



06/03/2009

PERSBERICHT

Het 'Early Warning System'

EEN BEDRIJFSINFORMATIENETWERK TEGEN TERRORISTISCHE DREIGINGEN

Vanaf vandaag, 6 maart 2009, treedt een bedrijfsinformatienetwerk tegen terroristische dreigingen formeel in actie in ons land. Bedrijven en overheidsdiensten zullen via een vaste procedure informatie uitwisselen om de economische sector en hun personeelsleden zo goed mogelijk te beschermen tegen mogelijke terroristische aanslagen.

De Federale Overheidsdiensten van Justitie en Binnenlandse Zaken hebben het informatienetwerk opgezet in nauwe samenwerking met het Verbond van Belgische Ondernemingen. Het protocol daarover is vandaag ondertekend door de minister van Justitie Stefaan De Clerck, minister van Binnenlandse Zaken Guido De Padt en de gedelegeerd bestuurder van het Verbond van Belgische Ondernemingen, de heer Rudi Thomaes.

Het informatienetwerk is een deeltje van het veel uitgebreider arsenaal dat de overheid al eerder in werking heeft gesteld in de strijd tegen het terrorisme (van gerechtelijke onderzoeken tot het Coördinatieorgaan van de Dreigingsanalyse of OCAD).

Bedoeling is dat een bedrijf dat bijvoorbeeld aan zijn toegangspoort dagen na elkaar dezelfde wagen ziet halt houden, de overheid daarover inlicht zodat dit kan worden onderzocht. Blijkt het incident echt verdacht, of heeft een ander bedrijf bijvoorbeeld zelfde feiten met dezelfde wagen vastgesteld, dan kan via het netwerk een hele sector worden gewaarschuwd. Omgekeerd zal de overheid, als er bijvoorbeeld een algemene dreiging is uitgesproken tegen een bepaalde bedrijfssector, die sector waarschuwen.

De uitwisseling van informatie over verdachte elementen gebeurt in een vroeg stadium - "early warning" -, zodat de ware aard van de dreiging snel kan worden onderzocht. Door het samenbrengen van informatie kunnen verdachte handelingen of dreigingen ook in een juiste context worden geplaatst. Wellicht zal blijken dat het overgrote deel van deze verdachte handelingen niets te maken heeft met een extreme dreiging.

ENKELE VOORBEELDEN VAN VERDACHTE HANDELINGEN

- verdachte bewegingen en/of voertuigen omheen een bedrijf
- anonieme meldingen gericht aan een onderneming
- een wagen die met gedoofde lichten en een bestuurder aan boord lange tijd vlakbij de toegang tot een bedrijf staat

→ VOOR EN DOOR WIE?

De informatiestroom loopt tussen vaste partners van de publieke en de private sector.

Langs de kant van de Belgische bedrijven speelt het VBO een cruciale rol om de informatie gericht te verspreiden.

Langs overheidszijde zijn de belangrijkste partners:

- De Algemene Directie van het Crisiscentrum (FOD Binnenlandse Zaken)
- De Veiligheid van de Staat (FOD Justitie)
- de federale politie
- het Coördinatieorgaan voor de Dreigingsanalyse (OCAD)
- het federaal parket

Het netwerk wordt op initiatief van zowel de publieke als de private partners gevoed: er wordt (geanonimiseerde) informatie uitgewisseld over verdachte handelingen of incidenten vastgesteld bij de ondernemingen of over mogelijke bedreigingen die door de overheid worden onderzocht.

→ WAT NIET?

Het informatienetwerk wordt niet gebruikt om systematisch alle mogelijke dreigingen en incidenten voor de openbare orde en veiligheid te communiceren.

Evenmin is het de bedoeling van dit netwerk om in de plaats te treden van de normale communicatie tussen plaatselijke bedrijven en de lokale politie.

→ HOE?

Via een permanent centraal contactpunt onderhouden de nationale verantwoordelijken van bedrijven contacten met de diensten die op nationaal vlak belast zijn met de strijd tegen het terrorisme.

Het systeem heeft al een geslaagde testperiode achter de rug en zal ook in de toekomst regelmatig geëvalueerd worden om het systeem efficiënt te houden.

