

# **WAT KAN UW BEDRIJF ONDERNEMEN TEGEN TERRORISME?**

**HANDREIKING VOOR BEDRIJVEN**







# **INHOUD**

|                                                             |           |
|-------------------------------------------------------------|-----------|
| <b>Voorwoord</b>                                            | <b>7</b>  |
| <br>                                                        |           |
| <b>1 Inleiding</b>                                          | <b>9</b>  |
| 1.1 Leeswijzer                                              | 9         |
| 1.2 Voor wie?                                               | 9         |
| 1.3 Waarom terrorisme bestrijden?                           | 10        |
| 1.4 Wat mogen overheden en bedrijven van elkaar verwachten? | 12        |
| <br>                                                        |           |
| <b>2 Terroristische dreigingen</b>                          | <b>15</b> |
| 2.1 Dreigingsbeeld terrorisme Nederland                     | 15        |
| 2.1.1 Profiel van (potentiële) terroristen                  | 16        |
| 2.1.2 Selectie van doelwitten                               | 16        |
| 2.1.3 Middelen om aanslagen te plegen                       | 17        |
| 2.1.4 Veranderlijke dreiging                                | 18        |
| 2.2 Potentiële en concrete dreigingen                       | 18        |
| 2.3 Herkennen van potentiële dreigingen                     | 21        |
| 2.3.1 Bedrijf als potentieel doelwit                        | 21        |
| 2.3.2 Bedrijf als potentieel middel                         | 25        |
| 2.3.3 De kwetsbaarheid van het bedrijf                      | 27        |
| 2.4 Herkennen van concrete dreigingen                       | 28        |
| 2.4.1 Verdachte handelingen, tijdstippen en locaties        | 28        |
| 2.4.2 Herkennen van radicalisering                          | 31        |
| <br>                                                        |           |
| <b>3 Wat kunnen bedrijven van de overheid verwachten?</b>   | <b>33</b> |
| 3.1 Landelijk                                               | 33        |
| 3.1.1 De Nationaal Coördinator Terrorismebestrijding (NCTb) | 33        |
| 3.1.2 Het algemene dreigingsbeeld                           | 34        |

|                                                     |           |
|-----------------------------------------------------|-----------|
| 3.1.3 Dreiging tegen een sector                     | 35        |
| 3.1.4 Bescherming Vitale Infrastructuur             | 37        |
| 3.1.5 Andere activiteiten                           | 39        |
| 3.2 Lokaal                                          | 40        |
| 3.2.1 Dreiging tegen personen, objecten of diensten | 42        |
| 3.3 Internationaal en Europees                      | 44        |
| 3.3.1 Veiligheid van de haven en de luchtvaart      | 45        |
| 3.3.2 Ketenbeveiliging                              | 46        |
| 3.4 Waar kunnen bedrijven terecht?                  | 48        |
| <b>4 Risicomanagement</b>                           | <b>53</b> |
| 4.1 Methodiek risicoanalyse                         | 53        |
| 4.2 Afhankelijkheidsanalyse                         | 55        |
| 4.3 Dreigingsanalyse                                | 56        |
| 4.4 Kwetsbaarheidsanalyse                           | 57        |
| 4.5 Risicoanalyse                                   | 58        |
| 4.6 Kosten- en batenanalyse                         | 60        |
| <b>5 Bedrijfsmaatregelen</b>                        | <b>61</b> |
| 5.1 Hoe komt u tot maatregelen?                     | 61        |
| 5.2 Welke maatregelen kunt u nemen?                 | 63        |
| 5.3 Proactieve maatregelen                          | 64        |
| 5.4 Preventieve maatregelen                         | 65        |
| 5.4.1 Objecten en diensten                          | 66        |
| 5.4.2 Personeel                                     | 70        |
| 5.4.3 Informatie                                    | 75        |
| 5.5 Preparatieve maatregelen                        | 77        |
| 5.6 Responsieve maatregelen                         | 80        |
| 5.7 Nazorgmaatregelen                               | 83        |
| 5.8 Checklist voor bedrijven                        | 84        |

|                                             |               |
|---------------------------------------------|---------------|
| <b>BIJLAGEN</b>                             | <b>86</b>     |
| <b>BIJLAGE I</b> VERKLARING VAN WOORDEN     | 86            |
| <b>BIJLAGE II</b> AFKORTINGEN               | 90            |
| <b>BIJLAGE III</b> WEBSITES                 | 91            |
| Binnenland                                  | 91            |
| Buitenland                                  | 93            |
| <b>BIJLAGE IV</b> ACHTERGRONDDOCUMENTATIE   | 95            |
| Binnenland                                  | 95            |
| Buitenland                                  | 95            |
| <b>BIJLAGE V</b> DREIGINGSNIVEAUS NEDERLAND | 96            |
| <b>BIJLAGE VI</b> DREIGINGSSYSTEMEN         | 97            |
| <b>BIJLAGE VII</b> VOORBEELDEN MAATREGELEN  | 98            |
| <br><b>COLOFON</b>                          | <br><b>99</b> |

# **VOORWOORD**

Terrorisme. U leest erover in de krant en hoort erover op radio en televisie. Misschien lijkt het voor uw bedrijf ver weg, maar ook u en uw medewerkers kunnen met terrorisme te maken krijgen. Direct, als terroristen uw bedrijf als doelwit op het oog hebben bijvoorbeeld. Ook indirect kunt u te maken krijgen met de consequenties van een terroristische aanslag als uw bedrijf afhankelijk is of in de buurt van een mogelijk doelwit staat. Daarnaast kunnen terroristen producten, diensten en informatie van uw bedrijf misbruiken.

Deze handreiking is bedoeld voor alle bedrijven. Of u nu eigenaar of werknemer bent van een groot of klein bedrijf: het is goed dat u weet dat ook u kwetsbaar kunt zijn voor terroristische dreigingen of aanslagen en op welke aspecten.

Dit klinkt misschien alarmerend, maar het is zeker niet onze bedoeling om met deze handreiking onrust te zaaien of een klopjacht op potentiële terroristen te ontketen. Toch moeten we ermee rekening houden dat ook in Nederland een aanslag kan plaatsvinden. Om dit bewustzijn te creëren biedt deze handreiking inzicht in terroristische dreigingen en de organisatie van en het beleid over terrorismebestrijding in Nederland.

7

Het is nuttig na te denken hoe uw bedrijf met terrorisme om zou kunnen én willen gaan. In deze handreiking leest u hoe u uw bestaande (veiligheids)beleid kunt aanpassen. U heeft al een belangrijke stap gezet wanneer uw personeel alert is op ongebruikelijke of verdachte activiteiten en deze doorgeeft aan de verantwoordelijke in uw bedrijf.

Zulke signalen verneemt de overheid ook graag. Het helpt de autoriteiten beter op te treden bij een dreiging. Geef signalen van ongebruikelijke handelingen en situaties altijd door aan de plaatselijke politie.

Terrorismebestrijding is niet alleen een zaak van landelijke en lokale overheden, maar ook van bedrijven. Bedrijven en overheden hebben beide een (maatschappelijke) verantwoordelijkheid voor de veiligheid van Nederland.

Over terrorismebestrijding is veel informatie beschikbaar. Aanvullende en actuele informatie kunt u vinden op de website [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven). Natuurlijk kunt u ook altijd contact opnemen met uw branche- of ondernemersorganisatie.

De minister van Justitie

De minister van Binnenlandse Zaken en Koninkrijksrelaties



# **1. INLEIDING**

## **1.1 LEESWIJZER**

Deze handreiking is zo opgesteld dat alle onderdelen los van elkaar te lezen zijn.

De handreiking is als volgt opgebouwd:

- In hoofdstuk 3 komt de organisatie van en het beleid over terrorismebestrijding door de Europese, landelijke en lokale overheid aan de orde;
- Hoofdstuk 4 behandelt de wijze waarop bedrijven hun eigen risico's kunnen inschatten;
- Hoofdstuk 5 gaat in op de (beveiligings)maatregelen die bedrijven kunnen nemen.

**Doel van deze handreiking is de bewustwording van bedrijven te vergroten, door inzicht te geven in:**

- potentiële terroristische dreigingen voor bedrijven;
- de organisatie van en het beleid over terrorismebestrijding door de overheden;
- de bijdrage die bedrijven kunnen leveren aan terrorismebestrijding;
- waar bedrijven terecht kunnen met signalen en vragen.

9

De bijlagen bij deze handreiking bevatten een overzicht van afkortingen, documentatie, websites en organisaties die bij terrorismebestrijding zijn betrokken. Ook vindt u aanvullende informatie over de dreigingniveaus, maatregelen en diverse overheidssystemen om de dreigingen in kaart te brengen.

## **1.2 VOOR WIE?**

Deze handreiking is bedoeld voor *alle* bedrijven. Voor grotere én kleinere bedrijven kan de handreiking aanleiding zijn om na te denken over terroristische dreigingen en de gevolgen daarvan voor hun bedrijf.

Het ene bedrijf loopt meer risico dan het andere. Sommige bedrijven weten dit al. Andere bedrijven realiseren zich niet altijd dat zij interessant zijn voor terroristen. Juist voor hen is deze handreiking bedoeld. Op basis van de informatie in deze handreiking kunnen bedrijven afwegen of het zinvol is om maatregelen te treffen.

### **Wat bedoelen we met terrorisme en terrorismebestrijding?**

#### **Terrorisme is:**

- het op mensenlevens gerichte plegen van of dreigen met geweld door individuen of groepen;
  - het ontwrichten van de samenleving; en/of
  - het toebrengen van ernstige schade,
- met als doel maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden.

#### **Terrorismebestrijding richt zich op:**

- de kans verkleinen op een terroristische aanslag of dreiging;
- de gevolgen van aanslagen beperken;
- terroristen opsporen en vervolgen.

10

### **1.3 WAAROM TERRORISME BESTRIJDEN?**

De continuïteit van uw bedrijf kan in gevaar komen als u kwetsbaar bent voor terrorisme. Terrorisme is dus één van de risico's waar uw bedrijf mee te maken kan krijgen. Net als bij andere risico's die zich kunnen voordoen zoals criminaliteit, neemt u maatregelen. Veel bedrijven hebben al een veiligheidsbeleid. Dan rijst de vraag of het nodig is om extra beveiligingsmaatregelen tegen terrorisme te nemen.

Laten we eerlijk zijn, aanvullende beveiligingsmaatregelen brengen kosten met zich mee. Bedrijven betalen zelf deze kosten. Een tweede nadeel is volgens sommige bedrijven dat de kans bestaat dat signalen die zij aan de overheid doorgeven, openbaar worden. Dat kan van invloed zijn op de goede naam van het bedrijf. Weinig bedrijven willen dat concurrenten weten dat terroristen een poging hebben gedaan om bijvoorbeeld informatie te stelen. Overigens wordt niet alle informatie openbaar. Ten slotte kunnen overheden bedrijven verplichten bepaalde maatregelen te nemen. Dit geldt ook voor bedrijven onderling. Zo moeten bedrijven voldoen aan extra eisen van de Amerikaanse overheid om goederen de douane te laten passeren. Bij een verhoogde terroristische dreiging kunnen bedrijven te maken krijgen met extra voorwaarden. Daarnaast kunnen overheden structurele eisen stellen om de kans op terroristische aanslagen te beperken. Deze eisen kunnen in eerste instantie een handelsbelemmerende werking hebben, zeker wanneer alleen een deel van de bedrijven aan deze eisen moet voldoen.

Gelukkig brengen extra beveiligingsmaatregelen ook voordelen met zich mee. Ze bevorderen de beveiliging van het bedrijf als geheel. Dat betekent dat deze maatregelen ook criminaliteit helpen te beperken. Daarnaast kan het nadenken over beveiliging een aanzet zijn tot organisatorische of informatietechnische maatregelen die kunnen leiden tot efficiënter werken. De maatregelen kunnen ook de bedrijfscontinuïteit beter helpen te waarborgen en kunnen de kans op economische schade beperken. Bijvoorbeeld omdat back-up-bestanden ergens anders worden bewaard, zodat het bedrijf weer snel kan overgaan tot de normale gang van zaken.

Aandacht voor terrorismebestrijding kan het bedrijfsimago verbeteren. Klanten doen waarschijnlijk sneller zaken met bedrijven waarvan ze weten dat hun goederen veilig zijn. Aandacht voor terrorismebestrijding kan ook het imago van het hele Nederlandse bedrijfsleven versterken. En dit is weer goed voor de concurrentiepositie van individuele bedrijven. Een ander voordeel van aandacht voor terrorisme in het veiligheidsbeleid van het bedrijf is dat daarmee bedrijven voldoen aan eisen die overheden of andere bedrijven stellen. Dat kan bijvoorbeeld een beperktere - en dus snellere - controle op de lading opleveren.

Een laatste voordeel is de informatievoorziening tussen overheden en bedrijven. Als bedrijven verdachte zaken melden bij de plaatselijke politie, ontstaat een beter beeld van dreigingen. De lokale autoriteiten kunnen bedrijven daardoor gerichter informeren en eventueel de kans op een aanslag verminderen.

Een nuance is hier op zijn plaats. Niet alle voordelen gelden voor alle bedrijven. Bovendien kunnen de voordelen optreden, maar het is geen wet van Meden en Perzen. En we moeten realistisch blijven. Nederland is een open maatschappij. We kunnen niet alle gevaren uitsluiten. Dat geldt ook voor terroristische dreigingen en aanslagen.

#### **Redenen om bedrijfsmaatregelen tegen terrorisme te nemen:**

1. voorkomen van een terroristische aanslag;
2. investeren in beveiliging van het bedrijf als geheel;
3. aanzet tot efficiënter werken;
4. waarborgen van de bedrijfscontinuïteit en voorkomen van economische schade;
5. verbeteren van het bedrijfsimago;
6. voldoen aan (wettelijke) verplichtingen;
7. betere informatievoorziening tussen overheden en bedrijven.

