field of public health (2003-2008) (OJ L 271, 9.10.2002, p. 1).
71. Commission Decision 2003/534/EC of 17 July 2003 amending Decision No 2119/98/EC of the European Parliament and of the Council and Decision 2000/96/EC as regards communicable diseases listed in those decisions and amending Decision 2002/253/EC as regards the case definitions for communicable diseases (OJ L 184, 23.07.2003, p. 35).
72. Regulation (EC) No 851/2004 of the European Parliament and of the Council of 21 April 2004 establishing a European Centre for Disease Prevention and Control (OJ L 142, 30.4.2004, p. 1).
73. Council conclusions of 2 and 3 June 2004 on Community Influenza Pandemic Preparedness Planning (9507/04).
74. World Health Assembly Resolution WHA 58.3 of 23 May 2005 on the Revised International Health Regulations.
75. Council conclusions of 5 February 2007 on the Communication from the Commission to the Council on the transitional prolongation and extension of the mandate of the Health Security Committee in view of a future general revision of the structures dealing with health threats at EU level (5862/07).
76. Decision 1350/2007/EC of the European Parliament and of the Council of 23 October 2007 establishing a second programme of Community action in the field of public health (2008-2013) (OJ L 301, 20.11.2007, p. 3).

Overall coordination (see p. 86)

77. Commission Decision 2006/25/EC, Euratom of 23.12.2005 amending its internal Rules of Procedure(OJ L 19, 24.1.2006, p. 20). (Introduction of ARGUS).
78. EU Emergency and Crisis Coordination Manual (CCA) (10011/1/07).

Military support (see p. 80)

79. p.m.

Non-proliferation, Global disarmament and Arms control (see p. 21)

80. Treaty on the Non-Proliferation of Nuclear Weapons.
81. Chemical Weapons Convention.
82. Biological Weapons Convention.
83. Council Regulation 1334/2000/EC setting up a Community regime for the control of exports of dual-use items and technology.
84. Joint Actions on the International Atomic Energy Agency : OJ L 165, 17.6.2006, p. 20; OJ L 193, 23.7.2005, p. 44; OJ L 182, 19.5.2004, p. 46.
85. Joint Actions on the Comprehensive Nuclear Test Ban Treaty Organisation : OJ L 176, 6.7.2007, p. 31; OJ L 88, 25.3.2006, p. 68.
86. Joint Actions on the Organisation for the Prohibition of Chemical Weapons : OJ L 85, 27.3.2007, p. 10, OJ L 331, 17.12.2005, p. 34, OJ L 349, 25.11.2004, p. 63.
87. Council Joint Action 2006/184/CFSP of February 2006 in support of the Biological and Toxin Weapons Convention, in the framework of the EU Strategy against the Proliferation of Weapons of Mass Destruction (OJ L 65, 7.3.2006, p. 51).
88. EU Action Plan on biological and toxin weapons, complementary to the EU Action Plan in support of BTWC (OJ C 57, 9.3.2006, p. 1).
89. Council Joint Action 2006/419/CFSP in support of the implementation of United Nations Security Council Resolution 1540 (2004) and in the framework of the implementation of the EU Strategy against the proliferation of Weapons of Mass Destruction, OJ L 165, 17.6.2006, p. 30.
90. Joint Action on the Security Proliferation Initiative : see 9211/04 and 10052/04.
91. Council Joint Action 2008/307/CFSP of 14 April 2008 in support of World Health Organisation activities in the area of laboratory bio-safety and bio-security in the framework of the European Union Strategy against the proliferation of Weapons of Mass Destruction (OJ L106, 16.4.2008, p. 17).

92. Common Positions :
 OJ L 176, 6.7.2007, p. 39, (CWC)
 OJ L 61, 28.2.2007, p. 49, (Iran)
 OJ L 88, 25.3.2006, p. 65, (BTW)
 OJ L **106**, 27.4.2005, p. 32, (NPT)
 OJ L 302, 20.11.2003, p. 34 (universalisation).

Pharmaceuticals for human use (see p. 77)

93. Directive 2001/83/EC of the European Parliament and of the Council of 6 November 2001 on the Community code relating to medicinal products for human use (OJ L 311, 28.11.2001, p. 1).
94. Council Regulation (EC) 726/2004 laying down Community procedures for the authorisation and supervision of medicinal products for human and veterinarian use and establishing a European Medicines Agency.
95. Commission Directive 2004/27/EC amending Directive 2001/83/EC on the Community code relating to medicinal products for human use.
96. Council conclusions of 6 December 2004 on a European response to emerging zoonotic diseases (16051/04).

Plant Protection and Plant Health (see p. 49)

97. International Plant Protection Convention **signed at Rome on 6 December 1951**.
98. Council Directive 91/414/EEC of 15 July 1997 concerning the placing of plant protection products on the market (OJ L 230, 19.8.1991, p. 1).
99. Council Directive 2000/29/EC of 8 May 2000 on protective measures against the introduction into the Community of organisms harmful to plants or plant products and against their spread within the Community and related regulations (OJ L 169, 10.7.2000, p. 1). Directive as last amended by Commission Directive **2007/41/EC of 28 June 2007 (OJ L 169, 26.9.2007, p. 51)**.
100. Regulation (EC) 396/2005 of the European Parliament and the Council of 23 February 2005 on maximum residue levels of pesticides in or on food and feed of plant and animal origin and amending Council Directive 91/414/EEC (OJ L 70, 16.3.2005, p. 1).

Police, security and intelligence (see p. 17)

101. Regulation (EC) No 2580/2001 on specific restrictive measures directed against certain persons and entities with a view to combating terrorism (OJ L 344, 28.12.2001, p. 93).
102. Council Framework Decision 2002/465/JHA of 13 June 2002 on Joint Investigation Teams (OJ L 162, 20.6.2002, p. 1)
103. Council Agreement 2003/C 1212/01 of 8 May 2003 on a model agreement for setting up joint investigation teams (JIT) (OJ C 121, 25.3.2003, p. 1).