→ PUBLIEK-PRIVATE-SAMENWERKING

Het protocolakkoord tussen de publieke en private partners treedt vandaag, na de ondertekening door de ministers van Justitie en Binnenlandse Zaken en de gedelegeerd bestuurder van het Verbond van Belgische Ondernemingen, formeel in werking.

Deze vorm van publiek-private samenwerking is een initiatief van het Permanent Overlegplatform Bedrijfsbeveiliging dat door de Dienst voor het Strafrechtelijk beleid van de FOD Justitie sinds vele jaren wordt voorgezeten.

Meer informatie:

Leo De Bock, woordvoerder minister van Justitie, GSM 0475 924 289

Els Cleemput, woordvoerster minister van Binnenlandse Zaken, GSM 0475 29 28 77

Elin De Vits, woordvoerster Verbond van Belgische Ondernemingen, GSM 0473 723 298

INFORMATIEFICHE

06/03/2009

EARLY WARNING SYSTEM IN HET KADER VAN DE STRIJD TEGEN HET TERRORISME: EEN PUBLIEK- PRIVAAT PARTNERSHIP

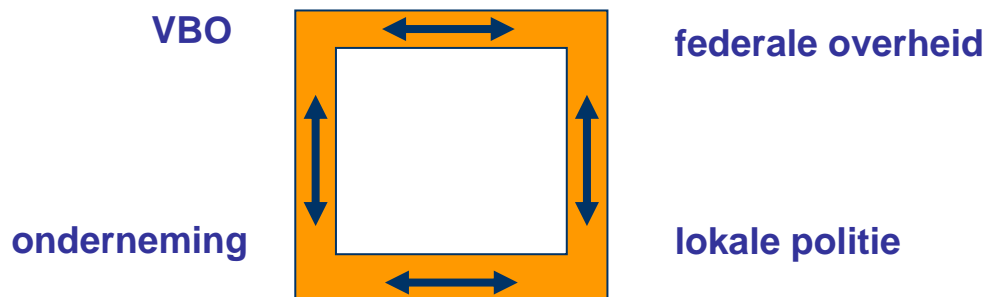
Werking van het informatievierkant

Het informatievierkant heeft tot doel om relevante informatie in het kader van een (mogelijke) terroristische dreiging uit te wisselen tussen de private en publieke sector.

Het informatievierkant is aanvullend aan de bestaande politiekkanalen: meldingen van verdachte situaties of dreigingen ten aanzien van een onderneming dienen dus steeds via de lokale politie te gebeuren. Die zal op haar beurt de informatie overmaken aan de federale autoriteiten, waar o.a. een grondige analyse van de informatie wordt gemaakt.

Bijkomend kan de onderneming deze informatie nu ook overmaken aan een nationaal contactpunt, georganiseerd door het bedrijfsleven. Dit contactpunt zal eveneens de informatie doorgeven aan de federale autoriteiten. Op die manier is er dus een 'early warning system' opgestart voor potentieel relevante informatie vanuit het bedrijfsleven.

Omgekeerd kan de overheid (naast de infodoorstroming naar en via de lokale politie) via het nationaal contactpunt één of meerdere sectoren informeren over een specifieke situatie of dreiging met het oog op een verhoogde waakzaamheid of bijkomende veiligheidsmaatregelen.



Voorbeelden van toepassingen van het informatievierkant en/of het contactpunt:

- verdachte bewegingen omheen een bedrijf(sterrein);
- anonieme meldingen gericht aan een onderneming;
- een samenshoring aan de bedrijfspoorten;
- feedback aan het bedrijfsleven omtrent (vermeende) verdachte handelingen;
- verschaffen van specifieke bedrijfs- of sectorgegevens (vb. contactgegevens van veiligheidsverantwoordelijken) aan de overheid.