12

### **1.4 WAT MOGEN OVERHEDEN EN BEDRIJVEN VAN ELKAAR VERWACHTEN?**

Alhoewel we niet alle gevaren kunnen uitsluiten, kunnen we wél proberen de risico's te verminderen. Dat vraagt om adequaat optreden van de publieke én de private sector. De overheid is verantwoordelijk voor de openbare orde en veiligheid. Bedrijven zijn verantwoordelijk voor de veiligheid van hun goederen, diensten en personeel. Dat betekent dat bedrijven zelf afdoende maatregelen moeten nemen om hun eigendommen en personeel te beschermen.

### **Praktijk: Maximale invloed op risico's aanwenden**

'Terrorismebestrijding begint met een risicoanalyse. Dan volgt een afweging hoe je met die risico's wilt omgaan. Het is vaak onvoorspelbaar hoe terroristische aanslagen zich zullen uiten. Alleen al in Nederland hebben wij 700 winkels, zodat fysieke beveiligingsmaatregelen nemen tegen bijvoorbeeld een bomaanslag, bijna onuitvoerbaar is. Ondernemers moeten vooral investeren in maatregelen die het risico op een aanslag ook echt kunnen beperken. Denk aan het verstoren van onze voedselketen door terroristen. Ahold verkoopt een kwetsbaar product: voedsel. Omdat we precies weten hoe de keten er bij ons uit ziet - van productie tot distributie en levering in de winkels - kunnen we maatregelen nemen om de levering van het product zoveel mogelijk te waarborgen. Daarnaast bouwen we winkels met voorzieningen die de veiligheid van onze klanten en personeel zo goed mogelijk garanderen.'

*John Fonteijn, Corporate Security Adviser van Ahold*

Omdat de overheid en bedrijven elk hun eigen verantwoordelijkheid hebben voor de veiligheid van Nederland, moeten ze erop kunnen vertrouwen dat ieder de gewenste en noodzakelijke maatregelen neemt als er een dreiging is. Zo zijn burgers en ook bedrijven verplicht aangifte te doen van misdrijven. Voor enkele gebieden geldt voor bedrijven ook een wettelijk plicht tot het nemen van maatregelen. Voor andere terreinen geldt dit niet. Toch kan de overheid bedrijven aanspreken op hun inspanning. Zeker als de overheid afhankelijk is van bedrijven om het gewenste veiligheidsniveau te bereiken. Als bedrijven geen acties ondernemen tegen een dreiging, kan de overheid ook de veiligheid niet garanderen, en andersom. Daarom is samenwerking belangrijk. Op alle niveaus, maar in het bijzonder op lokaal niveau: tussen bedrijven en de plaatselijke politie en gemeente.

**Dit mogen bedrijven van de overheid verwachten:**

- voldoende informatie over potentiële en concrete dreigingen;
- effectieve en efficiënte werking van systemen en besluitvormingsprocessen tijdens een terroristische dreiging of aanslag.

**Dit mag de overheid van bedrijven verwachten:**

- een bijdrage aan het bevorderen van veiligheid, inclusief het nemen van maatregelen als dat noodzakelijk is;
- melding of aangifte doen bij de politie in geval van verdachte handelingen of activiteiten.



## **2. TERRORISTISCHE DREIGINGEN**

Terrorismebestrijding begint met goede informatie. Op basis daarvan kunnen overheden en bedrijven terroristische dreigingen en activiteiten herkennen en zonodig maatregelen nemen.

In dit hoofdstuk beschrijven we:

- het dreigingsbeeld voor Nederland;
- hoe bedrijven terroristische dreigingen kunnen herkennen;
- op hoofdlijnen de trends en ontwikkelingen in de terroristische dreiging voor Nederland. Bedrijven kunnen deze informatie gebruiken om terroristische dreigingen die op hen gericht zijn in een bredere context te plaatsen;
- de aantrekkelijkheid en kwetsbaarheid van bedrijven voor terroristische dreiging;
- een inschatting van de potentiële dreiging voor een bedrijf aan de hand van de aantrekkelijkheid en de kwetsbaarheid van het bedrijf.

### **2.1 DREIGINGSBEELD TERRORISME NEDERLAND**

15

De Nationaal Coördinator Terrorismebestrijding (NCTb) stelt iedere drie maanden het niveau van de terroristische dreiging in Nederland vast. Dit niveau kan (oplopend) vastgesteld worden op minimaal, beperkt, substantieel of kritiek.

Het algemene dreigingsniveau voor terrorisme in Nederland is sinds de zomer van 2004 'substantieel'. Dat betekent dat de kans reëel is dat er in ons land een aanslag kan plaatsvinden. Deze kans is niet overal in dezelfde mate aanwezig, en kunnen we ook niet zonder meer specificeren naar een gebied of locatie. Het dreigingsniveau is gebaseerd op enkele belangrijke ontwikkelingen, zoals ideologieën, motivatie van potentiële terroristen, de vorming van potentieel terroristische netwerken en hun keuze voor doelwitten en middelen om activiteiten te ondernemen.

Nederland heeft het meest te maken met jihadistisch terrorisme en separatistisch terrorisme. De afgelopen jaren is de terroristische dreiging in Nederland vooral afkomstig van jihadistisch terrorisme: extremistische gelovigen die gewelddadige middelen accepteren en inzetten om

hun geloof te verdedigen of uit te breiden. Het aantal radicale gelovigen dat geweld wil gebruiken is overigens klein.

Separatistische terroristen strijden voor afscheiding van een bepaald deel van een land. Nederland kent zelf geen separatistische groepen. Soms zijn wel buitenlandse separatistische groepen actief in ons land.

### **2.1.1 PROFIEL VAN (POTENTIËLE) TERRORISTEN**

Het profiel van terroristen in Nederland verandert snel, is complex en niet altijd eenduidig. Daardoor is het niet makkelijk ze te herkennen. Het aantal (potentiële) terroristen in Nederland is beperkt, maar zij zijn wel in staat om een aanslag te plegen.

De huidige groep (potentiële) terroristen bestaat voor het grootste deel uit jonge mannen en vrouwen van verschillende nationaliteiten. Ze zijn meestal tussen de 16 en 25 jaar oud en ze zijn voornamelijk in Nederland geboren. Het gaat vaak om de tweede en derde generatie islamitische allochtonen én bekeerlingen. Ze radicaliseren veelal via internet zonder directe aansturing van anderen. Hierdoor zijn veel individuele (potentiële) terroristen en netwerken anarchistisch. De huidige generatie terroristen richt zich nadrukkelijker dan eerdere (buitenlandse) generaties op de Nederlandse samenleving.

### **2.1.2 SELECTIE VAN DOELWITTEN**

Traditionele doelwitten voor een terroristische aanslag zijn objecten die symbool staan voor landen of regeringen die als 'anti-islamitisch' worden gezien, zoals ambassades, regeringsgebouwen, militaire objecten of vliegtuigen van vliegmaatschappijen van die landen. Dit zijn meestal 'hard targets'. De afgelopen vijftien jaar richten terroristen zich ook steeds meer op 'soft targets'. Dit zijn locaties en objecten die een 'open' publieke functie hebben en daardoor moeilijk te beveiligen zijn, zoals hotels en stations. Met aanslagen op zulke doelwitten willen terroristen - meer dan in het verleden - de burgerbevolking treffen. Ze vinden dat de burgers medeverantwoordelijk zijn voor het beleid van hun regering en kunnen zo regeringen onder druk zetten.



Ook delen van de vitale infrastructuur, zoals bruggen en tunnels, zijn potentiële terroristische doelwitten. Tot slot richten terroristen hun aandacht op individuele personen, zoals columnisten en parlementariërs die zich negatief uitlaten over de islam. Doordat er zoveel mogelijke doelwitten zijn, wordt de hele samenleving steeds meer bedreigd.

### **Praktijk: De identiteit van de gast**

‘Als een buitenlandse diplomaat komt logeren, kan hij een doelwit zijn. Het is dus verstandig om als hotelier stil te staan bij de identiteit van gasten. Zo dacht ik laatst mee met de politie over de beveiliging van een Israëlisch feest.

Wie heb ik in huis? Dat is de centrale vraag. Natuurlijk is het onmogelijk elke gast te controleren. Maar met bewustwording kun je veel bereiken. Managers kunnen hun receptionisten er bijvoorbeeld op wijzen dat ze structureel aandacht besteden aan een nauwkeurige registratie, zodat de politie snel in actie kan komen. Daarnaast kunnen hoteliers allerlei algemene maatregelen nemen. We hebben wel eens aan de gemeente gevraagd metalen prullenbakken voor de deur te verwijderen. Een bom kan door het metaal extra schade veroorzaken.’

*Ron de Groot, zelfstandig veiligheidsadviseur*

17

### **2.1.3 MIDDELEN OM AANSLAGEN TE PLEGEN**

Terroristen hebben veel middelen om aanslagen mee te plegen, zoals een vuistwapen, een mes, een machinepistool en een handgranaat. Daarnaast maken terroristen zelf explosieven en experimenteren ze met giftige stoffen. Veel van de benodigde grondstoffen voor explosieven zijn in Nederland eenvoudig te verkrijgen.

#### **Eenvoudig explosieven maken en gebruiken**

Vaak gebruiken terroristen grondstoffen die op zichzelf ongevaarlijk zijn. Het is steeds makkelijker geworden om explosieven te maken en ze effectief te gebruiken. Op internet staat bijvoorbeeld hoe je een bom kunt maken van een mengsel van een bepaald type

kunstmest met stookolie. Bij de aanslagen in Londen maakten de daders gebruik van waterstofperoxide. Ook andere makkelijk verkrijgbare middelen worden gebruikt. In het buitenland zijn plannen gevonden om de watervoorziening met cyanide te vergiftigen. En bij terroristen in Engeland die burgers wilden vergiftigen, zijn recepten voor giftige stoffen aangetroffen met zelf gewonnen ricine uit de wonderboon (magic bean) als ingrediënt.

Een heel ander manier om aanslagen te plegen is een zelfmoordaanslag. Leden van terroristische netwerken in Nederland lijken hiertoe steeds meer bereid. Deze opofferingsbereidheid maakt het moeilijker de kans op aanslagen te verminderen, omdat waarschuwingssignalen, zoals verdachte pakketten of onbeheerde bagage, ontbreken. Tot slot is de kennis van terroristen over informatie- en communicatietechnologie toegenomen. Hierdoor kunnen terroristen ook digitale aanvallen uitvoeren op bijvoorbeeld websites en computersystemen.

#### **2.1.4 VERANDERLIJKE DREIGING**

18

De dreiging van het terrorisme kan uit veel hoeken komen en gericht zijn tegen veel doelwitten. Bovendien kunnen terroristen veel middelen inzetten. Door deze complexiteit is het moeilijk dreigingen tegen individuele objecten te onderkennen en in te schatten. Bovendien willen terroristen verrassen. Zij zullen hun best doen om op een ongebruikelijke manier toe te slaan en zo beveiligingsmaatregelen te omzeilen. De dreiging is dus veranderlijk. Daarom is het goed dat bedrijven zich op de hoogte stellen van de actuele algemene dreiging. Op de website [www.nctb.nl](http://www.nctb.nl) staat het actuele dreigingsniveau. Ook wordt uitgelegd waaruit de dreiging bestaat. De volgende paragraaf gaat in op dreiging die specifiek op bedrijven is gericht.

#### **2.2 POTENTIËLE EN CONCRETE DREIGINGEN**

Soms zijn er aanwijzingen dat een bedrijf daadwerkelijk geconfronteerd gaat worden met een terroristische dreiging. We spreken dan van een concrete dreiging. Deze dreiging heeft doorgaans betrekking op het bedrijf als doelwit. Soms gaat het om een bedrijf dat terroristen

als middel willen misbruiken. Bij een concrete dreiging is de precieze intentie van terroristen vastgesteld of zijn voorbereidende terroristische handelingen geconstateerd. Ontbreken zulke aanwijzingen, maar is een bedrijf wel aantrekkelijk voor terroristen, dan spreken we van een potentiële dreiging.

Naast het scenario waarbij een bedrijf een doelwit of middel is, kan een bedrijf nog op twee andere manieren te maken krijgen met terrorisme. Zo kan een bedrijf getroffen worden door uitstralingseffecten van een terroristische aanslag. Ook kan een bedrijf geradicaliseerd personeel in dienst hebben. Het gaat om personen die al vergevorderd zijn in hun radicalisering. Dat betekent dat zij in toenemende mate terroristische activiteiten goedkeuren en deze in de toekomst mogelijk ook willen ondersteunen of uitvoeren.

#### **Zo kunnen bedrijven te maken krijgen met terroristische dreiging:**

- **doelwit:** terroristen plegen doelbewust een aanslag op een bedrijf omdat het aan bepaalde eigenschappen voldoet. Een voorbeeld hiervan is een bedrijf waar door een aanslag veel slachtoffers zullen vallen;
- **middel/misbruik:** sommige bedrijven beschikken over informatie, producten of diensten die terroristen kunnen gebruiken voor de voorbereiding en uitvoering van een aanslag. Denk aan chemische bedrijven en apothekers;
- **schadelijke uitstralingseffecten van een aanslag:** een bedrijf is afhankelijk of staat in de buurt van een doelwit van een terroristische aanslag en loopt daardoor fysiek of economisch onbedoeld schade op. Bijvoorbeeld een bedrijf dat naast een bedreigde ambassade staat;
- **geradicaliseerd personeel:** soms zijn er aanwijzingen dat personeelsleden mogelijk bereid zijn terroristische activiteiten goed te keuren, te ondersteunen of uit te voeren. Personeel zou bijvoorbeeld informatie aan terroristen kunnen overhandigen.