Radiological and nuclear protection (see p. 61)

104. Council Decision 80/565/Euratom of 9 June 1980 approving the conclusion by the Commission of the International Convention on the Physical Protection of Nuclear Material (OJ L 149, 17.06.1980, p. 41).
105. Council Decision 87/600/Euratom of 14 December 1987 on Community arrangements for the early exchange of information in the event of a radiological emergency (ECURIE (OJ L 191, 27.7.2000, p. 37).
106. Council Regulation No 3954/87/Euratom of 22 December 1987 laying down maximum permitted levels of radioactive contamination of foodstuffs and of feeding stuffs following a nuclear accident or any other case of radiological emergency (OJ L 371, 30.12.1987, p. 11). Regulation as amended by Council Regulation No 2218/89/Euratom of 18 July 1989 (OJ L 211, 27.7.1989, p. 1).
107. Commission Regulation No 944/89/Euratom of 12 April 1989 laying down maximum permitted levels of radioactive contamination in minor foodstuffs following a nuclear accident or any other case of radiological emergency (OJ L 101, 13.4.1989, p. 17).
108. Council Regulation No 2219/89/EEC of 18 July 1989 on the special conditions for exporting foodstuffs and feeding stuffs following a nuclear accident or any other case of radiological emergency (OJ L 211, 22.7.1989, p. 4).
109. Council Directive 89/618/Euratom of 27 November 1989 on informing the general public about health protection measures to be applied and steps to be taken in the event of a radiological emergency (OJ L 357, 7.12.1989 p. 31).
110. Council Regulation No 737/90/EEC of 22 March 1990 on the conditions governing imports of agricultural products originating in third countries following the accident at the Chernobyl nuclear power-station (OJ L 82, 30.3.1990, p. 1). Regulation as amended by Council Regulation No 616/2000 of 20 March 2000 (OJ L 75, 24.3.2000, p. 1).
111. Commission Regulation No 770/90/Euratom of 29 March 1990 laying down maximum permitted levels of radioactive contamination of feeding stuffs following a nuclear accident or any other case of radiological emergency (OJ L 83, 29.03.90, p. 78).
112. Council Directive 90/641/Euratom of 4 December 1990 on *the operational protection of outside workers exposed to the risk of ionizing radiation during their activities in controlled areas* (OJ L 349, 13.12.1990 p. 21).
113. Commission Communication 91/C103/03 on the implementation of Council Directive 89/618/Euratom (OJ C 103, 19.4.1991, p. 12).
114. Council Directive 92/3/Euratom of 3 February 1992 on the supervision and control of shipments of radioactive waste between Member States and into and out of the Community (OJ L 35, 12.2.1992, p. 24).
115. Council Regulation No 1493/93/Euratom of 8 June 1993 on *shipments of radioactive substances between Member States* (OJ L 148, 19.6.1993, p. 1).

116. Commission Communication No 93/C335/02 concerning Council Regulation (Euratom) No 1493/93 (OJ C 335, 10.12.1993, p. 2).
117. Commission Decision 93/552/Euratom of 1 October 1993 establishing the standard document for the supervision and control of shipments of radioactive waste referred to in Council Directive 92/3/Euratom (OJ L 268, 29.10.1993, p. 83).
118. Commission Communication No 94/C224/02 concerning Council Directive 92/3/Euratom (OJ C 224, 12.8.1994, p. 2).
119. Council Directive 96/29/Euratom of 13 May 1996 laying down *basic safety standards for the health protection of the general public and workers against the dangers of ionizing radiation* (OJ L 159, 29 June 1996, p. 1) and repealing and replacing Council Directive 80/836/Euratom of 15 July 1980 (OJ L 246, 17.9.1980, p. 1) and Council Directive 84/467/Euratom of 3 September 1984 (OJ L 265, 5.10.1984 p. 4).
- Communication 98/C133/03 from the Commission concerning the implementation of Council Directive 96/29/Euratom of 13 May 1996 laying down basic safety standards for the protection of the health of workers and the general public against the dangers arising from ionising radiation (OJ C 133, 30.4.1998 p. 3).
120. Commission Recommendation 99/829/Euratom of 6 December 1999 on the application of Article 37 of the Euratom Treaty (OJ L 324, 16.12.1999, p. 23).
121. Commission Recommendation 2000/473/Euratom of 8 June 2000 on the application of Article 36 of the Euratom Treaty concerning the monitoring of the levels of radioactivity in the environment for the purpose of assessing the exposure of the population as a whole, (OJ L 191, 27.7.2000, p. 37).
122. Commission Regulation No 1609/2000/EC of 24 July 2000 establishing a list of products excluded from the application of Council Regulation (EEC) No 737/90 on the conditions governing imports of agricultural products originating in third countries following the accident at the Chernobyl nuclear power station (OJ L 185, 25.7.2000, p. 27).
123. Action Plan to combat nuclear terrorism approved by the IAEA Board of Governors in March 2002.
124. Agreement of 29 January 2003 between Euratom and non-member States of the European Union on the participation of the latter in the Community arrangements for the early exchange of information in the event of radiological emergency (Ecurie) (OJ C 102, 29.4.2003, p. 2).
125. Commission Recommendation (EC) No 274/2003 of 14 April 2003 on the protection and information of the public with regard to exposure resulting from the continued radioactive caesium contamination of certain wild food products as a consequence of the accident at the Chernobyl nuclear power station (OJ L 99, 17.4.2003, p. 55 + Corrigendum in OJ L 109, 1.5.2003, p. 27).
126. Commission Recommendation 2004/2/Euratom of 18 December 2003 on standardised information on radioactive airborne and liquid discharges into the environment from nuclear power reactors and reprocessing plants in normal operation (OJ L 2, 6.1.2004, p. 36).

127. Council Directive 2003/122/EURATOM of 22 December 2003 on the control of high-activity sealed radioactive sources and orphan sources.
128. Council Decision of 29 April 2004 enabling the Commission to adopt a Regulation on the *application of EURATOM safeguards* (7768/3/04 REV 3).
129. Council Decision of 29 September 2004 approving the conclusion by the Commission of an agreement for cooperation in the peaceful uses of nuclear energy between EURATOM and the Cabinet of Ministers of Ukraine (12033/04) + Commission Decision of 4 April 2006 on the conclusion of the Agreement (OJ L 261, 22.9.2006, p. 26).
130. Council Decision 2005/84/Euratom of 24 January 2005 approving the accession of the European Atomic Energy Community to the *Joint Convention on the Safety of Spent Fuel Management and on the Safety of Radioactive Waste Management* (OJ L 30, 3.2.2005 p. 10).
131. Commission Regulation (Euratom) No 302/2005 of 8 February 2005 on the application of Euratom safeguards (OJ L 54, 28.2.2005, p. 1).
132. Commission Decision 2005/844/Euratom of 25 November 2005 concerning the accession of the European Atomic Energy Community to the *Convention on Early Notification of a Nuclear Accident* (OJ L 314, 30.11.2005, p. 21).
133. Council Decision 2005/845/Euratom of 25 November 2005 concerning the accession of the European Atomic Energy Community to the *Convention on Assistance in the case of a Nuclear Accident or Radiological Emergency* (OJ L 314, 30.11.2005, p. 27).
134. Commission Recommendation of 15 December 2005 on guidelines for the application of Regulation (Euratom) No 302/2005 on the application of Euratom safeguards (OJ L 28, 1.2.2006, p. 1).
135. Communication 2006/C/155/02 from the Commission *on verification of environmental radioactivity monitoring facilities under the terms of Article 35 of the Euratom Treaty* — Practical arrangements for the conduct of verification visits in Member States (OJ C 155, 4.7.2006, p. 2).
136. Commission Regulation (EC) No 1635/2006 of 6 November 2006 laying down detailed rules for the application of Council Regulation (EEC) No 737/90 on the conditions governing imports of agricultural products originating in third countries following the accident at the Chernobyl nuclear power station (OJ L 306, 7.11.2006, p. 3).
137. Council Directive No 2006/117/Euratom of 20 November 2006 *on the supervision and control of shipments of radioactive waste and spent fuel* (OJ L 337, 5.12.2006, p. 21).
138. Council Decision of 4 December 2006 approving the conclusion by the Commission of an agreement for cooperation in the peaceful uses of nuclear energy between EURATOM and the Government of the Republic of Kazakhstan (15495/06).