PUBLIEK-PRIVAAT OVERLEG: COMMUNICATIEKANALEN INZAKE TERRORISME

PROTOCOLAKKOORD TUSSEN DE MINISTER VAN JUSTITIE, DE MINISTER VAN BINNENLANDSE ZAKEN EN HET VERBOND VAN BELGISCHE ONDERNEMINGEN

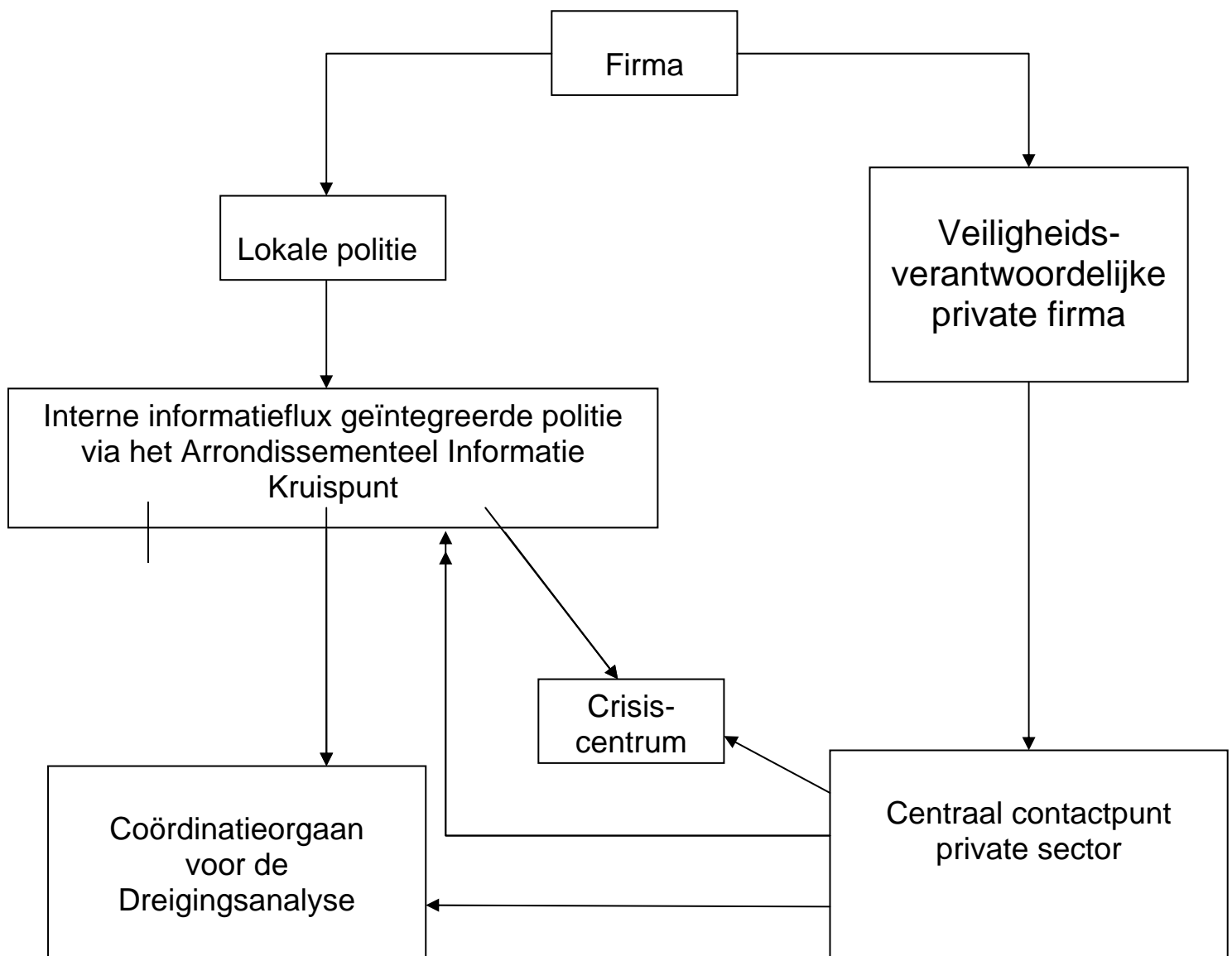
EARLY WARNING SYSTEM

UITGEWERKT IN HET KADER VAN DE WERKGROEP TERRORISME VAN HET PERMANENT OVERLEGPLATFORM BEDRIJFSBEVEILIGING

BIJLAGE A:

BOMALARM - INCIDENT – VERDACHTE HANDELING

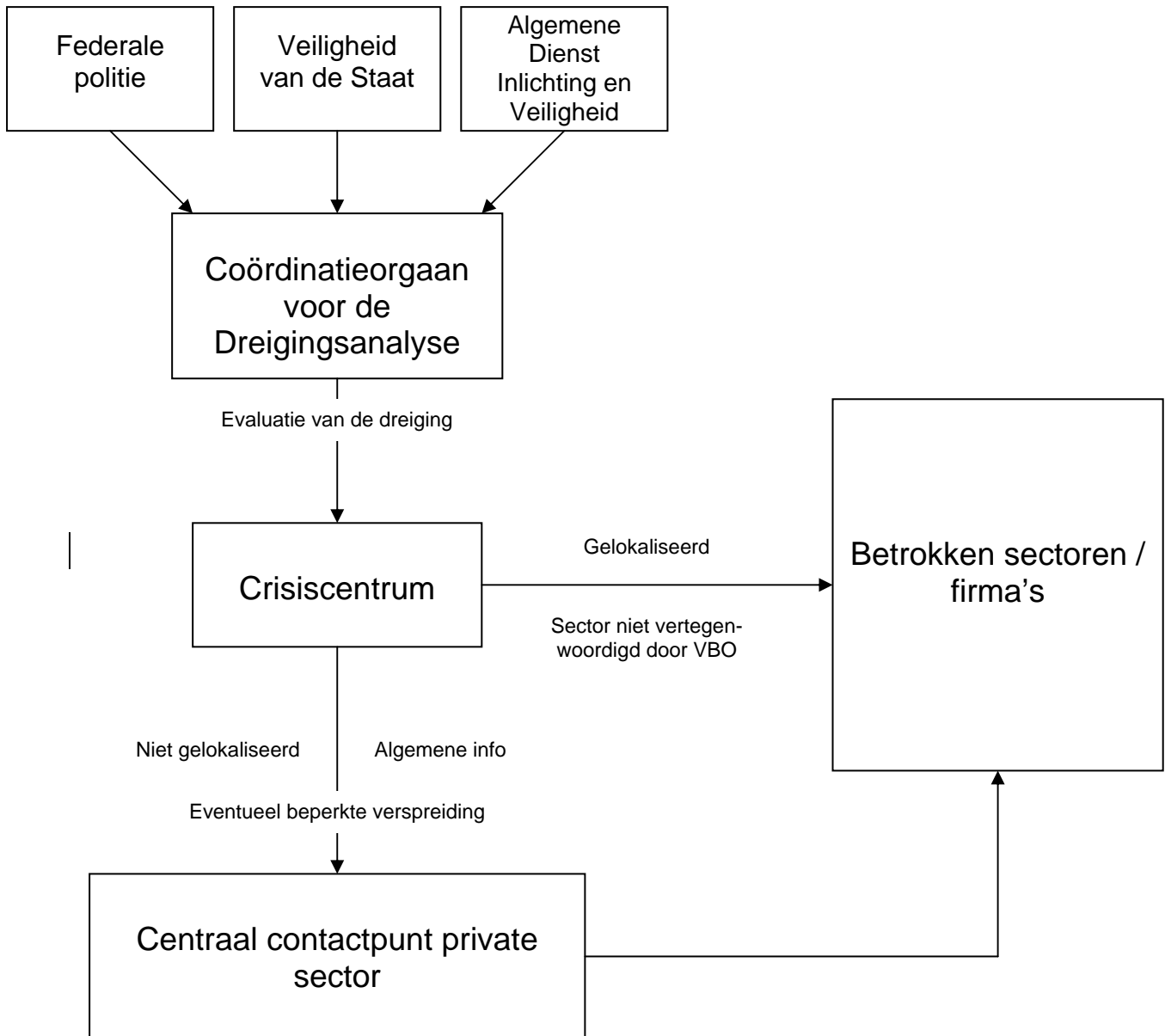
PRIVATE SECTOR → PUBLIEKE SECTOR





BIJLAGE B: BEDREIGINGEN – AANBEVELINGEN

PUBLIEKE SECTOR → PRIVATE SECTOR



(*ook informatiedoorstroming naar federale politie via geëigende kanalen)

Wanneer de private sector van het moederbedrijf in het buitenland verneemt dat de beveiligingsmaatregelen moeten worden opgevoerd, kan via het centrale meldpunt een cross-check van de private naar de publieke sector plaatsvinden.