### **Potentiële dreiging: voorstelbare dreiging**

Om te bepalen of een bedrijf een aantrekkelijk doelwit of middel is, moeten we kijken naar het 'aantrekkelijkheidsprofiel' dat terroristen lijken te gebruiken. Dit profiel bestaat uit verschillende bedrijfseigenschappen die terroristen lijken te hanteren om te bepalen of het bedrijf in aanmerking komt voor een terroristische activiteit.

Het 'aantrekkelijkheidsprofiel' is te achterhalen aan de hand van informatie over terroristische aanslagen uit het verleden en/of uit documenten van terroristische groepen. Hoe duidelijker het 'aantrekkelijkheidsprofiel' is, en hoe meer dit profiel overeenkomt met de eigenschappen van een bedrijf (het 'bedrijfsprofiel'), des te waarschijnlijker de (potentiële) dreiging van een aanslag op of misbruik van het betreffende bedrijf is. In dit geval is het bedrijf een potentieel doelwit of middel. Bij bedrijven in de directe omgeving van een potentieel doelwit of bedrijven die als klant van dat bedrijf afhankelijk zijn, is een potentieel risico op schadelijke uitstralingseffecten aanwezig. De potentiële dreiging wordt vergroot als een bedrijf kwetsbaar is, bijvoorbeeld omdat het weinig beveiligingsmaatregelen heeft genomen.

20

Als het 'aantrekkelijkheidsprofiel' sterk overeenkomt met de werkelijke eigenschappen van een bedrijf (het 'bedrijfsprofiel'), geeft dat zelden zekerheid over de potentiële dreiging. Het 'aantrekkelijkheidsprofiel' is immers verkregen op basis van informatie uit het verleden, terwijl terroristen hun werkwijze continu veranderen. Toch biedt een vergelijking tussen een bedrijfsprofiel en een aantrekkelijkheidsprofiel wel enige houvast.

### **Concrete dreiging: aanwijzingen dat een reële dreiging bestaat**

Als er aanwijzingen zijn dat terroristen daadwerkelijk de intentie hebben of voorbereidingen treffen om een terroristische aanslag te plegen of om misbruik te maken van informatie, producten of diensten van een bedrijf, spreken we van een concrete dreiging. Hoe duidelijker en specifieker de informatie, hoe beter we de dreiging kunnen voorspellen. Bovendien maakt eenduidige informatie het makkelijker maatregelen te nemen.

Een concrete dreiging kan blijken uit informatie die politie en inlichtingendiensten hebben over potentiële aanslagplegers. Als de informatie concreet is, onderneemt de lokale en/of landelijke overheid altijd actie.

Een concrete dreiging kan ook blijken uit informatie over een bepaald doelwit. Het gaat dan om gedragingen en gebeurtenissen nabij of ten aanzien van een bedrijf waaruit afgeleid kan worden dat terroristen bezig zijn om bijvoorbeeld een aanslag voor te bereiden. Soms beschikken overheden en bedrijven over informatie die, als ze bij elkaar wordt gevoegd, leidt tot bruikbare informatie over dreigingen. Daarom is het belangrijk dat bedrijven signalen van ongebruikelijke handelingen en situaties doorgeven aan de plaatselijke politie.

## **2.3 HERKENNEN VAN POTENTIËLE DREIGINGEN**

De sterkste dreiging gaat op dit moment uit van het jihadistisch terrorisme. Daarom besteden we de meeste aandacht aan elementen die hiermee samenhangen.

### **2.3.1 BEDRIJF ALS POTENTIEEL DOELWIT**

Bij de keuze van een doelwit kijken terroristen naar de effecten die zij met een aanslag kunnen bereiken:

- zoveel mogelijk slachtoffers maken;
- een zo groot mogelijke economische schade veroorzaken;
- calamiteiten veroorzaken;
- maatschappelijke waarden treffen (symbolische daad stellen);
- maatschappelijke onrust veroorzaken.

Deze elementen maken deel uit van het aantrekkelijkheidsprofiel van een bedrijf.

## Slachtoffers

Terroristen waarschuwen tegenwoordig zelden tot nooit voor een specifieke aanslag. Hierdoor vergroten zij de kans op een aanzienlijk aantal slachtoffers. Met het maximale afschrikkingseffect dat terroristen hiermee bereiken, kunnen ze maatschappelijke en politieke processen beïnvloeden. Zoals de bomslagen op treinen in maart 2004 die kort voor de Spaanse landelijke verkiezingen plaatsvonden.

De volgende bedrijfseigenschappen vergroten de kans op een groot aantal slachtoffers:

- **concentraties van mensen:** bijvoorbeeld in en rond winkelcentra, stadions, concerten, bioscopen, horeca, bedrijven op luchthavens en treinstations;
- **specifieke omstandigheden die de dodelijkheid van een aanslag vergroten:** de hoogte en snelheid van een doelwit, materiaal in de omgeving dat kan branden of als rondvliegend gruis kan dienen (bijvoorbeeld glas);
- **problematische toegankelijkheid voor hulpverlening:** ondergrondse (tunnels) of hooggelegen locaties, locaties op het water of in de lucht.

22

## Economische schade

Het toebrengen van economische schade aan individuele bedrijven én aan landen is voor terroristen niet alleen een manier om wraak te nemen op de westerse welvaart, maar ook een methode om de slagkracht en prioriteitstelling van landen te beïnvloeden. Bij grote binnenlandse economische problemen zal de regering haar aandacht daaraan moeten besteden.

De kans op economische schade neemt toe als door het uitschakelen van een doelwit:

- de marktprijs van een noodzakelijke dienst of product - zoals energie - sterk en/of langdurig stijgt;
- een product of dienst niet beschikbaar is terwijl de samenleving daarvan afhankelijk is. Denk aan het uitvallen van vitale diensten en infrastructuur waarvan andere productieprocessen afhankelijk zijn, zoals het telecomnetwerk;

- veel investeringen nodig zijn voor herstel, bijvoorbeeld een aanslag op grootschalige infrastructuur.

### **Activiteiten die calamiteiten veroorzaken**

Bij terroristische activiteiten die erop zijn gericht calamiteiten te veroorzaken, is de verwoestende schade pas in tweede instantie het gevolg van een terroristische aanslag. Dit is bijvoorbeeld het geval bij een:

- explosie, als explosieve middelen zijn opgeslagen in het bedrijf;
- vergiftiging, als giftige biologische en/of chemische middelen zijn opgeslagen in het bedrijf;
- besmetting, als giftige biologische en/of nucleaire middelen zijn opgeslagen in het bedrijf.



23

### **Maatschappelijke waarden (symbolische daad)**

Terroristen keuren sommige maatschappelijke waarden af vanwege hun inhoud. Hierbij gaat het om ideologische en religieuze waarden. Als terroristen maatschappelijke waarden willen treffen, treffen ze bedrijven die daarvoor representatief zijn of model staan. Ze stellen daarmee een symbolische daad. Het gaat om:

- bedrijven met een specifieke 'nationaliteit' vanwege hun verbondenheid met de 'anti-islamitische' waarden van een land of regering. De verbondenheid kan ontstaan door persoonlijke banden met een regering. Ook is het mogelijk dat een bedrijf specifieke diensten of goederen zoals wapens levert aan een overheid die betrokken of aanwezig is bij een militair conflict in islamitische landen. De lijst van vermeende 'anti-islamitische' landen verandert continu. Terroristen noemen op dit moment vaak landen als de Verenigde Staten, het Verenigd Koninkrijk, Israël en Australië.
- bedrijven die goederen of diensten produceren en/of verlenen die jihadisten als 'verboden' beschouwen. Denk aan objecten die staan voor de consumptie en verkoop van onder andere alcohol, en goederen en diensten die in relatie staan tot de seksuele moraal.

**Een bedrijf heeft een hoger aantrekkelijkheidsprofiel als er kans is op:**

- veel slachtoffers;
- grote economische schade;
- het veroorzaken van calamiteiten;
- aantasting van specifieke maatschappelijke waarden / stellen van een symbolische daad;
- maatschappelijke onrust.

### **Maatschappelijke onrust**

De mate van maatschappelijke onrust die terroristen door een aanslag kunnen veroorzaken is ook een element van het 'aantrekkelijkheidsprofiel' van een bedrijf. Hiervoor is niet eens altijd een aanslag nodig. Een dreiging met een aanslag kan een zo grote angst veroorzaken, dat er maatschappelijke onrust optreedt.

Angst kan toenemen als de dreigingen:

- zich richten op een doel dat de hulpverlening bemoeilijkt, bijvoorbeeld bij moeilijk toegankelijke locaties;



- zich richten op een doel dat de slachtoffers een gevoel geeft van afhankelijkheid en hulpeloosheid omdat zij niet weg kunnen. Denk aan een vliegtuig in de lucht en een rijdende trein;
- zich zodanig manifesteren dat het gevaar - het middel om de aanslag te plegen - onzichtbaar is. Chemische, biologische, radiologische of nucleaire middelen kunnen bijvoorbeeld vergiftiging binnen de voedselketen veroorzaken;
- zich richten op specifieke categorieën slachtoffers, zoals kinderen en bejaarden.

### **2.3.2 BEDRIJF ALS POTENTIEEL MIDDEL**

Terroristen kunnen bedrijven misbruiken om aanslagen voor te bereiden en uit te voeren. Het gaat om informatie, goederen of diensten die terroristen kunnen gebruiken voor de selectie of verkenning van doelwitten. Ook kunnen terroristen producten gebruiken als grondstof voor explosieven. Ten slotte hebben terroristen financiële middelen nodig om een aanslag te kunnen plegen of in hun eigen onderhoud te voorzien.

#### **Praktijk: Authentieke recepten**

‘De echtheid van het recept speelt een belangrijke rol in het voorkomen van misbruik. Als het recept er anders uit ziet dan we gewend zijn, is dat verdacht. Denk aan afwijkend taalgebruik of de naam van een onbekende arts. En natuurlijk zijn we extra waakzaam als het gaat om giftige of explosieve stoffen. Van elke stof weten we in welke hoeveelheden ze normaal gesproken worden gebruikt. Als iemand hier komt voor een liter zuivere alcohol of ether, is het logisch dat hij dat niet meekrijgt. Dat geldt ook voor stoffen die minder bekend zijn bij het grote publiek. Als apotheker voel ik mij niet alleen verantwoordelijk voor de gezondheid van mensen, maar ook voor de veiligheid in het algemeen.’

*Lisa Budihardjo, apotheker van apotheek Tanthof, Delft*

De kans dat terroristen producten, informatie of goederen van een bedrijf gebruiken, is afhankelijk van:

- **de locatie van het bedrijf:**
  - vlakbij een potentieel doelwit, zoals een bedreigde ambassade.
- **de kennis en informatie van een bedrijf over:**
  - **middelen** zoals 'recepten' om wapens en explosieven te vervaardigen;
  - **potentiële doelwitten** zoals de adresgegevens van belangrijke politici en openbare gebouwen;
  - **kwetsbaarheidsgegevens** zoals de beveiliging van potentiële doelwitten.
- **de informatie, goederen en diensten van het bedrijf die van nut kunnen zijn bij het voorbereiden van aanslagen:**
  - **bieden van onderdak** zoals (huur)woningen, hotelkamers en logeeradressen. Type bedrijven: hotels, woningcorporaties, campings en vakantieparken;
  - **financiële diensten** zoals het omwisselen, ontvangen en verzenden van geld. Type bedrijven: banken, wisselkantoren en moneytransferbedrijven;
  - **communicatiemiddelen** zoals het aanbieden van (mobiele) telefonie en internet. Type bedrijven: belhuizen, telecom operators en internetcafés;
  - **verkenningmiddelen** zoals survivaluitrustingen en verrekijkers. Type bedrijven: 'dumpshops' en elektronicazaken;
  - **aanslagmiddelen** zoals explosieven en grondstoffen. Type bedrijven: technologische centra, ziekenhuizen, chemische centra, apotheken, drogisterijen, tuincentra en bouwmarkten.
- **de toegang tot doelwitten vanuit het bedrijf:**
  - medewerkers van uitzendbureaus, adviesbureaus en onderhoud-, installatie-, schoonmaak-, catering- of beveiligingsbedrijven hebben een goede toegang tot potentiële doelwitten.

### Praktijk: Geen autoverhuur zonder borg

‘Onze klanten komen uit alle windstreken bij ons aan de balie op Schiphol om een auto te huren. Ook uit risicolanden. We zijn ons er terdege van bewust dat de auto’s gebruikt kunnen worden voor terroristische doeleinden. Daarnaast zijn we een Amerikaans bedrijf. Dat maakt ons kwetsbaar. Daarom nemen we veiligheid serieus. Sinds kort verhuren we bijvoorbeeld geen auto’s meer zonder borg. Het bedrag moet per creditcard worden voldaan. Geeft de creditcardmaatschappij geen autorisatie, dan krijgt de klant de auto niet mee. We hebben ook veel geïnvesteerd in geavanceerde apparatuur om rijbewijzen en paspoorten op echtheid te controleren. Maar veiligheid zit hem vooral in details. Elke medewerker van Hertz is hierop getraind. Als iemand bijvoorbeeld in Amsterdam woont en bij onze vestiging in Arnhem een auto wil huren, is dat niet erg logisch en dan vragen we naar de reden hiervan.’

*Henk van den Helder, algemeen directeur van Hertz Autoverhuur Nederland BV*

### 2.3.3 DE KWETSBAARHEID VAN HET BEDRIJF

Terroristen willen natuurlijk een zo groot mogelijke kans van slagen hebben. Of een bedrijf slachtoffer van terrorisme wordt, hangt af van de kwetsbaarheid en weerbaarheid van een bedrijf. Beveiligingsmaatregelen kunnen de kans op succes verminderen. Zulke maatregelen kunnen ertoe bijdragen dat terroristen besluiten een bepaald doelwit niet te kiezen.