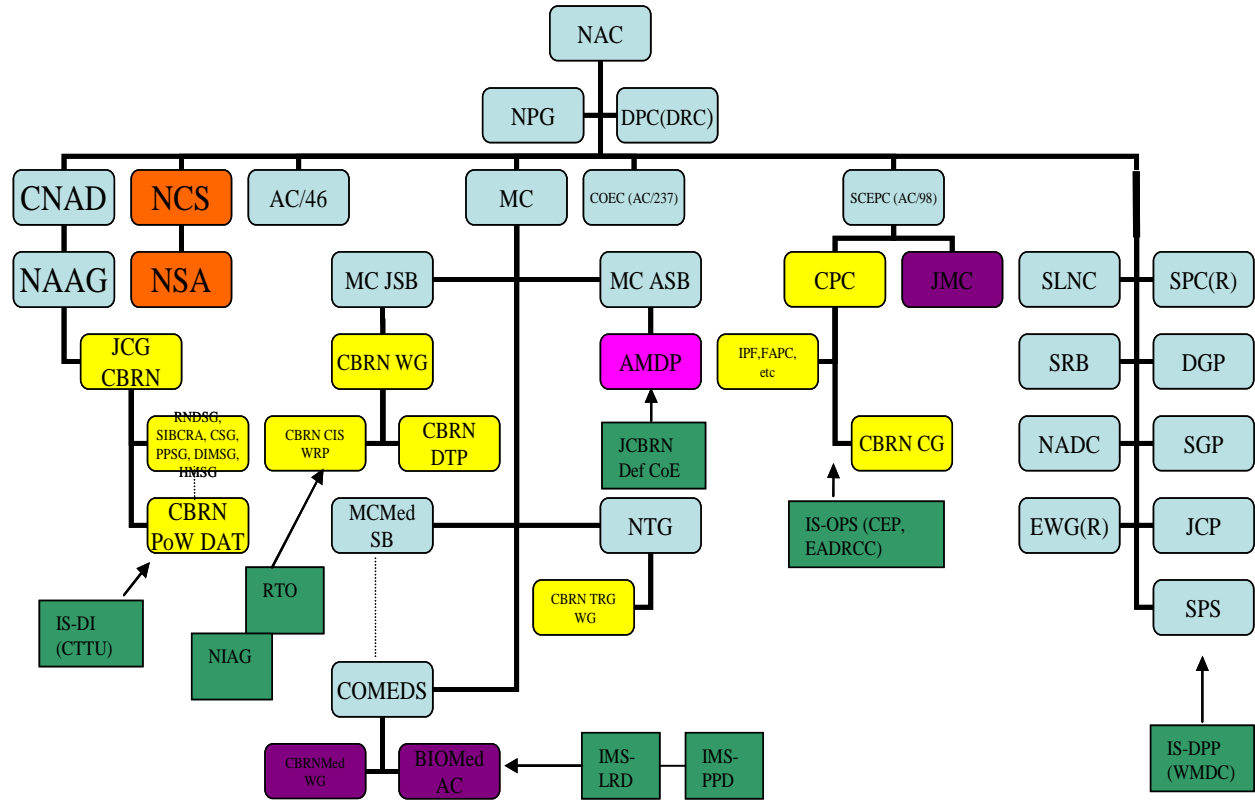
139. Council Decision 2007/513/Euratom of 10 July 2007 approving the accession of the European Atomic Energy Community to the *amended Convention on the Physical Protection of Nuclear Material and Nuclear Facilities* – Declaration by the European Atomic Energy Community according to Articles 18(4) and 17(3) of the CPPNM (OJ L 190, 21.7.2007, p. 12).

Research (see p. 81)

140. Decision 1513/2002/EC of the European Parliament and of the Council of 27 June 2002 concerning the sixth framework programme of the European Community for research, technological development and demonstration activities, contributing to the creation of the European Research Area and to Innovation (2002 to 2006).

Transport of chemicals and dangerous substances (see p. 59)

141. Council common position for a Directive of the European Parliament and of the Council on the inland transport of dangerous goods (3658/07).
142. Directive 95/50/EC on uniform procedures for checks on the transport of dangerous goods by road, last amended by Directive 2001/26/EC.
143. Directive 98/91/EC relating to motor vehicles and their trailers intended for the transport of dangerous goods by road and amending Directive 70/156/EEC relating to the type approval of motor vehicles and their trailers.



Legende :

- Tasking and Policy Guiding bodies
- CBRN Defence and preparedness
- CBRN Medical Defence
- Standardization guidance
- Support and Cooperation