HET PERMANENT OVERLEGPLATFORM BEDRIJFSBEVEILIGING (POB): Historiek en werking

Onder impuls van de Dienst voor het Strafrechtelijk beleid (DSB) vonden in 1996 de eerste besprekingen plaats rond de creatie van een overlegplatform bedrijfsbeveiliging. In 2000 werd dit opgenomen in het Federaal Veiligheids- en Detentieplan van de toenmalige Minister van Justitie als project 25 rond geweldsdelicten. In 2003 sloten de Minister van Justitie en het Verbond van Belgische Ondernemingen (VBO) een protocolakkoord waarmee het overlegplatform officieel werd opgericht. In dit akkoord worden de structuur, de praktische invulling en de organisatie van het POB vastgelegd en bracht de private sector en de overheid nog dichter bij elkaar. De publiek-private samenwerking is in deze zin een belangrijk instrument in het kader van een integraal en geïntegreerd veiligheidsbeleid.

Naast een Federale Stuurgroep, voorgezeten door de Dienst voor het Strafrechtelijk beleid, werden 4 werkgroepen opgericht die initiatieven hebben uitgewerkt rond specifieke thema's.

Concrete realisaties van het POB zijn de permanente informatie-uitwisseling, het Early Warning System inzake terrorisme en doorgedreven sensibilisering door de organisatie van studiedagen.

Het POB stelt zich de volgende doelstellingen:

- een coherent publiek-privaat overleg;
- de beeldvorming verfijnen, en zodoende een nauwkeurig beeld verkrijgen van de aard en omvang van de criminaliteit tegen bedrijven, de interne criminaliteit, de preventieve maatregelen, de ondervonden schade, het meldings- en aangiftegedrag etc.;
- de aandacht vestigen op nieuwe fenomenen en trends en waar nodig nieuwe (sub)werkgroepen oprichten.

Leden:

- Private sector: VBO
- Publieke sector: Dienst voor het Strafrechtelijk beleid (centraal aanspreekpunt), Cel beleidsvoorbereiding van de Minister van Justitie, College van Procureurs-generaal, federaal parket, federale politie, Veiligheid van de Staat, FOD Binnenlandse Zaken (Crisiscentrum).

A) FEDERALE STUURGROEP (vergaderingen: viermaandelijks)

- Taak:
 - overleg over relevante bedreigingen (nieuwe fenomenen, trends, ...)
 - projecten van PPS en/of overleg begeleiden en evalueren

- Periodieke briefings/dreigingsanalyses door de Veiligheid van de Staat en de federale politie en voorstellingen door de private sector.

B) GEMENGDE WERKGROEPEN (vergaderingen: periodiek)

- 4 werkgroepen (terrorisme, WEP, informaticacriminaliteit, georganiseerde misdaad)
- Taken:
 - inventariseren van wederzijdse behoeften
 - plannen en organiseren van opleiding en vorming
 - opstellen en uitvoeren van actieplannen
 - uitwerking informatiekanaal (dringende uitwisseling van info inzake dreigingen)

Aandachtspunten en realisaties:

WERKGROEP TERRORISME

- Uitwerking modaliteiten inzake communicatie tussen publieke en private partners.
- Preventieve aanpak van terrorisme.

WERKGROEP WETENSCHAPPELIJK EN ECONOMISCH POTENTIEEL

- Definiëring WEP en kritieke infrastructuren.
- Informatiesessies (cases).
- Awareness en sensibilisering.
- Gefundeerde uitbouw WEP.

WERKGROEP INFORMATICACRIMINALITEIT

- Awareness (bedrijven – particulieren) d.m.v. gerichte informatiesessies.
- Beeldvorming.
- National Infrastructure Protection.
- Alarmprocedure bij ICT Security Incidenten.