27

Een bedrijf is kwetsbaarder als:

- **terroristen makkelijk toegang hebben** in en om het gebouw doordat er weinig of geen beveiligingsmaatregelen zijn;
- **er vaste routines zijn** die terroristen veel houvast geven bij het plannen van activiteiten. Denk aan vaste routes van goederenvervoer of het laden en lossen van goederen op vaste tijdstippen;
- **er veel bezoekers zijn** zodat terroristen makkelijk onopgemerkt op kunnen gaan in de massa.

De kwetsbaarheid van een bedrijf is daarnaast afhankelijk van de weerbaarheid van de bedrijfsprocessen, -systemen en -gebouwen. Bedrijven kunnen veel maatregelen nemen om hun weerbaarheid tegen een dreiging of aanslag te vergroten. Hoofdstuk 5 gaat hierop in.

## **2.4 HERKENNEN VAN CONCRETE DREIGINGEN**

### **2.4.1 VERDACHTE HANDELINGEN, TIJDSTIPPEN EN LOCATIES**

Om signalen voor concrete dreigingen op te merken, is het nodig te weten wat verdachte of ongebruikelijke handelingen en situaties zijn. Dit zijn handelingen en situaties die niet passen in het normale plaatje. Bedrijven die heldere procedures hebben voor orde, netheid en controle en deze naleven, maken het voor zichzelf makkelijker om afwijkingen te constateren. Daarbij moeten bedrijven zich wel realiseren dat voorbereidingen voor terroristische aanslagen, zoals verkenningen van een doelwit, lange tijd in beslag kunnen nemen. Hierdoor is het niet altijd eenvoudig om deze activiteiten op te merken.

28

In deze handreiking geven we een indicatieve maar niet uitputtende lijst met aanwijzingen voor terroristische activiteiten. Het is daarbij belangrijk dat bedrijven deze lijst steeds afzetten tegen de normale situatie en de context in ogenschouw nemen. De kans dat een signaal wijst op iets verdachts is groter als er sprake is van een combinatie van signalen. De elementen van het aantrekkelijkheidsprofiel, zoals het aantal mogelijke slachtoffers en het veroorzaken van grote economische schade, spelen hierbij ook een rol (zie paragraaf 2.3.1). Als elementen van het aantrekkelijkheidsprofiel aanwezig zijn en er doen zich bijzondere omstandigheden voor, vergroot dit de kans dat sprake is van een verdachte situatie. Stel bij mogelijk verdachte situaties de plaatselijke politie op de hoogte.

#### **Signalen kunnen verdacht zijn omdat:**

- de handeling die gesignaleerd is, zelf verdacht is;
- het tijdstip van de handeling verdacht is;
- de locatie waar de handeling plaatsvindt verdacht is.

### Handelingen:

- handelingen die de beveiliging van een bedrijf raken:
  - aandacht en interesse voor de beveiliging;
  - vastleggen van de beveiligingssituatie van een bedrijf: fotograferen, filmen, noteren;
  - diefstal van bedrijfslegitimatiebewijzen, -kleding en -voertuigen;
  - testen van de beveiliging van een bedrijf (bijvoorbeeld door het alarm diverse keren te laten afgaan).
- handelingen waarbij iemand zijn of haar identiteit probeert af te schermen:
  - geen legitimatie bij zich hebben of een vals paspoort of rijbewijs;
  - geen contactgegevens kunnen overleggen zoals een telefoonnummer of een adres van de betreffende persoon;
  - grote bedragen in contanten betalen, met vals geld of met gestolen betaalkaarten.
- (digitale) pogingen om kennis, informatie en goederen te verkrijgen die geschikt zijn voor de voorbereiding van een aanslag:
  - interesse in dergelijke kennis, informatie en goederen;
  - aanschaf en diefstal van dergelijke kennis, informatie en goederen.

29

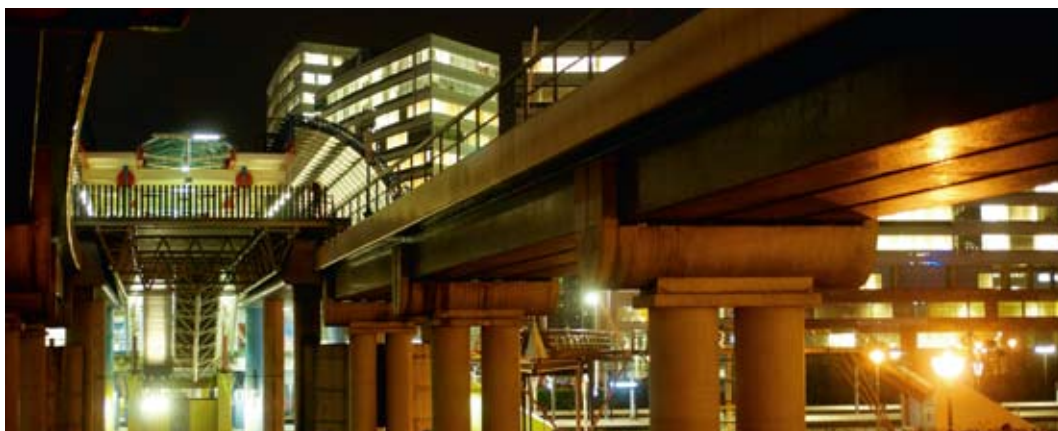
### Tijdstippen:

- incidenten op tijdstippen waarop bedrijfsprocessen stil horen te liggen, zoals na sluitingstijd;
- terugkerende verdachte handelingen: vaak is een verkenning niet eenmalig;
- signalen op tijdstippen vlak nadat de gebruikelijke beveiligingsronde heeft plaatsgevonden (bijvoorbeeld afgaan van alarmen).

### Locaties:

- locaties in de nabijheid of met zicht op potentiële doelwitten;
- locaties die om welke reden dan ook beveiligd zijn. Bijvoorbeeld omdat daar producten of diensten worden geproduceerd die onderdeel zijn van de vitale infrastructuur;
- locaties waar eindcontroles plaatsvinden (een vergiftiging na de eindcontrole in de voedingsmiddelenindustrie wordt bijvoorbeeld niet meer opgemerkt);

- locaties waar zich informatie of middelen bevinden die geschikt of nodig zijn in de voorbereiding van een aanslag.



Bedrijven kunnen voorbereidende handelingen en activiteiten van terroristen ook herkennen aan de hand van zes V's. Dit systeem is minder ruim dan bovenstaande beschrijving aan de hand van 'handelingen', 'tijdstippen' en 'locaties'. Dit zijn de zes V's:

- **Valuta** Vals geld, grote hoeveelheden contant geld of vreemde valuta, ongebruikelijke financiële transacties, fraude met sof-nummers en financiële gegevens;
- **Verblijf** Regelmatige bewonerswisselingen, langdurige afwezigheid van bewoners, frequente in- en uitloop van personen, illegale bewoning, afwijkend gebruik van opslagplaatsen;
- **Voorbereiding** Video's of foto's maken van potentiële doelwitten, samenstellen van plattegronden, observeren van bewakingsprocedures, verdacht ophouden in de nabijheid van potentiële doelwitten;
- **Voorwerpen** Aanwezigheid van plattegronden, bouwtekeningen, navigatiemiddelen, militaire of chemische handboeken, observatiemiddelen, stoffen om explosieven mee te maken, wapens;
- **Vervoer** Auto als observatievoertuig, buitenlands kenteken, een langdurig onbeheerd achtergelaten auto, aankoop van de auto via contante betaling, diefstal van een bedrijfsauto;
- **Valse documenten** Aanwezigheid van paspoorten, rijbewijzen, creditcards, verblijfsvergunningen en veelvuldige aangifte van vermissing van zulke documenten.

### **2.4.2 HERKENNEN VAN RADICALISERING**

Geradicaliseerd personeel kan een toekomstige terroristische dreiging vormen. Namelijk wanneer personeel bereid is steun te verlenen aan terroristische aanslagen of bereid is deze uit te voeren. Het gaat om personen die al vergevorderd zijn in hun radicalisering. Hun aantal is zeer beperkt.

Radicalisering is een proces dat heel snel, maar ook heel geleidelijk kan plaatsvinden. Radicalisering is op zichzelf niet meteen gerelateerd aan een doelwit of een middel. Informatie over geradicaliseerd personeel kan wel leiden tot de ontdekking van activiteiten die mogelijk een relatie hebben met de voorbereiding en uitvoering van terroristische aanslagen. Daarmee kan de politie zicht krijgen op toekomstige concrete dreigingen. Licht de plaatselijke politie in over geradicaliseerd personeel.

Of sprake is van geradicaliseerd personeel hangt af van een combinatie van factoren. Dit zijn enkele signalen voor de aanwezigheid van geradicaliseerd personeel:

- het voorhanden hebben of opzoeken via internet van extremistische literatuur, pamfletten, geluids- en gegevensdragers. Dit kan voor bedrijven lastig te beoordelen zijn, omdat vaak gebruik wordt gemaakt van een andere taal, zoals Arabisch;
- goedkeurende signalen afgeven over terroristische aanslagen;
- reizen naar regio's of landen waar zich een terroristisch conflict afspeelt of waar terroristische trainingskampen zijn. Denk aan Tsjetsjenië, Kasjmir, Irak en Pakistan;
- een plotselinge afkeer hebben van 'westerse gewoonten' zoals gemengde activiteiten (man/vrouw), het drinken van alcohol en het vragen om specifieke islamitische maaltijden;
- het dragen van specifieke kleding en symbolen of een plotselinge verandering van kledingsgedrag.





### **3. WAT KUNNEN BEDRIJVEN VAN DE OVERHEID VERWACHTEN?**

Overheden proberen de kans op terroristische dreigingen en aanslagen te verminderen. Op internationaal, Europees, landelijk en lokaal niveau stellen overheden wet- en regelgeving op, of maken beleid. In dit hoofdstuk komen de overheidsactiviteiten aan de orde, zodat bedrijven weten wat ze van de overheden mogen verwachten als het gaat om terrorismebestrijding.

#### **3.1 LANDELIJK**

##### **3.1.1 DE NATIONAAL COÖRDINATOR TERRORISMEBESTRIJDING (NCTb)**

Op 1 januari 2005 is de Nationaal Coördinator Terrorismebestrijding (NCTb) ingesteld. De NCTb coördineert de terrorismebestrijding. De organisatie valt onder de verantwoordelijkheid van de minister van Justitie - coördinerend minister voor terrorismebestrijding - en de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK). De NCTb probeert de kans op terroristische aanslagen in Nederland te verkleinen en neemt maatregelen om de gevolgen van een eventuele aanslag te beperken.

33

#### **Dit zijn de kerntaken van de NCTb:**

- verwerken van informatie van inlichtingendiensten en bestuurlijke en wetenschappelijke bronnen tot dreigingsanalyses en dreigingsbeelden;
- ontwikkelen van contra-terrorismebeleid;
- regisseren van de samenwerking tussen de partijen die betrokken zijn bij terrorismebestrijding;
- onderhouden en uitvoeren van het Stelsel Bewaken en Beveiligen;
- toezicht houden op de beveiliging van de burgerluchtvaart.

De NCTb bekijkt terroristische dreigingen vanuit drie invalshoeken:

- de algemene dreiging voor Nederland;
- dreiging tegen vitale bedrijfssectoren;
- dreiging tegen een object, dienst of persoon.

Voor elke invalshoek heeft de NCTb een systeem ontwikkeld om tijdig het beleid aan te passen of maatregelen te nemen.

| Drie systemen om met een terroristische dreiging om te gaan |                                                                                                                                                                        |
|-------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Dreigingsbeeld Terrorisme Nederland (DTN)                   | Het DTN geeft een beeld van de potentiële dreiging voor Nederland en is bedoeld om contra-terrorismebeleid te formuleren.                                              |
| Alerteringssysteem Terrorismebestrijding (ATb)              | Dit systeem is gericht op de dreiging voor vitale bedrijfssectoren en vormt de basis voor maatregelen door bedrijfssectoren en overheden.                              |
| Stelsel Bewaken en Beveiligen                               | Dit stelsel is gericht op een dreiging voor een object, dienst of persoon. Op basis van dit stelsel neemt de lokale en/of landelijke overheid beveiligingsmaatregelen. |

34

**3.1.2 HET ALGEMENE DREIGINGSBEELD**

De NCTb stelt minstens elk kwartaal het Dreigingsbeeld Terrorisme Nederland (DTN) op. Dit systeem beschrijft de (inter)nationale terroristische dreiging tegen Nederland op hoofdlijnen en besteedt vooral aandacht aan terroristische fenomenen en ontwikkelingen. Het DTN is gebaseerd op onder meer geheime informatie van inlichtingen- en veiligheidsdiensten en op informatie uit (inter)nationale openbare bronnen. De landelijke overheid gebruikt het DTN om contra-terrorismebeleid te formuleren.

**Kijk voor een samenvatting van het Dreigingsbeeld Terrorisme Nederland (DTN) en het actuele dreigingsniveau op [www.nctb.nl](http://www.nctb.nl)**

Er zijn in Nederland vier dreigingsniveaus: minimaal, beperkt, substantieel en kritiek. Enkele criteria van de niveaus zijn vermeld in Bijlage V. Eind 2006 is de terroristische dreiging

‘substantieel’. Dat betekent dat er een kans is dat in Nederland een aanslag kan plaatsvinden. Dit is onder meer gebaseerd op het beeld dat terroristen hebben van ons land. Deelname aan internationale vredesoperaties en het maatschappelijk debat over de islam kunnen dit beeld beïnvloeden. Binnenlandse radicalisering en de aanwezigheid van netwerken beïnvloeden eveneens de kans op een terroristische aanslag.

Om terroristische dreigingen nauwkeurig in beeld te brengen is informatie van gemeente, politie en bedrijven nodig. Geef daarom signalen van ongebruikelijke handelingen of verdachte objecten door aan de plaatselijke politie.