I. List of NATO Bodies involved on CBRN Defence and Non-proliferation Related Activities - Basic Information

No.	Committee, Group, Panel	Reference	Level	Overview	Reporting to
1	Nuclear Planning Group High Level Group	NPG(HLG)	1	Review issues involving NATO's nuclear policy, force structure and posture and formulate policy recommendations on nuclear issues. Provide advice to Ministers	NPG
2	Nuclear Planning Group Staff Group	NPG(Staff Group)	1	Assists in the development of all matters of nuclear policy, strategy and force posture, including nuclear planning and procedures, consultations, exercises and training. Provides day-to-day coverage of all nuclear issues. Prepares NPG meetings at Ministerial and Permanent Representative levels. Develops public information on NATO's nuclear policy and posture	NPG HLG
3	Defence Review Committee	DRC	1	Advises on defence capability, force planning (including Ministerial Guidance) and other issues related to the integrated military structure	DPC
4	Joint Committee on Proliferation	JCP	1	Provides coordinated reports on politico-military and defence aspects of WMD proliferation. Made up of members of the SGP and DGP	NAC
5	Senior Politico-Military Group on Proliferation	SGP	1	Advises on politico-military aspects of the WMD proliferation and serves as forum for exchange of information on these issues	NAC via JCP
6	Senior Defence Group on Proliferation	DGP	1	Examines defence aspects of the WMD proliferation including proliferation of ballistic missiles, planning and capabilities. Provides policy guidance, makes recommendations and monitors implementation of resulting actions in fulfilment of NATO's defence response to proliferation	NAC via JCP
7	Political Committee at Senior Level (reinforced)	SPC(R)	1	Advises on political and specific political-military issues. Responsible body for Ministerial and Summit communications	NAC
8	Executive Working Group (reinforced)	EWG(R)	1	Advises on defence matters concerning NATO nations. Currently the main area of business is Missile Defence	NAC
9	NATO Special Committee	AC/46	1	Acts as an advisory body on matters of espionage and terrorist or related threats which may affect the Alliance	NAC
10	Terrorist Task Force	TTF	1	Acts as coordinating body for overall NATO efforts related to the Defence Against Terrorism and supports the work of the SPC(R)	indirectly SPC(R)
11	NATO Committee for Standardization	NCS (AC/321)	1	Supervises all standardisation activities in NATO	NAC
12	MC Joint Standardization Board	MC JSB	2	Responsible for Joint operational standardization and tasking authority for CBRN WG	MC
13	CBRN Operations Working Group	CBRN WG	3	Staffs doctrine and procedures in the area of CBRN Defence. Coordinates standardization of the required techniques, organization, standards of proficiency and the related training procedures	MC JSB
14	CBRN Communication and Information Systems and Warning & Reporting Panel	CBRN CIS WRP	4	Develops, harmonizes and validates CBRN Defence Information Exchange Requirement proposals. Is also responsible for development and Maintenance ATP-45 and AEP-45	CBRN WG
15	CBRN Doctrine and Terminology Panel	CBRN DTP	4	Monitors the structure and hierarchy of NATO CBRN Defence APs and STANAGs and proposes and monitors development of related Doctrine and Procedures	CBRN WG
16	MC Air Standardization Board	MC ASB	2	Foster operational standardization initiatives within the aerospace area of responsibility, with the aim of achieving optimal interoperability of Alliance	MC
17	Aeromedical Panel	AMDP	4	Develops standards in Aviation Medicine including the effects of CBRN agents	MC ASB

No.	Committee, Group, Panel	Reference	PAR 1	Overview	Reporting to
18	Military Committee Medical Standardization Board	MCMedSB	2	Manages the standardization efforts in the area of the Military Medicine including CBRN Medical Defence	MC
19	Committee of the Chiefs of the Military Medical Services in NATO	COMEDS	1	Provides medical advice on all defence and operational planning scenarios and serves as coordinating body for military medical standardization	MC
20	Military Medical Steering Board	MM SG	2	Exercises coordinating authority across the whole spectrum of military medical matters for which COMEDS is responsible	COMEDS
21	CBRN Medical Working Group	CBRNMedWG	3	Staffs medical CBRN operational concepts, policies and procedures for defence against CBRN weapons (hazards and Terrorist Action). Preventive and occupational medicine related to these hazards are excluded	COMEDS and MCMedSB
22	Biological Medical Advisory Committee	BIOMedAC	3	Co-ordinates standardization work in the biological medical defence field, develops policy, identifies gaps between authoritative bodies and research, development and study groups and advises all Medical Working Groups on the development of NATO biological medical defence	CBRN MedWG
23	Conference of National Armaments Directors	CNAD AC/259	1	Promotes NATO armaments cooperation and considers political, economic and technical aspects of the development and procurement of equipment for NATO forces.	NAC
24	NATO Army Armaments Group	NAAG (AC/225)	2	Harmonises of requirements, standardisation and information exchange in the area of Land Armaments and Joint Services	CNAD
25	Joint Capabilities Group on CBRN Defence	JCG CBRN	3	Harmonises of requirements, standardisation and information exchange in the area of Joint Nuclear, Biological and Chemical Defence	NAAG
26	Challenge Sub Group	CSG	4	Standardisation and information exchange in the area of Chemical and Biological Challenge/Threats	JCG CBRN
27	Detection, Identification and Monitoring Sub Group	DIMSG	4	Harmonisation of requirements, standardisation and information exchange in the area of Joint CBRN detection Identification and Monitoring	JCG CBRN
28	Hazard Management Sub Group	HMSG	4	Harmonisation of requirement, standardisation and information in the area of Joint CBRN Hazard Management	JCG CBRN
29	Physical Protection Sub Group	PPSG	4	Standardisation and information exchange in the area of Joint CBRN Physical Protection	JCG CBRN
30	Radiological and Nuclear Defence Sub Group	RNDSG	4	Harmonisation of requirements, standardisation and information exchange in the area of Radiological and Nuclear Defence	JCG CBRN
31	Sampling and Identification of Biological, Chemical and Radiological Agents Sub Group	SIBGRA	4	Harmonisation of requirements, standardisation and information exchange in the area of Sampling and Identification of Biological, Chemical and Radiological Agents	JCG CBRN
32	POW DAT Detect, Protect & Defeat CBRN Project Group	CBRN PoW DAT	4	Project Group is designed to develop capabilities to detect, protect against, and manage the hazards caused by the use of CBRN weapons by terrorist including development of the better methods of consequence management, de-contamination, and stand-off detection capability.	JCG CBRN
33	NATO Training Group	NTG	1	Coordinates and harmonizes training with objectives to improve and expand existing training arrangements and to initiate new training activities	MC
34	Joint Services Sub Group	NTG JSSG	2	Initiates and develops coordination and standardization of joint individual and collective education and training in order to enhance interoperability among Alliance and partners forces	NTG