WERKGROEP GEORGANISEERDE MISDAAD

- Fenomenen (hold-up, middaginbraken, rondtrekkende dadergroepen, ...).
- Definitie en perceptie georganiseerde misdaad.
- Punctuele info-uitwisseling.
- Gestructureerde inbreng private partners in jaarrapport georganiseerde criminaliteit.
- Onderzoek kwetsbaarheid economische sectoren.
- Concreet samenwerkingsproject m.b.t. diefstalproblematiek.
- Brochure 'Ondernemingen en Veiligheid'.

PROJECT BEELDVORMING

- Gaat na op welke wijze gegevens van incidenten, ingezameld door de bedrijven, beter kunnen uitgewisseld worden met de statistische criminaliteitsgegevens ingezameld door de politiediensten. (cfr. bevragingen van federaties aan leden omtrent de slachtoffergevoeligheid met betrekking tot bijvoorbeeld geweld).
- Inventarisering van allerlei classificaties die door verschillende privé-sectoren worden gebruikt (aan de hand van overleg met de financiële sector, dienstensector, transportsector, enz...).
- Initiatieven voor het faciliteren van de uitwisseling van deze statistische gegevens.



PUBLIEK-PRIVAAT OVERLEG: COMMUNICATIEKANALEN INZAKE TERRORISME

**PROTOCOLAKKOORD TUSSEN DE MINISTER VAN JUSTITIE,
DE MINISTER VAN BINNENLANDSE ZAKEN EN HET
VERBOND VAN BELGISCHE ONDERNEMINGEN**

EARLY WARNING SYSTEM

**UITGEWERKT IN HET KADER VAN DE WERKGROEP TERRORISME VAN HET
PERMANENT OVERLEGPLATFORM BEDRIJFSBEVEILIGING**

INLEIDING

Zowel de private sector als de publieke overheid zijn er zich van bewust dat een goede wederzijdse communicatie noodzakelijk is en voor beide sectoren een meerwaarde kan opleveren. In het domein van het terrorisme *sensu lato* komen hiervoor in aanmerking: verdachte handelingen, incidenten, bestaande dreigingen, analyses, nieuwe tendensen en te nemen maatregelen.

De rode draad doorheen dit geheel betreft de creatie van een informatievierkant waar de logica wordt gerespecteerd dat lokale bedrijven of lokale vestigingen de lokale politie beschouwen als centraal aanspreekpunt en dat de nationale vertegenwoordigers van de bedrijven via het *centraal invalspunt* (Belgacom) contacten onderhouden met de diensten die zijn belast met de strijd tegen het terrorisme zoals de Algemene Directie Crisiscentrum (ADCC), het Coördinatieorgaan voor de Dreigingsanalyse (OCAD), de federale politie (DJP/Terrorisme en DGA/DAO) en de Veiligheid van de Staat (VS). Dergelijk informatievierkant is mede gebaseerd op een gestructureerde infolux binnen de respectieve sectoren, waar de informatie doorstroomt van de lokale entiteiten naar de federale partners en vice versa.

De huidige informatiekkanalen tussen de bestuurlijke overheden en politiediensten blijven hierbij onaangetast, alsook de mogelijkheid voor de overheden om de communicatie te beperken tot een aantal sectoren en bedrijven.

Het protocolakkoord doet geen afbreuk aan de meldingsplicht van de politiediensten aan de gerechtelijke autoriteiten. Indien de feiten het voorwerp uitmaken van een strafonderzoek gebeurt de communicatie van dreigingen en aanbevelingen aan de private sector, tenzij andersluidende beslissing van de magistraat wanneer deze mededeling de uitoefening van de strafvordering of de veiligheid van een persoon in gevaar kan brengen.

COMMUNICATIE VAN VERDACHTE HANDELINGEN – INCIDENTEN AAN DE OVERHEID

Indien een bedrijf verdachte handelingen vaststelt, kan het dit melden aan de lokale politie die een eerste beoordeling zal maken. Ook wanneer een bedrijf het slachtoffer is geworden van een incident is het logisch dat klacht wordt neergelegd bij de lokale politie.

Indien uit een eerste analyse blijkt dat de verdachte handelingen of incidenten mogelijk kunnen worden gelinkt aan subversieve, extremistische of zelfs terroristische groeperingen, zal de lokale politie, via de geëigende kanalen, de gespecialiseerde diensten van de federale politie hiervan in kennis stellen. Deze gespecialiseerde diensten stellen op hun beurt de ADCC en OCAD, waarin ook de VS vertegenwoordigers heeft, in kennis.