**3.1.3 DREIGING TEGEN EEN SECTOR**

Het Alerteringssysteem Terrorismebestrijding is een waarschuwingssysteem voor overheden en bedrijven. Het waarschuwt ministeries, provincies en gemeenten, politie, inlichtingen-diensten en de aangesloten bedrijfssectoren als er een verhoogde dreiging is. Overheids-diensten en betrokken bedrijfssectoren kunnen zo snel adequate maatregelen nemen als er een verhoogde dreiging is.

35

| Aangesloten bedrijfssectoren Alerteringssysteem Terrorismebestrijding (eind 2006) |                            |
|-----------------------------------------------------------------------------------|----------------------------|
| 1. Luchthaven Schiphol (wordt uitgebreid met andere luchthavens)                  | 6. Elektriciteitssector    |
| 2. Haven Rotterdam (wordt uitgebreid tot ‘zeehavens’)                             | 7. Nucleaire sector        |
| 3. Drinkwatersector                                                               | 8. Stads- en streekvervoer |
| 4. Spoorsector                                                                    | 9. Financiële sector       |
| 5. Gassector                                                                      |                            |

Het Alerteringssysteem heeft vier niveaus: het basisniveau en een lichte, matige en hoge dreiging. Elk niveau en elke sector heeft zijn eigen maatregelenpakket. Bij het ‘basisniveau’ zijn dit maatregelen die tot de reguliere bedrijfsvoering horen. Hoe hoger het alerterings-niveau, hoe zwaarder en ingrijpender de maatregelen zijn (zie ook bijlage VII).

Bedrijfssectoren kunnen zich aansluiten bij het Alerteringssysteem als ze van vitaal belang zijn voor Nederland en/of een aantrekkelijk doelwit zijn voor terroristen. Eind 2006 zijn negen sectoren aangesloten bij het systeem.

In 2007 wordt dit aantal vermoedelijk uitgebreid met de oliesector, chemische sector, internationale hotels en grote publieksevenementen. De alerteringsniveaus van de aangesloten bedrijfssectoren staan vermeld op [www.nctb.nl/alartering](http://www.nctb.nl/alartering)

**Deze organisaties worden op de hoogte gesteld als het alertingsniveau is verhoogd of verlaagd:**

- de betrokken bedrijfssector;
- de politie;
- het openbaar ministerie;
- de gemeente waarop de dreiging betrekking heeft.

De minister van Justitie besluit in overleg met de minister van Binnenlandse Zaken en Koninkrijkrelaties (BZK) over de verhoging of verlaging van het alerteringsniveau. Hij doet dit op basis van een dreigingsanalyse die de NCTb opstelt. Voordat de minister een besluit neemt vindt overleg plaats met de meest relevante partijen. In ieder geval met de politie en de bedrijfssector. Zij formuleren samen met de NCTb een advies over de maatregelen die een bedrijf kan nemen. De bedrijven voeren de maatregelen vrijwillig uit en betalen de kosten ervan. Het lokale bestuur is grotendeels verantwoordelijk voor de uitvoering van de overheidsmaatregelen. Maatregelen die aangesloten sectoren bij een verhoogde dreiging nemen, kunnen merkbaar zijn voor niet aangesloten bedrijven en het publiek.

**Lichte dreiging op het spoor**

Op 9 september 2005 werd het alerteringsniveau voor de spoorsector verhoogd naar een 'lichte dreiging'. Er kwam meer toezicht op stations. Het personeel werd - onder meer per sms - gevraagd alert te zijn op verdachte gebeurtenissen en handelingen. Treinreizigers werden opgeroepen hun bagage niet onbeheerd achter te laten. De politie surveilleerde extra op en rond diverse treinstations.

### **3.1.4 BESCHERMING VITALE INFRASTRUCTUUR**

Het kabinet wil de vitale infrastructuur beschermen. Het ministerie van Binnenlandse Zaken en Koninkrijkrelaties (BZK) werkt hiervoor samen met onder meer de NCTb, de Algemene Inlichtingen- en Veiligheidsdienst (AIVD), een groot aantal ministeries, lokale overheden en bedrijven. De aanpak bij de vitale sectoren verschilt met het Alerteringssysteem Terrorismebestrijding. Het Alerteringssysteem is bedoeld om de weerbaarheid van de bedrijfssectoren tegen terrorisme tijdelijk te verhogen naar aanleiding van een specifieke dreiging. Het project Bescherming Vitale Infrastructuur is een middel om het (basis)niveau van beveiliging van vitale bedrijven structureel te verhogen. Het project richt zich op uitval van vitale infrastructuur veroorzaakt door onder andere criminaliteit en terrorisme, maar ook door natuurrampen en technisch of menselijk falen.



37

Producten, diensten en processen behoren tot de vitale infrastructuur als ze bij uitval grootschalige maatschappelijke ontwrichting kunnen veroorzaken. Dat is bijvoorbeeld het geval bij een grote economische schade en als herstel lang duurt of als er geen alternatieven voorhanden zijn terwijl de samenleving het product of de dienst niet kan missen. Zeventig procent van de vitale infrastructuur is in handen van bedrijven.

**Doel van het project Bescherming Vitale Infrastructuur is:**

- zoveel mogelijk voorkomen van grootschalige uitval of verstoring van de vitale infrastructuur;
- een adequate voorbereiding van overheid en bedrijven op de gevolgen van uitval en verstoring;
- effectieve maatregelen nemen om de schade zoveel mogelijk te beperken.

De vitale infrastructuur in Nederland omvat twaalf sectoren, die 33 vitale producten, diensten en processen omvatten. Voorbeelden van vitale producten, diensten en processen zijn: elektriciteit, aardgas, olie, telecommunicatie, drinkwatervoorziening, betalingsdiensten, beheer van oppervlaktewater, rechtshandhaving, informatieverstrekking van overheid, voedselvoorziening, vervoer, opslag en productie/verwerking van chemische en nucleaire stoffen.

| Sectoren vitale infrastructuur     |                                          |
|------------------------------------|------------------------------------------|
| 1. Energie                         | 7. Financiën                             |
| 2. Telecommunicatie                | 8. Keren en beheren van oppervlaktewater |
| 3. Voedsel                         | 9. Drinkwater                            |
| 4. Gezondheidszorg                 | 10. Rechtsorde                           |
| 5. Chemische / nucleaire industrie | 11. Openbaar bestuur                     |
| 6. Transport                       | 12. Openbare Orde en Veiligheid          |

Overheid en bedrijven verankeren de maatregelen uit het project Bescherming Vitale Infrastructuur in de reguliere bedrijfsvoering. Voor elke sector is een risicoanalyse opgesteld. Dit geeft inzicht in de risico's die bedrijven lopen en hoe kwetsbaar zij zijn, welke risico's acceptabel zijn en tegen welke risico's maatregelen nodig zijn. Het meest betrokken ministerie bij een bepaalde sector voert deze analyses samen met de bedrijfssector uit. De AIVD levert onder bepaalde voorwaarden veelal informatie over dreigingen en ondersteunt op deze wijze de uitvoering van risicoanalyses.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) stelt samen met de vitale bedrijfssectoren, diverse ministeries, de AIVD, de NCTb en de politie in Nederland een Nationaal Adviescentrum Vitale Infrastructuur (NAVI) in. Dit adviescentrum gaat een bijdrage leveren aan de bescherming van de vitale infrastructuur op basis van vragen en verzoeken vanuit de aangesloten vitale bedrijfssectoren. Het NAVI moet de informatie-uitwisseling op het terrein van beveiliging tussen overheden en bedrijven bevorderen. Ook kan het adviescentrum expertise en kennis over maatregelen en best practices bundelen. Kijk voor actuele informatie over het NAVI en de taken van deze organisatie op [www.veiligheid.minbzk.nl](http://www.veiligheid.minbzk.nl)

### **3.1.5 ANDERE ACTIVITEITEN**

De landelijke overheid doet veel om de kans op terroristische dreigingen te verkleinen. Ook voor bedrijven die niet zijn aangesloten bij het Alerteringssysteem of het project Bescherming Vitale Infrastructuur. Het is niet mogelijk om alle activiteiten in deze handreiking te noemen, maar hieronder worden er nog een paar uitgelicht.

#### **Bewustzijn bevorderen**

In 2006 startte de NCTb een traject om het bewustzijn bij alle bedrijven over terroristische dreigingen te bevorderen. Samen met onder meer VNO-NCW, MKB-Nederland, het Nederlands Politie Instituut (NPI), de AIVD en de Kamer van Koophandel Nederland, wil de NCTb de kennis van bedrijven over terroristische dreigingen vergroten. Deze handreiking én een brochure voor bedrijven zijn eerste producten. Daarnaast is de website [www.nederlandtegenterrorisme.nl](http://www.nederlandtegenterrorisme.nl) voorzien van informatie voor bedrijven.

Ook informeren VNO-NCW, MKB-Nederland en allerlei brancheorganisaties hun leden door middel van nieuwsberichten, artikelen en bijeenkomsten over wat bedrijven kunnen doen om de kans op terroristische dreiging te verminderen. De activiteiten binnen dit traject stimuleren bedrijven na te denken over de wijze waarop zij terrorismebestrijding kunnen inpassen in hun reguliere veiligheidsbeleid.

Daarnaast willen de landelijke overheid en bedrijven elkaar beter informeren over concrete dreigingen en de maatregelen die zij daartegen treffen. Zij praten nog met elkaar over de wijze waarop zij dat gaan doen.

Zie voor actuele informatie [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)

### **CBRN-terrorisme**

De NCTb besteedt met andere ministeries ook aandacht aan de dreiging van CBRN-terrorisme. Dit zijn aanslagen met chemische, biologische, radiologische en nucleaire wapens. De NCTb en de ministeries inventariseerden een beperkt aantal bedrijven dat beschikt over grote voorraden middelen die als grondstof kunnen dienen voor CBRN-wapens. De landelijke overheid maakt met deze bedrijven afspraken over maatregelen die ze kunnen nemen om hun weerbaarheid te verhogen. Op deze manier verkleinen de bedrijven de kans om gebruikt te worden als doelwit of als middel voor een terroristische aanslag.

### **Verzekering voor Terrorismeschade**

In 2003 hebben de landelijke overheid, het Verbond van Verzekeraars en de Pensioen- en Verzekeringskamer de Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden N.V. opgericht (NHT). Via deze organisatie kunnen verzekeraars de schade van bedrijven als gevolg van terrorisme tot een maximumbedrag van één miljard euro per jaar vergoeden. Zonder het NHT zouden verzekeraars over onvoldoende verantwoorde dekking beschikken voor deze schadeclaims. Vergoeding kan alleen als dekking voor terrorisme in de polis van het bedrijf is opgenomen. Meer informatie over de NHT is te vinden via [www.terrorismeverzeker.nl](http://www.terrorismeverzeker.nl)

### **3.2 LOKAAL**

Op lokaal niveau werken politie en gemeenten samen om de veiligheid te vergroten. Daaronder valt ook terrorismebestrijding. De gemeente is in eerste instantie verantwoordelijk voor het lokale veiligheidsbeleid. De politie is het eerste aanspreekpunt voor bedrijven bij een terroristische dreiging of bij verdachte of ongebruikelijke handelingen.



De gemeente bekijkt terrorismebestrijding doorgaans vanuit het perspectief van het brede veiligheids- en crisisbeheersingsbeleid. Terrorismebestrijding valt daardoor vaak onder de ambtenaar Openbare Orde en Veiligheid of de ambtenaar Rampenbestrijding. Ook kunnen bedrijven te maken krijgen met de ambtenaar verantwoordelijk voor Economische Zaken, bijvoorbeeld als bedrijven op een bedrijventerrein of in een winkelcentrum gezamenlijk de veiligheid willen verbeteren.

Bedrijven hebben met de politie te maken als er een concrete dreiging is. Een aantal politieregio's, zoals Amsterdam-Amstelland en Kennemerland, overlegt met bedrijven over structurele preventieve maatregelen rond terrorismebestrijding. Voor risicoanalyses en individueel advies zal de politie bedrijven meestal doorwijzen naar particuliere beveiligingsbedrijven (zie ook hoofdstuk 5).

#### **Praktijk: korps regiopolitie Kennemerland**

Het korps regiopolitie Kennemerland inventariseerde samen met het staalbedrijf Corus de kans op een terroristische dreiging of aanslag. De weerbaarheid van Corus werd in beeld gebracht en er werden afspraken gemaakt over maatregelen bij een bepaalde dreiging. Deze aanpak komt grotendeels overeen met die van het Alerteringssysteem Terrorismebestrijding.

Het korps regiopolitie Kennemerland realiseerde zich dat er in de regio meer bedrijven doelwit of middel kunnen zijn voor terroristen. Daarom organiseerde de politie in juni 2006 een conferentie voor bedrijven en lokale autoriteiten om de bewustwording over risico's te versterken. Ook stelde de politie een contactpunt in bij het veiligheidsbureau Kennemerland die bedrijven op weg helpt als ze vragen hebben over terrorismebestrijding. Het veiligheidsbureau zet bovendien een platform op voor bedrijven waarin best practices uitgewisseld kunnen worden.

### **3.2.1 DREIGING TEGEN PERSONEN, OBJECTEN OF DIENSTEN**

Elke Nederlander is verantwoordelijk voor de veiligheid van zijn eigen persoon en goederen. Zo moet iedereen zelf zorgen voor goede inbraakbeveiliging. Ook bedrijven zijn zelf verantwoordelijk voor de beveiliging van hun terrein, gebouw en werknemers. Soms is de dreiging zo groot dat personen, organisaties of bedrijven hier geen weerstand tegen kunnen bieden. Dan kan de (lokale) overheid voor maatregelen zorgen. Deze maatregelen hebben vrijwel altijd betrekking op het publieke domein. Bedrijven blijven verantwoordelijk voor de interne beveiliging van het bedrijf.