No.	Committee, Group, Panel	Reference	Level	Overview	Reporting to
35	CBRN Training Working Group	CBRN TRG WG	3	Promotes relevant individual and collective CBRN defence training. Consists of four Working Teams (WT1 - Army and Joint Services, WT2 - Navy, WT3 - Air Operations, WT4 - Medical Service)	JSSG
36	Senior Civil Emergency Planning Committee	SCEPC (AC/98)	1	Senior advisory body on civil emergency planning and disaster relief	NAC
37	Civil Protection Committee	CPC (AC/23)	2	Assess national arrangements for disaster planning and protection of civil population. Leads for CEP on Terrorism and WMD consequence management	SCEPC
38	CPC CBRN Coordination Group	CBRN CG	3	Steering group for practical coordination of CBRN activities across the Planning Boards and Committees subordinated to SCEPC	CPC
39	Joint Medical Committee	JMC	2	Advises on civil-military planning aspects of medical emergency arrangements. Maintain pool of medical experts for use in crises.	SCEPC
40	NATO Air Defence Committee	NADC	1	Advises and co-ordinates all aspects of air defence including terrorism consequences to the air defence. Support Alliance work on Missile Defence.	NAC, DPC
41	Council Operations and Exercise Committee	COEC (AC/237)	1	Forum for consultation and coordination of crisis management arrangements and procedures. Supports NAC and/or DPC in periods of tension or crisis and oversight SITCEN. Plans and conducts of NATO-wide crisis management exercises	NAC
42	Senior Resource Board	SRB	1	Advises on mid- and long- term requirements for, and availability of, military common-funded resources. Screen & endorse Capability Packages for approval.	NAC
43	Senior Logistician Conference	SNLC (AC/305)	1	Coordinating Authority for logistics and provides forum for harmonizing and coordinating logistic initiatives in NATO.	NAC MC
44	Committee on Science for Peace and Security	SPS (AC/328)	1	Supports practical cooperation with all partners in civil science and innovation	NAC
45	NATO Research and Technology Organization	RTO	2	Conducts and promotes cooperative research and technical information exchange to support the development and effective use of national defence R&T activities; develops a long term NATO Research and Technology strategy; and provides advice to NATO and national decision makers. It comprises <i>Research and Technology Board</i> and <i>Research and Technology Agency</i> .	MC CNAD
46	Research and Technology Board	RTB (AC/323)	2	Highest authority within NATO's Research and Technology Organisation (RTO). It is the policy body tasked to carry out the mission of the RTO. Working in concert with other NATO defence R&T bodies, it serves as the single integrating body within NATO for the direction and/or coordination of defence research and technology issues. Consist of six panels and one group: - Studies, Analysis and Simulation (SAS); - Systems, Concepts and Integration (SCI); - Information Systems Technology (IST); - Modelling and Simulation Group (M&S Group).	MC CNAD
47	Research and Technology Agency	RTA	3	Serves as the supporting body of the RTO	RTB
48	Human Factors and Medicine Panel	HFM	3	Optimizes performance, health, well being, and safety of the human in operational environments with consideration of affordability. Covers following areas: Human Performance, Operational Medicine and Human Protection in Adverse Environments	RTB
49	NATO Industrial Advisory Group	NIAG	2	High level consultative and advisory body of senior NATO countries industrialists on research,	CNAD



Organization for Security and Co-operation in Europe
Ministerial Council
Porto 2002

MC(10).JOUR/2
7 December 2002
Annex 1

Original: ENGLISH

2nd day of the Tenth Meeting
MC(10) Journal No. 2, Agenda item 8

OSCE CHARTER ON PREVENTING AND COMBATING TERRORISM

The OSCE participating States, firmly committed to the joint fight against terrorism,

1. Condemn in the strongest terms terrorism in all its forms and manifestations, committed no matter when, where or by whom and reiterate that no circumstance or motive can justify acts of or support for terrorism;
2. Firmly reject identification of terrorism with any nationality or religion and reaffirm that action against terrorism is not aimed against any religion, nation or people;
3. Recognize that terrorism requires a co-ordinated and comprehensive response and that acts of international terrorism, as stated in the United Nations Security Council resolution 1373 (2001), constitute a threat to international and regional peace and security;
4. Declare that acts, methods and practices of terrorism, as well as knowingly providing assistance to, acquiescing in, financing, planning and inciting such acts, are contrary to the purposes and principles of the United Nations and the OSCE;
5. Consider of utmost importance to complement the ongoing implementation of OSCE commitments on terrorism with a reaffirmation of the fundamental and timeless principles on which OSCE action has been undertaken and will continue to be based in the future, and to which participating States fully subscribe;
6. Reaffirm their commitment to take the measures needed to protect human rights and fundamental freedoms, especially the right to life, of everyone within their jurisdiction against terrorist acts;
7. Undertake to implement effective and resolute measures against terrorism and to conduct all counter-terrorism measures and co-operation in accordance with the rule of law, the United Nations Charter and the relevant provisions of international law, international standards of human rights and, where applicable, international humanitarian law;
8. Reaffirm that every State is obliged to refrain from harbouring terrorists, organizing, instigating, providing active or passive support or assistance to, or otherwise sponsoring

MC10EW08

terrorist acts in another State, or acquiescing in organized activities within its territory directed towards the commission of such acts;

9. Will co-operate to ensure that any person who wilfully participates in financing, planning, preparing or perpetrating terrorist acts, or in supporting such acts, is brought to justice and, to that end, will afford one another the greatest measure of assistance in providing information in connection with criminal investigations or criminal extradition proceedings relating to terrorist acts, in accordance with their domestic law and international obligations;
10. Will take appropriate steps to ensure that asylum is not granted to any person who has planned, facilitated or participated in terrorist acts, in conformity with relevant provisions of national and international law, and through the proper application of the exclusion clauses contained in the 1951 Convention Relating to the Status of Refugees and its 1967 Protocol;
11. Recognize that the relevant United Nations conventions and protocols, and United Nations Security Council resolutions, in particular United Nations Security Council resolution 1373 (2001), constitute the primary international legal framework for the fight against terrorism;
12. Recognize the importance of the work developed by the United Nations Security Council Counter-Terrorism Committee and reaffirm the obligation and willingness of participating States and the OSCE to co-operate with this Committee;
13. Recall the OSCE's role as a regional arrangement under Chapter VIII of the United Nations Charter, and its obligations in this context to contribute to the global fight against terrorism;
14. Recall their Decision on Combating Terrorism and its Plan of Action for Combating Terrorism, adopted at the Ninth Meeting of the OSCE Ministerial Council in Bucharest and reaffirm the commitments contained therein;
15. Take note with satisfaction of the Declaration and the Programme of Action adopted at the Bishkek International Conference on Enhancing Security and Stability in Central Asia: Strengthening Comprehensive Efforts to Counter Terrorism, held on 13 and 14 December 2001;
16. Reiterate the commitment undertaken in the framework of the Charter for European Security, including the Platform for Co-operative Security, adopted at the Istanbul Summit, to co-operate more actively and closely with each other and with other international organizations to meet threats and challenges to security;
17. Underscore that the prevention of and fight against terrorism must be built upon a concept of common and comprehensive security and enduring approach, and commit to using the three dimensions and all the bodies and institutions of the OSCE to assist participating States, at their request, in preventing and combating terrorism in all its forms;
18. Undertake to fulfil their obligation, in accordance with the United Nations conventions, protocols and Security Council resolutions, as well as other international