Daarenboven wordt gevraagd dat de lokale bedrijven, via de daartoe aangeduide verantwoordelijke, het *centraal invalspunt* verwittigen van deze verdachte handelingen of incidenten. Dit *centraal invalspunt* maakt de informatie verder ter exploitatie over aan zowel de ADCC, OCAD als de federale politie (DJP/Terrorisme en DGA/DAO). De VS zal deze informatie krijgen via de ADCC.

COMMUNICATIE VAN DREIGINGEN EN AANBEVELINGEN AAN DE PRIVATE SECTOR

In de schoot van de overheid analyseert OCAD permanent alle gegevens omtrent terrorisme en stelt hieromtrent evaluatieverslagen op ten behoeve van de bestuurlijke en gerechtelijke overheden. De bestuurlijke overheden nemen op basis van deze dreigingsanalyses de nodige preventieve beschermingsmaatregelen.

De genoemde analyses omvatten alle mogelijke potentiële terroristische doelwitten. Derhalve stelt OCAD evaluaties op nopens politieke, diplomatieke en militaire instellingen en personaliteiten. Daarenboven stelt zij ook evaluaties op omtrent private personaliteiten en etnische gemeenschappen. Een derde soort dreigingsanalyse betreft de industriële, financiële en commerciële sectoren.

Specifiek ingevolge deze laatste analyses is het aangewezen om te streven naar een gestructureerde communicatie tussen de (federale) overheid en de bedrijfswereld, opdat de betrokken bedrijven tijdig zouden worden ingelicht van een eventuele dreiging en aldus de gepaste preventieve maatregelen zouden kunnen nemen.

Bij gelokaliseerde dreigingen en bij dreigingen in sectoren die door het Verbond van Belgische Ondernemingen (VBO) niet worden vertegenwoordigd, richt de ADCC zich rechtstreeks en exclusief tot de betrokken sectoren en bedrijven, naast het verwittigen van de federale politie via de geëigende kanalen. De bijdrage die van het VBO wordt verwacht beperkt zich in deze gevallen tot eventuele hulp met betrekking tot het verzamelen van de nodige coördinaten.

De meerwaarde die de nieuwe communicatielijn tussen de ADCC en de private sector zal bieden zit dan ook eerder in algemene en niet-gelokaliseerde dreigingen die zowel gericht kunnen zijn tegen bepaalde sectoren als in een bepaalde regio of zelfs over het hele grondgebied. In dit geval kan de ADCC, naast de gebruikelijke partners, eveneens het *centraal invalspunt* van het VBO verwittigen. Dit *centraal*

invalspunt zorgt dan *on line* voor de verdere verspreiding binnen de private sector, die in de mate van het mogelijke de gepaste preventieve maatregelen neemt.

Ook in deze gevallen behoudt de overheid echter steeds de mogelijkheid om zich rechtstreeks tot bepaalde sectoren te richten, of kan zij het *centraal invalspunt* voorschrijven dat de informatie enkel aan bepaalde sectoren of regio's mag worden meegedeeld.

Indien ondernemingen vernemen van hun buitenlandse moedermaatschappijen dat de dreiging zou zijn toegenomen, kunnen zij dit via het *centraal invalspunt cross-checken* met de ADCC.

De concrete uitwisseling van geclassificeerde informatie zal gebeuren conform de beschikkingen van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen.

OVERLEG MET BETREKKING TOT TENDENSEN, ANALYSES EN MAATREGELEN

De werkgroep Terrorisme van het Permanent Overlegplatform Bedrijfsbeveiliging komt periodiek samen teneinde recente incidenten te ontleden, analyses uit te wisselen, nieuwe tendensen te bespreken, preventiemaatregelen te ontwikkelen, ... Het spreekt voor zich dat deze planning in geval van hoogdringendheid kan worden aangepast.

Ondertekend te Brussel op

De Minister van Justitie

.....

De Minister van Binnenlandse Zaken

.....

Het Verbond van Belgische Ondernemingen

.....