Bij een terroristische dreiging moeten personen, organisaties en bedrijven altijd contact opnemen met de plaatselijke politie voor een melding of een aangifte. Deze wettelijke verplichting is er niet voor niets. Want zonder aangifte kan de politie de concrete dreiging niet goed inschatten. Bovendien kan de politie deze informatie gebruiken om een beeld te krijgen van de algemene dreiging in Nederland.

42

De afdeling Conflict- en Crisisbeheersing van de plaatselijke politie beoordeelt de concrete dreiging en gebruikt eventueel informatie van inlichtingendiensten. Bedrijven die bij de plaatselijke politie melding of aangifte doen van dreiging tegen hun bedrijf, tegen hun medewerkers of van ongebruikelijke handelingen of verdachte objecten, krijgen in eerste instantie met een politiefunctionaris te maken die de melding of aangifte opneemt. Daarna volgt waarschijnlijk contact met de politiefunctionaris die zich bezighoudt met conflict- en crisisbeheersing. Hij behandelt de dreigingsmeldingen en informeert andere lokale autoriteiten, zoals de burgemeester of de (hoofd)officier van justitie. Meldingen van dreigingen kunnen ook via andere kanalen binnen komen, zoals de landelijke overheid.

Op basis van de informatie van de afdeling Conflict- en Crisisbeheersing wegen de burgemeester, de (hoofd)officier van justitie en de korpschef - die gezamenlijk de zogenoemde driehoek vormen - de ernst en waarschijnlijkheid van de dreiging. De driehoek bepaalt of en welke beveiligingsmaatregelen van de zijde van de overheid nodig zijn. Hoe

ernstiger en waarschijnlijker een dreiging is, hoe zwaarder het maatregelenpakket. De politie voert de beveiligingmaatregelen uit.



#### **Praktijk: uitgever en spraakmakende columnist**

Een uitgeverij vraagt een spraakmakende columnist dagelijks een prikkelende column voor zijn krant te schrijven. Na enige tijd ontvangt de krant negatieve reacties op de columns. De uitgever besluit - na overleg met een beveiligingsbedrijf - zijn alarminstallatie en hang- en sluitwerk te verbeteren. Hij vraagt de columnist ook zelf goed op te passen. Als er ernstige doodsbedreigingen aan het adres van de columnist volgen, doet de uitgever aangifte bij de politie. De politie vindt de situatie zo ernstig dat zij de schrijver een direct noodtelefoonnummer geeft, waarmee hij in het geval van dreigende situaties direct contact met de politie kan opnemen.

43

De lokale autoriteiten onderhouden het contact met de bedreigde persoon, instelling of bedrijf over de genomen beveiligingsmaatregelen. De plaatselijke politie voert deze maatregelen uit en kan daarbij gebruikmaken van faciliteiten van de landelijke overheid. Zo kan de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) van het Korps Landelijke

Politiediensten (KLPD) worden gevraagd om persoonsbeveiliging. Daarnaast nemen bedrijven ook zelf maatregelen en stellen de politie daarvan in kennis. Bedrijven kunnen bij een (particuliere) veiligheidsadviseur advies inwinnen over maatregelen die passen bij de aard van het bedrijf of navraag doen bij hun brancheorganisatie (zie ook hoofdstuk 5).

#### **Praktijk: evenement met politici**

Een directeur van een conferentieoord besluit om het veertigjarig bestaan van zijn organisatie te vieren met een debat tussen politici. Hij moet daarvoor de catering, de audiovisuele middelen en het personeel regelen. Ook is hij verantwoordelijk voor de beveiliging van het festijn. De directeur huurt een adviseur in om de beveiliging van de locatie door te lichten en meldt de komst van de speciale gasten bij de plaatselijke politie. De politie beoordeelt de dreiging en zorgt voor twee geüniformeerde agenten bij de ingang van het terrein. De organisator zorgt zelf voor een goede toegangscontrole.

44

Voor sommige personen, objecten en diensten die een bijzondere functie hebben in onze democratische rechtsorde heeft de landelijke overheid een specifieke verantwoordelijkheid. Denk aan leden van het Koninklijk Huis, politici, buitenlandse staatshoofden en ambassadeurs en hun woon- en werkvertrekken. Bedrijven die een evenement organiseren en deze personen bevestigen daarbij aanwezig te zijn, informeren de plaatselijke politie. Die neemt vervolgens contact op met de Coördinator Bewaking en Beveiliging (CBB) van de NCTb om passende maatregelen te treffen. Bedrijven hoeven dus zelf niet contact op te nemen met de NCTb.

### **3.3 INTERNATIONAAL EN EUROPEES**

Veel bedrijven hebben te maken met internationale of Europese regelgeving over terrorisme en/of beveiliging. Deze regelgeving is volop in beweging. Zo ontwikkelt de Europese Unie (EU) een 'European Programme for Critical Infrastructure Protection' (EPCIP). Dit programma omvat de bescherming van Europese vitale infrastructuur met grensoverschrijdende effecten. Naar verwachting treedt het EPCIP in 2007 in werking.

Kijk voor actuele informatie op [www.ec.europa.eu/justice\\_home/funding/epcip](http://www.ec.europa.eu/justice_home/funding/epcip)

Mede door de vele ontwikkelingen op het gebied van logistiek, verkeer, water en luchtvaart besloten bedrijven, de landelijke overheid en kennisinstellingen samen te werken in het Transumo-project 'Protect'. Doel is te kijken hoe bedrijven en de landelijke overheid internationale goederenstromen veiliger kunnen maken.

Zie voor meer informatie [www.protect.transumo.nl](http://www.protect.transumo.nl)

### **3.3.1 VEILIGHEID VAN DE HAVEN EN DE LUCHTVAART**

In 2002 stelde de Internationale Maritieme Organisatie (IMO) een internationale norm op om zeeschepen en havens beter te beveiligen: de International Ship & Port facility Security Code. Deze ISPS-code bestaat uit een kwaliteitszorgsysteem, waarin taken en verantwoordelijkheden zijn vastgelegd en maatregelen worden voorgeschreven om de kans op veiligheidsincidenten, zoals terrorisme, te verkleinen. De ISPS-Code verscherpt de controle op de toegang tot havenfaciliteiten en grote schepen. Alle bedrijven kunnen hiermee te maken krijgen. De burgemeester van de gemeente waarin de haven is gelegen, is de bevoegde autoriteit voor de havenbeveiliging. Hij laat beveiligingsplannen beoordelen en geeft certificaten af. Zonder geldig certificaat mag een bedrijf geen internationale schepen ontvangen.

45

De EU heeft de ISPS-code omgezet in verordening 725/2004. Nederland heeft deze verordening opgenomen in de Havenbeveiligingswet. De nieuwe EU-richtlijn 2005/65/EG, die op 15 juni 2007 van kracht wordt, breidt de beveiliging uit met vitale activiteiten en infrastructuur die belangrijk zijn voor de veiligheid van de hele haven. Het veiligheidsregime van de Havenbeveiligingswet sluit naadloos aan op de alerteringsniveaus van de sector 'zeehavens' van het Alerteringssysteem Terrorismebestrijding. Het ministerie van Verkeer en Waterstaat heeft enkele brochures opgesteld over de Havenbeveiligingswet (zie Bijlage IV).

Voor het opstellen van veiligheidsplannen is ook een toolkit ontworpen. Deze toolkit en informatie over de ISPS-Code is te vinden op [www.portsecuritytoolkit.com](http://www.portsecuritytoolkit.com)

De regelgeving om havens te beveiligen komt overeen met de regels om de luchtvaart tegen terroristische aanslagen te beschermen. Informatie over de Europese en landelijke regels is te vinden op [www.ec.europa.eu/transport/air\\_portal](http://www.ec.europa.eu/transport/air_portal) en [www.nctb.nl](http://www.nctb.nl)

### **3.3.2 KETENBEVEILIGING**

Internationaal is er veel aandacht voor de ketenbeveiliging. Daarmee bedoelen we dat elke schakel in een keten de veiligheid moet kunnen garanderen tegenover de andere schakels. De vervoersketen is hier een voorbeeld van.

Binnen de ketenbeveiliging is ook aandacht voor terroristische dreiging. Verschillende organisaties ondernemen initiatieven. Zo heeft de World Customs Organization (WCO) in 2006 het 'Framework of Standards' uitgebreid met veiligheid. Daarin beïnvloeden veiligheidsmaatregelen de reguliere douanehandelingen. Vrijwillige deelname van bedrijven hieraan kan een beperktere - en dus snellere - douanecontrole opleveren.

46

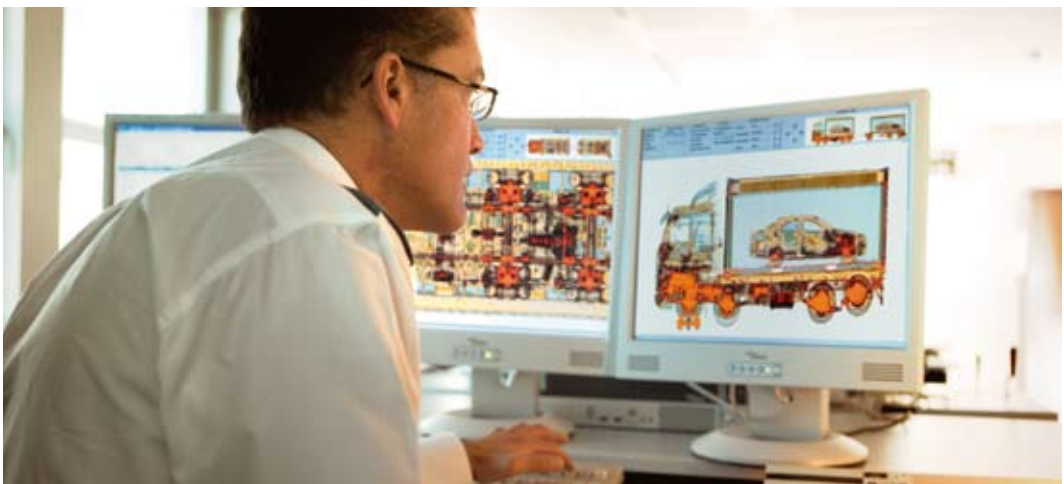
De EU heeft een verordening aan de lidstaten voorgesteld om de beveiliging van de bevoorradingketens te verbeteren en het Europese goederenvervoer beter tegen mogelijke terroristische aanslagen te beschermen. Deze conceptverordening moet het verschil tussen de beveiliging van schepen, havens en de luchtvaart én andere vervoersmodaliteiten opheffen. De bevoorradingketen omvat alle vervoershandelingen en de daarmee verbonden handelingen en processen vanaf de productielocatie tot op de plaats van bestemming van de goederen. Bedrijven die - vrijwillig - voldoen aan eisen rond fysieke veiligheid, toegangscontrole, veilige procedures, veiligheid voor het personeel, registratieprocedures, informatiebeveiliging en opleiding en bewustmaking, kunnen erkend worden als 'veilige exploitant'. Deze erkenning kan in de toekomst praktische voordelen bij veiligheidscontroles zoals douanecontroles opleveren. Voor meer informatie zie [www.ec.europa.eu/transport](http://www.ec.europa.eu/transport) of [www.eur-lex.europa.eu/nl](http://www.eur-lex.europa.eu/nl)

### **De ketenverordening van de EU richt zich op vier groepen logistieke activiteiten:**

- verzendingsklaar maken van goederen en verzending van goederen vanaf de productielocatie;
- vervoer van goederen;
- distributie van goederen;
- overslag en opslag van goederen.

Parallel aan de ontwikkeling van de verordening voor de beveiliging van de bevoorradingsketen moeten alle EU-lidstaten per 1 januari 2008 het beginsel van 'geautoriseerde marktdeelnemer' (Authorised Economic Operator, AEO) in de douanewetgeving invoeren. De bedoeling is om een onderscheid te maken tussen bedrijven die investeren in beveiliging en bedrijven die dat niet doen. Het gaat bijvoorbeeld om maatregelen ter beveiliging van de automatisering en gebouwen. Een bedrijf dat deze investeringen maakt, krijgt de status van 'geautoriseerde marktdeelnemer'. Hij moet daarvoor een vergunning bij de douane aanvragen. Bedrijven met zo'n status hoeven minder informatie aan te leveren bij de douane. Ook zullen zij waarschijnlijk minder controles aan de buitengrens moeten ondergaan. Daarnaast moeten bedrijven vanaf 2009 voorafgaand aan invoer en uitvoer van goederen informatie aanleveren aan de douane. De douane kan dan een goede risicoanalyse uitvoeren. Voor meer informatie zie [www.ec.europa.eu/taxation\\_customs](http://www.ec.europa.eu/taxation_customs), [www.eur-lex.europa.eu/nl](http://www.eur-lex.europa.eu/nl) en [www.minfin.nl](http://www.minfin.nl)

47



Deze ontwikkelingen vragen om een nadere invulling van risicomanagementsystemen voor veiligheid. De International Organization for Standardization (ISO) ontwikkelde ISO 28000 om onderwerpen rond de veiligheidsprocedure te inventariseren. Binnenkort fungeert ISO 28001 als standaardnorm voor een risicoanalysemethodiek. Daarnaast laat de European Committee for Standardization (CEN) een onderzoek uitvoeren naar de noodzaak van aanvullende Europese normen. Actuele informatie is te vinden op: [www.iso.org](http://www.iso.org) en [www.ec.europa.eu](http://www.ec.europa.eu)

Ook buitenlandse bedrijven of overheden stellen diverse managementsystemen voor veiligheid op. Voorbeelden hiervan zijn TAPA (Technology Asset Protection Association) en C-TPAT (Customs Trade Partnership Against Terrorism). Kijk voor meer informatie op [www.cbp.gov](http://www.cbp.gov)



### **3.4 WAAR KUNNEN BEDRIJVEN TERECHT?**

Bedrijven kunnen over informatie beschikken die mogelijk interessant is voor de landelijke en lokale overheid. Daarnaast ontvangt bedrijven graag overheidsinformatie over potentiële en concrete dreigingen en willen bedrijven weten bij wie zij terecht kunnen voor adviezen over de beveiliging van hun bedrijf.