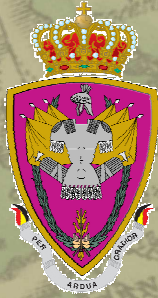
commitments, to ensure that terrorist acts and activities that support such acts, including the financing of terrorism, are established as serious criminal offences in domestic laws;

19. Will work together to prevent, suppress, investigate and prosecute terrorist acts, including through increased co-operation and full implementation of the relevant international conventions and protocols relating to terrorism;
20. Are convinced of the need to address conditions that may foster and sustain terrorism, in particular by fully respecting democracy and the rule of law, by allowing all citizens to participate fully in political life, by preventing discrimination and encouraging intercultural and inter-religious dialogue in their societies, by engaging civil society in finding common political settlement for conflicts, by promoting human rights and tolerance and by combating poverty;
21. Acknowledge the positive role the media can play in promoting tolerance and understanding among religions, beliefs, cultures and peoples, as well as for raising awareness of the threat of terrorism;
22. Commit themselves to combat hate speech and to take the necessary measures to prevent the abuse of the media and information technology for terrorist purposes, ensuring that such measures are consistent with domestic and international law and OSCE commitments;
23. Will prevent the movement of terrorist individuals or groups through effective border controls and controls relating to the issuance of identity papers and travel documents;
24. Recognize the need to complement international co-operation by taking all necessary measures to prevent and suppress, in their territories through all lawful means, assistance to, and the financing and preparation of, any acts of terrorism, and to criminalize the wilful provision or collection of funds for terrorist purposes, in the framework of their obligations under the International Convention for the Suppression of the Financing of Terrorism and relevant Security Council resolutions;
25. Reaffirm their commitment to fulfil their international obligations, as set out in United Nations Security Council resolutions 1373 (2001) and 1390 (2002), and in particular to freeze the assets of those designated by the Committee established pursuant to United Nations Security Council resolution 1267 (1999);
26. Note with concern the links between terrorism and transnational organized crime, money laundering, trafficking in human beings, drugs and arms, and in this regard emphasize the need to enhance co-ordination and to develop co-operative approaches at all levels in order to strengthen their response to these serious threats and challenges to security and stability;
27. Declare their determination to use in good faith all relevant instruments available within the politico-military dimension of the OSCE, as represented by the Forum for Security Co-operation, and emphasize the importance of fully implementing these instruments in particular, the Code of Conduct on Politico-Military Aspects of Security and the OSCE Document on Small Arms and Light Weapons;

28. Reaffirm that arms control, disarmament and non-proliferation remain indispensable elements of co-operative security between States; that they can also make an essential contribution by reducing the risk of terrorists gaining access to weapons and materials of mass destruction and their means of delivery;

Express determination to combat the risk posed by the illicit spread of and access to conventional weapons, including small arms and light weapons;

Will make every effort to minimize those dangers through national efforts and through strengthening and enhancing the existing multilateral instruments in the fields of arms control, disarmament and non-proliferation including the OSCE Principles Governing Non-Proliferation and to support their effective implementation and, where applicable, universalization.



Bibliografie





Officiële documenten

Report of the Secretary-General of the United Nations' General Assembly A/57/229 : « The issue of missiles in all its aspects », 23 July 2002.

Council of the European Union 14310/03, « Council Common Position on the universal position and reinforcement of multilateral agreements in the field of non-proliferation of weapons of mass destruction and means of delivery », Brussels, 11 November 2003.

SOLANA, J., A secure Europe in a better world. EUROPEAN COUNCIL, Thessaloniki, 20 June 2003.

Note from the Council to the European Council 15656/03, « Fight against the proliferation of weapons of mass destruction-EU strategy against the proliferation of Weapons of Mass Destruction », Brussels, 10 December 2003.

Note from the General Secretariat to the EU Delegations 16694/06, « EU strategy against the proliferation of WMD: Monitoring and enhancing consistent implementation », Brussels, 12 December 2006.

Treaty on the non-proliferation of nuclear weapons :
<http://disarmament.un.org/wmd/npt/npttext.html>

Model protocol additional to the agreement(s) between the State(s) and the International Atomic Energy Agency for the application safeguards:
<http://www.iaea.org/Publications/Documents/Infcircs/1997/infcirc540.pdf>

Convention on the prohibition of the development, production, stockpiling and use of chemical weapons and on their destruction :
<http://disarmament.un.org/wmd/cwc/cwctext.htm>

Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their destruction:
<http://disarmament.un.org/wmd/bwc/index.html>

Hague code of conduct against ballistic missile proliferation:
<http://www.un.org/News/Press/docs/2004/gadis3286.doc.htm>

Comprehensive Nuclear Test Ban Treaty:
<http://disarmament.un.org/wmd/ctbt/index.html>

Operations in the UK: The Defence Contribution to Resilience. Interim Joint Doctrine Publication 02. Ministry of Defence, December 2004.

Office of the Secretary of Defense, Proliferation: Threat and Response, January 2001.

EU NBC EOD POLICY, Headline Goal Task Force, Februari 2006.

Vlaamse buitenlandse handel in wapens en goederen in tweeërlei gebruik 2007, Vlaams vredesinstituut, Rapport maart 2008.

Een vergelijkende studie van het wapenexportbeleid: Vlaanderen en zijn burens, Vlaams vredesinstituut, Rapport maart 2007.

Het Vlaams wapenexportbeleid: een analyse van de juridische context, Vlaams vredesinstituut, Rapport oktober 2007.

Algemene beleidsnota van de minister van Binnenlandse zaken, Belgische Kamer van volksvertegenwoordigers, DOC 51 1371/021, 24 november 2004.

Algemene beleidsnota van de minister van Binnenlandse zaken, Belgische Kamer van volksvertegenwoordigers, DOC 52 0995/010, 11 april 2008.

White paper opgesteld door het overlegplatform voor de informatieveiligheid, Juli 2007.

Groenboek van de Europese Commissie, COM(2005), Commissie van de Europese Gemeenschappen, Brussel, 2005.

Manual for First Responders to a Radiological Emergency. International Atomic Energy Agency, October 2006.



Boeken

CIRINCIONE, J., WOLFSTHAL, J., RAJKUMAR, M., Deadly Arsenals: nuclear, biological and chemical threats. Carnegie Endowment for International Peace, 2005.

DANDO, M., Biological Warfare in the 21st Century, Brassey's Ltd, 1994.