## **Informatie over beveiligingsmaatregelen**

De politie kan bedrijven doorgaans van algemeen beveiligingsadvies voorzien. De verschillende regiokorpsen hebben hier geen vast aanspreekpunt voor. Soms is dit de buurtregisseur. Het veiligheidsbureau Kennemerland heeft het anders geregeld met een contactpunt voor bedrijven. Voor meer specialistische kennis kunt u terecht bij particuliere beveiligingsadviesbureaus. Deze bureaus kunnen bedrijven ook helpen bij het prioriteren van beveiligingsmaatregelen op basis van de meest risicovolle bedrijfsonderdelen en -processen. Er zijn veel beveiligingsadviesbureaus. Het overgrote deel is aangesloten bij een brancheorganisatie. In 2006 heeft de Vpb (Vereniging van Particuliere Beveiligingsorganisaties) een keurmerk geïntroduceerd, dat ook beschikbaar is voor niet-leden. Het Keurmerk stelt eisen aan de organisatie, kwaliteits- en middelenbeheer, integriteitsbeleid en dienstverlening. Er worden geen eisen gesteld aan de kwaliteit van de producten.

Via de website [www.vvbo.nl](http://www.vvbo.nl) kunt u informatie over brancheorganisaties van beveiligingsadviesbureaus en hun leden verkrijgen.

Daarnaast is informatie over veilig ondernemen onder meer beschikbaar op de sites van de Kamer van Koophandel ([www.kvk.nl/veiligondernemen](http://www.kvk.nl/veiligondernemen)) en het CCV (Centrum voor Criminaliteitspreventie en Veiligheid, [www.hetccv.nl](http://www.hetccv.nl)). Ook kunnen bedrijven contact opnemen met hun eigen branche- of ondernemersorganisatie.

49

## **Signalen doorgeven**

Het is verstandig altijd incidenten en ongebruikelijke handelingen en objecten te registreren. Aan de hand van ervaringen kunnen bedrijven maatregelen nemen of aanscherpen. Informeer de plaatselijke politie over dreigingen van het bedrijf en de medewerkers en verdachte handelingen en objecten. Op basis van deze signalen kan de politie de concrete dreiging beoordelen en zonodig actie ondernemen. De signalen die het bedrijf doorgeeft verbeteren ook de informatiepositie van de landelijke en lokale overheid, omdat de informatie bijdraagt aan een accuraat beeld van de algemene terroristische dreiging. Mocht een bedrijf signalen anoniem willen doorgeven, dan kan contact worden opgenomen met Meld Misdaad Anoniem (0800-7000).

Het delen van informatie is geen éénrichtingsverkeer. Een bedrijf wil ook goed op de hoogte zijn van dreigingen in het algemeen en voor het bedrijf. Naast deze handreiking is algemene informatie ook te vinden op [www.nctb.nl](http://www.nctb.nl) en [www.aivd.nl](http://www.aivd.nl)

Specifieke informatie rond dreigingen voor een bedrijf ontvangt dat bedrijf van de lokale autoriteiten zodra daarvoor aanleiding is. Bestaande contacten met de plaatselijke politie bevorderen een snelle informatie-uitwisseling. Zorg ervoor dat de politie op de hoogte is bij wie ze terecht kan.

Veel bedrijven willen ook weten wat de lokale autoriteiten hebben gedaan met hun signalen. Dat is niet altijd mogelijk. Een belangrijke reden daarvoor is dat actie vaak pas mogelijk is als verschillende stukjes informatie bij elkaar worden gelegd.

#### **Praktijk: Griffin Project van de City of London Police**

De City of London Police informeert wekelijks bedrijven over (terroristische) dreigingen, ontwikkelingen rond criminaliteit en komende evenementen of manifestaties. Bij het Project Griffin zijn Londense bedrijven aangesloten. Meer specifiek gaat het om de beveiligingscoördinatoren, eventueel van particuliere beveiligingsbedrijven.

Het project Griffin omvat drie elementen:

- training voor beveiligingscoördinatoren en -mensen over (terroristische) dreiging, methodieken en middelen en de bijdrage van beveiligingscoördinatoren en -mensen bij een (terroristische) dreiging of aanslag;
- bridge call: elke vrijdag licht de politie de bedrijven in over de stand van zaken en ontwikkelingen. Dit gebeurt via een conference call. Deze informatie bevat dreigingsinformatie;
- de inzet van beveiligingsmensen naast politiemensen tijdens incidenten en aanslagen.

Het traject dat de NCTb is gestart met partners rond terrorismebestrijding en bedrijven besteedt ook aandacht aan verbetering van de wederzijdse informatievoorziening. Een belangrijke vraag daarbij is hoe overheden en bedrijven informatie en kennis kunnen delen. Het is niet eenvoudig om kennis en informatie te ontsluiten, omdat het om informatie gaat die niet op straat mag komen te liggen. Daarnaast is het ook niet de bedoeling om bedrijven onnodig ongerust te maken. De NCTb en partners onderzoeken aan de hand van buitenlandse voorbeelden hoe zij het delen van informatie tussen overheden en bedrijven kunnen verbeteren. De bedoeling is om deze uitwisseling zoveel mogelijk via bestaande overlegstructuren te laten verlopen.

#### **Praktijk: Operation NEXUS (Verenigde Staten)**

De New York Police Department zette Operation NEXUS op om opvallende, niet alledaagse handelingen te signaleren die mogelijk op terrorisme duiden.

De politie instrueerde ongeveer 70 bedrijfssectoren om bepaalde verdachte of ongebruikelijke handelingen en situaties te signaleren en door te geven. Elke bedrijfssector kreeg zijn eigen instructies. Hotels, maar ook duikscholen, ziekenhuizen, musea, restaurants, theaters, juweliers, drogisterijen en scholen doen mee. De politie beslist op basis van de signalen die zij krijgt of actie nodig is.

Een drogisterij kan bijvoorbeeld contact opnemen met de politie als een kale man liters waterstofperoxide 'inslaat'. Ook stomerijen doen mee. Als u in de Verenigde Staten een jasje naar de stomerij brengt, is de kans groot dat u het colbert terug krijgt met de sticker 'Member of Operation NEXUS' erop.



## **4. RISICOMANAGEMENT**

### **4.1 METHODIEK RISICOANALYSE**

Mensen en organisaties zijn voortdurend bezig dagelijkse risico's te beheersen. Vaak gebeurt dat intuïtief, zonder een expliciete aanpak of methodiek. Maar er zijn ook bedrijfssectoren en vakgebieden die gespecialiseerd zijn in het analyseren en managen van risico's. Een voorbeeld hiervan is de financiële sector, die zich bezighoudt met het beperken van risico's rond investeringen, verzekeringen en beleggingen. En de chemische industrie doet dat met ongevalrisico's.

Een ander soort risicomanagement is het beperken van risico's die kwaadwillende personen, zoals terroristen, bewust veroorzaken. Hiervoor zijn specifieke risicoanalysemethoden ontwikkeld. Ze bestaan meestal uit een combinatie van een afhankelijkheidsanalyse, een dreigingsanalyse en een kwetsbaarheidsanalyse.

53

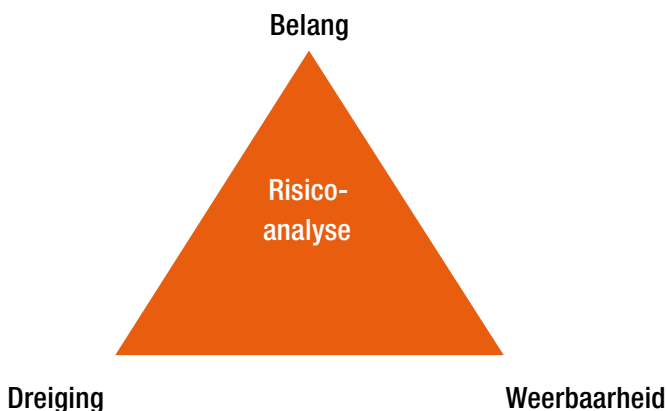
**In de afhankelijkheidsanalyse** staan de kroonjuwelen van het bedrijf centraal: vitale bedrijfsprocessen en cruciale onderdelen van het bedrijf. Deze belangen en afhankelijkheden moeten beschermd worden om ernstige bedrijfseconomische of maatschappelijke schade te voorkomen.

**In de dreigingsanalyse** worden kwaadwillende personen en hun activiteiten onderzocht. Hier staat de kans op de dreiging centraal. In dit geval: de terroristische dreiging.

**In de kwetsbaarheidsanalyse** gaat het om de weerbaarheid van een bedrijf. Als deze tekortschiet kan het bedrijf kwetsbaar zijn voor terroristische aanslagen.

**In de risicoanalyse** worden de cruciale belangen en afhankelijkheden, de kans op dreigingen en de weerbaarheid van een bedrijf aan elkaar gerelateerd. Dat levert een beeld op van de risico's van een bedrijf.

Om een goede risicoanalyse uit te voeren is kennis en informatie nodig over het bedrijf, over concrete en potentiële dreigingen én over maatregelen die de weerbaarheid van een bedrijf verhogen. Doel van een risicoanalyse is om in te spelen op ernstige risico's van nu en in de nabije toekomst.



Figuur 1: Onderdelen van een risicoanalyse

54

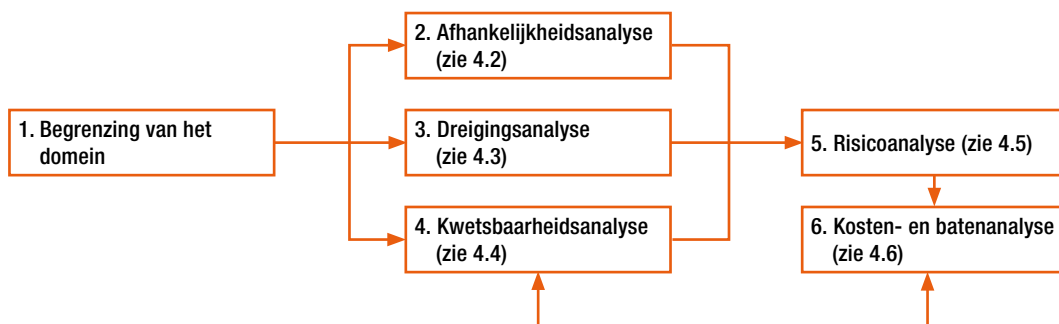
Verschillende organisaties, commerciële instellingen of adviesbureaus hanteren diverse methoden om risicoanalyses op te stellen. Ook zijn er risicoanalysemethoden die specifiek bedoeld zijn om beveiligingsmaatregelen te evalueren. In deze handreiking spreken we geen voorkeur uit voor één van deze methodieken. We geven slechts aan uit welke elementen een risicoanalyse hoort te bestaan.

Een risicoanalyse kan op verschillende manieren worden uitgevoerd. Het is mogelijk om een adviesbureau in te schakelen voor een gedegen analyse. Dit is aan te bevelen voor bedrijven die menen dat ze veel risico lopen of voor grotere bedrijven. Ook is het mogelijk met een aantal gelijksoortige bedrijven een gezamenlijke analyse uit te voeren.

Hoe dan ook, het is belangrijk om in ieder geval een beproefde methodiek te hanteren en deskundigen te betrekken bij de verschillende onderdelen van de analyse. Voor kleinere bedrijven is het misschien niet mogelijk een analyse op te laten stellen door een extern bureau.

Het volgende schema kan (dan) helpen bij de uitvoering van een minder omvangrijke

risicoanalyse. Het illustreert een cyclus voor risicomanagement. Aan de hand van zes stappen kunnen de risico's van een bedrijf worden gerangschikt en benoemd. Dit vormt de basis voor (aanvullende) maatregelen om risico's te verminderen.



Figuur 2: Proces risicoanalyse

## **4.2 AFHANKELIJKHEIDSANALYSE**

De afhankelijkheidsanalyse biedt zicht op de belangen van bedrijven. Denk aan mensen, bedrijfsprocessen, cruciale bedrijfselementen, grondstoffen, objecten of locaties. Het gaat om belangrijke waarden die kunnen worden aangetast en waarvan een bedrijf afhankelijk is.

55

Hieronder volgen een paar invalshoeken om de belangen en de afhankelijkheden van bedrijven te verhelderen:

- **mensen en hun veiligheid** zijn natuurlijk van het grootste belang voor iedere organisatie. Elk bedrijf moet de fysieke veiligheid van mensen kunnen waarborgen;
- **informatie** kan uniek, kostbaar, imagogevoelig, vertrouwelijk of cruciaal zijn voor de continuïteit of concurrentiepositie van een bedrijf. De beschikbaarheid, vertrouwelijkheid of de integriteit van de informatie moet dan ook worden veiliggesteld;
- **bedrijfsprocessen** zijn vaak cruciaal voor de continuïteit of concurrentiepositie van een bedrijf. Deze processen mogen niet of zo min mogelijk worden verstoord;
- **grondstoffen, productiemiddelen, producten en diensten** kunnen kostbaar en aantrekkelijk zijn voor kwaadwillenden. Het is dan ook belangrijk om de beschikbaarheid en integriteit hiervan te waarborgen.