DUMOULIN, A., WASINSKI, C., La dissuasion nucléaire française : Paramètres doctrinaux, politiques et techniques. Révolution ou inflexion de la stratégie en post-guerre froide (1990-2006) ?, Ibidem, n°2006/1, Septembre 2006.

Kol SBH DE KIMPE, J., Bescherming van vitale infrastructuur. Welke rol voor Defensie? Kabinet Defensie, 2007.

EPSTEIN, G., Technologies underlying weapons of mass destruction, International Security and Commerce Program, December 1993.

Global Fissile Material Report 2008, International Panel on Fissile Materials, Princeton University, September 2008.

IAEA TECDOC 1529, Management of reprocessed Uranium, International Atomic Energy Agency, Vienna , 2007.

IAEA Nuclear Security Series N°2, Nuclear Forensics Support, International Atomic Energy Agency, Vienna , 2006.

IAEA Nuclear Security Series N°3, Monitoring for Radioactive Material in International Mail Transported by Public Postal Operators, International Atomic Energy Agency, Vienna , 2006.

IAEA Nuclear Security Series N°4, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, International Atomic Energy Agency, Vienna , 2007.

IAEA Nuclear Security Series N°5, Identification of Radioactive Sources and Devices, International Atomic Energy Agency, Vienna , 2007.

IAEA Nuclear Security Series N°6, Combating Illicit trafficking in Nuclear and other Radioactive Material, International Atomic Energy Agency, Vienna , 2007.

KRASS, A., BOSKMA, P., ELZEN, B., SMIT, W., « Uranium enrichment and Nuclear Weapon Proliferations », Stockholm International Peace Research Institute, SIPRI London, Taylor & Francis Ltd, 1983.

LANGFORD, E., Introduction to Weapons of Mass Destruction : Radiological, Chemical and Biological. Wiley-Interscience, 2004.

LAVOY, P., SAGAN, S., WIRTZ, J, Planning the Unthinkable, Cornell University Press, 2000.

LAVOY, P., Nuclear weapons proliferation in the next decade, Routledge, 2007.

The National Institute for Defense Studies Japan, East Asian Strategic Review 2008, April 2008.

Office of the Secretary of Defense, Proliferation : threat and response, January 2001.

RUSSELL, J., WIRTZ, J, Globalization and WMD proliferation: terrorism, transnational networks and international security, Routledge, 2008.

PERKOVICH, G., Universal Compliance: a strategy for nuclear security. 2007 Report Card. Carnegie Endowment for International Peace, June 2007.

SOKOLSKI, H., Pakistan's nuclear future: worries beyond war. DOD, Strategic Studies Institute, January 2008.



Artikels uit tijdschriften en pers

ARNOLD, J., « Disaster Medicine in the 21st Century: Future Hazards, Vulnerabilities and Risk », in *Prehospital and Disaster Medicine*, January-March 2002.

AUGUSTINE, A., « India missile test to start arms race: Pakistan », Reuters van 27 Feb 2008.

BECK, M., « Strengthening Multilateral Export Controls », Center for International Trade and Security, University of Georgia, September 2002.

BOND, R., « The proliferation security initiative: Targeting Iran and North Korea? », British American Security Information Council, BASIC Papers, N°53, January 2007.

BUNN, M., WIER, A., *Terrorist Nuclear Weapon Construction: How Difficult?*, The annals of the American Academy of Political and Social Science, N°607, September 2006.

CARNEGIE ENDOWMENT FOR PEACE, « NKorea almost ready on nuclear statement », in *Proliferation news*, 3 June 2008.

CARTER, A., « How to counter WMD », in *Foreign Affairs*, September-October 2004.

CHESTNUT, S., « Illicit activity and proliferation: North Korean smuggling networks », in *International Security*, Vol.31, N°1, 2007.

EISENSTADT, M., « Can the United States Influence the WMD Policies of Iraq and Iran? », in *Nonproliferation Review*, Summer 2000.

FORDEN, G., « Smoke and mirrors: Analyzing the Iranian missile test », in *Jane's Intelligence Review*, April 2008.

GASQUARD, S., « La politique de sécurité et de défense de la Turquie: éléments de convergence et de divergence avec la PESC/PESD », in *Sécurité et Stratégie*, N°96, Septembre 2007.

KHAITOUS, T., « Is Syria a candidate for Nuclear Proliferation? », in *Issue Brief*, James Martin Center for Nonproliferation Studies, March 2008.

KASSENOVA, T., « Central Asia: regional security and WMD proliferation threats », in *Disarmament Forum*, N°4, 2007.

KAMPANI, G., « WMD diffusion in Asia: heading towards a disaster », in *Strategic Asia*, 2004-2005, September 2004.

HOCHMAN, D., « Rehabilitating a Rogue: Libya's WMD Reversal and Lessons for US Policy », in Parameters, Spring 2006.

JOHEE, C., « North Korea Flexes Missile Muscles » op
<http://abcnews.go.com/International/Story?id=4541837&page=1>

LAVOY, P., « Nuclear proliferation over the next decade : Causes, Warning Signs and Policy Responses », in Nonproliferation Review, Vol.13, N°3, November 2006.

LIEGGI, S., « China strengthens nuclear related export controls », in WMD insights, April 2007.

LIPPERT, W., « Geiger counting: Interpol's hunt for radiological and nuclear threat », in Jane's Intelligence Review, April 2008.

MARCHAND, G., « CBRN Going CBRNE: A New Perspective Behind The Words? », in IFAS, Juin 2007.

Mc LEISH, C., NIGHTINGALE, P., « Biosecurity, bioterrorism and the governance of science: The increasing convergence of science and the security policy. », in Research Policy, Vol.36, October 2007.

MOODIE, M., ARMSTRONG, R., MERKELEY, T., « Responding in the Homeland: A Snapshot of NATO's readiness for CBRN Attacks », in Defense Horizons, N°56, June 2007.

NELSON, D., « Trafficking in Destruction », Center for Arms Control and Non-Proliferation, June 2007.

PARACHINI, J., « Putting WMD Terrorism into Perspective », in The Washington Quarterly, Autumn 2003.

PERKOVICH, G., « Bush's Nuclear Revolution: A Regime Change in Nonproliferation », in Foreign Affairs, March-April 2003.

PERKOVICH, G., « Taming Tehran », in Foreign Affairs, November 2004.

PINKSTON, A., « DPRK relying on multiple approaches to acquire foreign technology », in WMD insights, March 2006.

PROSSER, A., « Nuclear Trafficking Routes: Dangerous Trends in Southern Asia », Centre for Defense Information, November 2004.

RUSSELL, J., « Peering into the abyss: non-state actors and the 2016 proliferation environment », in Nonproliferation Reviews, Vol.13, N°3, November 2006.

SQUASSONI, S., « India and Iran: WMD proliferation activities », in Congressional Research Service, Report for Congress, November 2006.

SCHULTE, G., « Responding to proliferation: NATO's role », in NATO Review, Vol.43, N°4, July 1995.

KHAITOUS, T., « Is Syria a candidate for Nuclear Proliferation? », in Issue Brief, James Martin Center for Nonproliferation Studies, March 2008.

WIRTZ, J., « Whatever happened to arms control? », in NATO Review, Vol.5, 2003.

WORMUTH, C., « The Next Catastrophe: Ready or Not? », in The Washington Quarterly, January 2009.

YUAN, J-D., « Beijing Keenly watching Japan's Nuclear Debate », in International Studies Review, November 2006.

YUAN, J-D., « Strengthening China's export control system », Center of Nonproliferation studies, Monterey, 4 October 2002.

ZAITSEVA, L., HAND, K., « Nuclear smuggling chains », in American Behavioral Scientist, Vol.46, N°6, February 2003, pp. 822-844.



Jaarboeken

Stockholm International Peace Research Institute, SIPRI Yearbook 2007, Summary. Armaments, Disarmament and International Security, Oxford, Oxford University Press, 2007.

Algemene Directie Crisiscentrum, Activiteitenrapport 2003. Federale Overheidsdienst Binnenlandse Zaken, 10 juli 2004.

Algemene Directie Crisiscentrum, Activiteitenrapport 2004. Federale Overheidsdienst Binnenlandse Zaken, 26 oktober 2005.

Algemene Directie Crisiscentrum, Activiteitenrapport 2005. Federale Overheidsdienst Binnenlandse Zaken, 23 oktober 2006.

Algemene Directie Crisiscentrum, Activiteitenrapport 2006. Federale Overheidsdienst Binnenlandse Zaken, 4 juli 2007.

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Activiteitenverslag 2005, 2006.



Internet sites

<http://www.defenselink.mil>.

<http://emergency.cdc.gov>

<http://www.nato.int>

<http://www.sipri.org>

<http://www.armscontrol.org>

<http://www.globalsecurity.org>

<http://jdw.janes.com/public/jdw/index.shtml>

<http://cns.miis.edu/research/cbw/possess.htm>

<http://www.isis-online.org/>

<http://carnegieeurope.eu/>



Toespraken en conferenties.

Transcript of a presentation held on 11 April 2007 at United Nations Headquarters: « A verifiable Fissile-Material Treaty as a Foundation for Nuclear Disarmament », in Disarmament 2007: Critical Disarmament Issues, United Nations 2008.

BUNN, M., « The risk of nuclear terrorism and the next steps to reduce the danger », testimony of M.BUNN for the committee on homeland security and governmental affairs, United States Senate, 02 April 2008.

Conferentie « Over-the-Horizon Threats: WMD proliferation 2020 » georganiseerd door Center for Contemporary Conflict, Paris, 28-29 June 2007, rapport te vinden op <http://www.ccc.nps.navy.mil/si/2007/Aug/lavoyAug07.asp>.

ROFFEY, R., « The need to promote global biosecurity and biosafety and the BTWC », Roundtable discussion on “Developing a Comprehensive Global Biosecurity Regime”, Geneva, 8 November 2006.

Conferentie « Terrorism, Transnational Networks and WMD Proliferation: Indications and Warning in an Era of Globalization » georganiseerd door Center for Contemporary Conflict, Monterey, 25-27 July 2006, rapport te vinden op http://www.ccc.nps.navy.mil/events/recent/TerrorismTransnationalNetworksandWMDProliferationJul06_rpt.asp.

Conferentie « Strengthening European Action on WMD NON-Proliferation and Disarmament : How Can Community Instruments Contribute » georganiseerd door SIPRI, Brussels, 7-8 December 2005, rapport te vinden op <http://www.sipri.org>.

Conferentie « Globalization and WMD Proliferation Networks: Challenges to U.S. Security » georganiseerd door Center for Contemporary Conflict, Naval Postgraduate School, 01 July 2005, rapport te vinden op http://www.ccc.nps.navy.mil/events/recent/WMDConferenceAug05_rpt.asp

Conferentie « Non-proliferation and Disarmament Cooperation Initiative (NDCI) » Londen, 4-5 Maart 2004.

Toespraak van Javier SOLANA op 20 juni 2003 te Thessaloniki, « A secure Europe in a better world », beschikbaar op het internet via <http://ue.eu.int/newsroom>.

Toespraak van Javier SOLANA op 12 december 2003 te Brussel, « A secure Europe in a better World, European Security Strategy », beschikbaar op het internet via <http://ue.eu.int/newsroom>.

G8 St Petersburg, MITROVA, T., Paper on Global energy security beschikbaar via http://en.g8russia.ru/i/eng_nrgsafety.doc

Toespraak van Nicolas SARKOZY op 21 Maart 2008 ter gelegenheid van de voorstelling van de kernduikboot « Le Terrible » beschikbaar via <http://www.ambafrance-uk.org/Presentation-du-SNLE-Le-Terrible.html>



Interviews

Onderhoud met Maj LENAERTS en FKP DE JONGHE SBH (ACOS Ops&Trg/Div Plans), op 14 april 2008.

Onderhoud met Maj FEROOZ (ACOS Ops&Trg/Div D&R/Force protection), op 22 april 2008.

Onderhoud met Kol SBH BREYNE (ACOS Strat), op 24 april 2008.

Onderhoud met Maj v/h Vlw SBH VAN BOCXLAER (ACOS Strat), op 16 mei 2008.

Onderhoud met Commissaris DE WINNE (DVI), op 02 juni 2008.

Onderhoud met Commissaris BEIRENS (FCUU), op 26 juni 2008.

Onderhoud met Commissaris DE BAERDEMAEKER (Centrale Dienst Terro_Task Force DVI), op 27 juni 2008.

Onderhoud met Kol v/h Vlw CROES (ACOS Strat), op 30 juni 2008.

Onderhoud met Col COLLINS BEM (CNVV), op 29 juli 2008.

Onderhoud met Bde Gen COELMONT (EGMONT), op 04 december 2008.

Veiligheid & Strategie
Nr 100
ISSN 0770-9005

Massavernietigingswapens :
erfenis van de Koude Oorlog
en bedreiging voor de toekomst

Bart Smedts

is een publicatie van:



Koninklijk Hoger Instituut voor Defensie
Studiecentrum voor Veiligheid en Defensie
Renaissancelaan 30
1000 Brussel
België

Voor deze en andere publicaties:
www.mil.be/rdc