Een goede afhankelijkheidsanalyse geeft inzicht in de belangen die het bedrijf onderkent en de omvang ervan. Ook geeft de analyse aan waarvan die belangen afhankelijk zijn. Zo kan bepaalde informatie cruciaal voor een bedrijf zijn. Om deze informatie te beschermen is het bedrijf afhankelijk van een betrouwbaar computersysteem. Mede op basis van de afhankelijkheidsanalyse krijgen bedrijven inzicht in de aard en omvang van de schade die een ernstig incident kan aanrichten. Dit noemen we ook wel het effect of de ernst van een incident. Deze schade kan van bedrijfseconomische of meer maatschappelijke aard zijn. Een categorisering en rangschikking van de ernst van mogelijke schades vormt de basis voor de risicoanalyse.

### **4.3 DREIGINGSANALYSE**

Als de belangen en de afhankelijkheden van een bedrijf zijn benoemd en gerangschikt, moeten we systematisch bekijken hoe die belangen kunnen worden bedreigd. Wie kunnen een belang schaden en hoe gaan ze te werk?

56

Een dreigingsanalyse spreekt zich uit over (potentiële) dreigingen. Bij deze analyse is het verstandig eerst mogelijke kwaadwillende personen zoals terroristen in kaart te brengen. Wie heeft de kennis, kunde en intentie om specifieke bedrijven schade toe te brengen? Vervolgens moeten we vaststellen met welke middelen en met welke methoden terroristen te werk kunnen of zullen gaan.

Om een dreigingsanalyse op te stellen, kunnen bedrijven gebruikmaken van de informatie uit hoofdstuk 2, waarin de terroristische dreiging centraal staat. Aanvullende informatie staat op

[www.aivd.nl](http://www.aivd.nl) en [www.nctb.nl](http://www.nctb.nl)

Om een inschatting te maken van dreiging die uitgaat van bijvoorbeeld criminelen, moeten bedrijven andere bronnen en deskundigen raadplegen.

Een categorisering en inschatting van de kans op een terroristische dreiging of een aanslag is de tweede bouwsteen voor de risicoanalyse.



#### **4.4 KWETSBAARHEIDSANALYSE**

De kwetsbaarheidsanalyse onderzoekt de kwetsbaarheid van bedrijven voor terroristische activiteiten. Het legt een relatie tussen de methoden en de middelen van terroristen en de weerbaarheid van het bedrijf daartegen. De methoden en middelen die terroristen kunnen of zullen gebruiken, vloeien voort uit de dreigingsanalyse. Welk bedrijf terroristen uitzoeken is afhankelijk van de aantrekkelijkheid van het bedrijf (zie hoofdstuk 2) en de genomen beveiligingsmaatregelen.

De weerbaarheid van een bedrijf kunnen we onderzoeken en eventueel verbeteren aan de hand van de vijf schakels van de veiligheidsketen: proactie, preventie, preparatie, respons en nazorg.

##### **De veiligheidsketen bestaat uit vijf schakels:**

**Proactie:** voorkomen of wegnemen van structurele oorzaken van onveiligheid;

**Preventie:** voorkomen van directe oorzaken van onveiligheid en beperken van de gevolgen van eventuele inbreuken op die veiligheid;

**Preparatie:** voorbereiden op het optreden bij een aanslag;

**Respons:** bestrijden en beperken van de nadelige gevolgen van een aanslag en hulp verlenen. Soms gebruiken we voor het woord respons ook 'repressie';

**Nazorg:** activiteiten gericht op het verhelpen van de gevolgen van een aanslag en de terugkeer naar de 'normale' situatie.

57

Hieronder beschrijven we de aard van de beveiligingsmaatregelen per schakel in de veiligheidsketen.

- **proactieve maatregelen** moeten voorkomen dat kwetsbaarheden ontstaan. Een bedrijf kan bijvoorbeeld bedrijfsonderdelen naar een minder risicovolle locatie verplaatsen;
- **preventieve maatregelen** verkleinen de kwetsbaarheid en dus de kans op een incident. Voorbeelden hiervan zijn goed hang- en sluitwerk aanbrengen, een toegangscontrole instellen en virusscanners gebruiken;
- **preparatieve maatregelen** zijn gericht op een goede voorbereiding op incidenten. Een

bedrijf kan bijvoorbeeld een ontruimingsplan opstellen voor het personeel en geregeld oefenen;

- **responsieve maatregelen** moeten de directe nadelige gevolgen van een incident beperken. Denk aan het inzetten van blusmiddelen, het organiseren van de eerste hulp en het managen van de crisis;
- **nazorgsmaatregelen** moeten de bedrijfscontinuïteit en de teruggang naar de normale situatie bevorderen. Een voorbeeld is het regelen van een uitwijklocatie.

#### **4.5 RISICOANALYSE**

De risicoanalyse brengt de belangen, dreigingen en weerbaarheid van het bedrijf bij elkaar. Het geeft inzicht in de risico's, welke risico's acceptabel zijn en tegen welke risico's het bedrijf maatregelen moeten nemen.

De risicoanalyse maakt de ernst en het effect van de meest waarschijnlijke terroristische acties duidelijk en houdt rekening met de weerbaarheid van het bedrijf.

58

De risicoanalyse betreft de resultaten uit de andere analyses:

- de kans op dreigingen en aanslagen;
- de weerbaarheid van het bedrijf tegen specifieke dreigingen of activiteiten;
- de ernst van de schade die incidenten ondanks de weerbaarheid van het bedrijf veroorzaken.

De kans op incidenten uit de dreigingsanalyse wordt concreter in het licht van de bestaande én ontbrekende weerbaarheid (maatregelen) uit de kwetsbaarheidsanalyse. Sommige incidenten zullen bij nader inzien door de al aanwezige maatregelen minder aannemelijk blijken te zijn. Zo kan een bedrijf beschikken over informatie die voor terroristen interessant is. Als blijkt dat een bedrijf adequate beveiligingsmaatregelen heeft genomen, is de kans dat deze informatie misbruikt wordt - en daarmee de kans op een incident - kleiner.

De kans dat een bedrijf te maken krijgt met een terroristische aanslag is doorgaans veel lager dan bijvoorbeeld de kans op diefstal. Daar staat tegenover dat de schade door een terroristische aanslag veel ernstiger kan zijn dan de schade die door criminaliteit wordt veroorzaakt.

In de risicoanalyse wordt de kans op een terroristische aanslag daarom gerelateerd aan de ernst van de schade die daaruit kan voortkomen. Dit noemen we ook wel effect. Het resultaat is een waardering van het risico. Een veel gebruikte formule hiervoor is:

**RISICO = KANS X EFFECT**

Nadat de risico's in een rangorde geplaatst zijn, geeft het bedrijf aan welke risico's acceptabel zijn en tegen welke risico's het aanvullende maatregelen moet nemen.

Deze tabel laat zien hoe de afhankelijkheidsanalyse, dreigingsanalyse, kwetsbaarheidsanalyse en risicoanalyse met elkaar samenhangen.

| Type analyse                         | Focus op                                                                                                                   | Leidt tot                                                                                                 |
|--------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Afhankelijkheidsanalyse              | Aard en omvang van de bedrijfsbelangen                                                                                     | Inschatting van de schade bij een incident                                                                |
| Dreigingsanalyse                     | <ul style="list-style-type: none"><li>• potentiële dreiging</li><li>• terroristen</li><li>• middelen en methoden</li></ul> | Inschatting van de kans op terroristische acties of incidenten                                            |
| Kwetsbaarheidsanalyse                | <ul style="list-style-type: none"><li>• weerbaarheid</li><li>• maatregelen</li></ul>                                       | Inschatting van de weerbaarheid van het bedrijf tegen terroristische activiteiten                         |
| <div>+</div> Risicoanalyse           | <ul style="list-style-type: none"><li>• belangen</li><li>• potentiële dreiging</li><li>• weerbaarheid</li></ul>            | Inschatting van de ernst van de schade die incidenten ondanks de weerbaarheid van een bedrijf veroorzaken |
| <div>+</div> Kosten- en batenanalyse | <ul style="list-style-type: none"><li>• effect / baten van de maatregelen</li><li>• kosten van de maatregelen</li></ul>    | Inschatting van de meest kosten-effectieve maatregelen: keuze van aanvullende maatregelen                 |

## **4.6 KOSTEN- EN BATENANALYSE**

De kosten- en batenanalyse bekijkt de aanvullende maatregelen die de geconstateerde risico's uit de risicoanalyse kunnen verminderen. Het is belangrijk om alle fasen uit de veiligheidsketen hierbij te betrekken en alle mogelijke maatregelen te inventariseren (zie ook hoofdstuk 5).

Aan de hand van deze maatregelen is het mogelijk de vermindering van risico's, ofwel de baten, van de maatregelen te bepalen. Centraal staat de vraag of de risico's echt minder worden door de maatregelen. Om het effect van deze maatregelen te beoordelen is enige deskundigheid vereist. Particuliere adviseurs kunnen deze expertise leveren.

De volgende stap is het afzetten van de baten tegen de kosten van de maatregelen. Daardoor wordt duidelijk welke maatregelen het meest kosteneffectief zijn. Staan de kosten in een acceptabele verhouding tot de baten? Aan de hand van een kosten- en batenoverzicht kan het bedrijf aanvullende maatregelen samenstellen. Het bedrijf is zelf verantwoordelijk voor deze afweging van kosten en baten en voor de keuze van de maatregelen. Met andere woorden: bedrijven bepalen zelf het risico dat ze willen lopen.

Na de keuze voor maatregelen is het mogelijk de kwetsbaarheidsanalyse en de risicoanalyse op onderdelen bij te stellen. De nieuwe uitkomst van de risicoanalyse geeft dan zicht op de beheersbaarheid en de acceptatie van de verschillende risico's door het bedrijf.

## **5. BEDRIJFSMAATREGELEN**

### **5.1 HOE KOMT U TOT MAATREGELEN?**

U kunt veel doen om uw bedrijf ook tegen terroristische acties te beveiligen en om goed te reageren als een incident heeft plaatsgevonden. Om een goede keuze uit alle mogelijke maatregelen te maken, is het verstandig eerst een risicoanalyse uit te voeren. Hiervoor is het nodig bestaande en eventuele aanvullende beveiligingsmaatregelen die de kans op een terroristische aanslag beperken, te inventariseren. De maatregelen die u kunt nemen zijn aanzienlijk. Op basis van de analyses bepaalt u zelf welke acties u wel en niet wilt nemen. Daarmee geeft u ook aan welk risico uw bedrijf bereid is te lopen.

De uitkomsten van de analyses kunt u vastleggen in een veiligheidsplan. Dit bevat de bedrijfsvisie op het veiligheidsbeleid. In het plan geeft u aan hoe u de bedrijfscontinuïteit probeert zeker te stellen en hoe uw bedrijf na een incident zo snel mogelijk over kan gaan tot de normale gang van zaken.

#### **Waaruit kan een veiligheidsplan bestaan?**

- bedrijfsstrategie voor bedrijfscontinuïteit en veiligheid (safety en security);
- risicomanagement;
- beveiligingsmaatregelen;
- procedures die personeel en externen, zoals bezoekers, in acht moeten nemen in het geval van verdachte objecten en pakketjes, personen, handelingen en bommeldingen;
- ontruimingsplan.

Het veiligheidsbeleid omvat maatregelen die onveiligheid door opzettelijk menselijk handelen, zoals criminaliteit en terrorisme, beperken (securitybeleid) en maatregelen die de onveiligheid die wordt veroorzaakt door natuurrampen of menselijk falen verminderen (safetybeleid). In deze handreiking komen alleen de securitymaatregelen, ofwel beveiligingsmaatregelen, aan bod.

Veel bedrijven hebben al maatregelen genomen of een veiligheidsplan opgesteld. In dat geval kunt u het onderdeel terrorismebestrijding inpassen in het bestaande (veiligheids)beleid. U zult zien dat veel genomen maatregelen ook bijdragen aan het verminderen van de kans op een terroristische aanslag. U kunt bestaande maatregelen om bijvoorbeeld criminaliteit te voorkomen, behouden en aanvullen met maatregelen tegen terrorisme.

Wie het veiligheidsplan opstelt en de keuze voor de maatregelen neemt, verschilt per bedrijf. Soms doet een security-manager dat, soms de eigenaar of directeur van het bedrijf. Het is handig om een beveiligingscoördinator aan te wijzen die het aanspreekpunt is voor de beveiliging binnen het bedrijf.

**De beveiligingscoördinator kan deze taken op zich nemen:**

- opstellen van een risicoanalyse en kosten- en batenanalyse;
- opstellen van een veiligheidsplan en zorgdragen voor draagvlak voor het plan;
- personeel informeren over het veiligheidsplan, maatregelen en procedures;
- testen, uitvoeren en oefenen van de maatregelen;
- contact leggen en afspraken maken over beveiliging en informatievoorziening met de plaatselijke politie, de gemeente, overige lokale autoriteiten, particuliere beveiligingsorganisaties en naastgelegen bedrijven;
- regelmatig herzien van (onderdelen van) het veiligheidsplan.

Steun van de bedrijfsleiding voor het veiligheidsplan helpt de beveiligingscoördinator zijn werk te doen. Als leidinggevend en hun steun ook uitdragen naar het personeel en zelf de procedures volgen, is de kans op naleving door de werknemers groot. Daarnaast is het verstandig ook eventuele (andere) afdelingen te raadplegen bij het opstellen van het veiligheidsplan. Zij kunnen de beveiligingscoördinator vertellen of bepaalde procedures in de praktijk werken.

## **5.2 WELKE MAATREGELEN KUNT U NEMEN?**

U kunt veel doen om uw bedrijf tegen terroristische acties te beveiligen en om goed te reageren op een eventuele aanslag. In deze handreiking besteden we vooral aandacht aan preventieve maatregelen. Die zorgen ervoor dat een bedrijf een minder aantrekkelijk doelwit is voor criminelen en terroristen. Preventieve maatregelen kunnen niet alleen de kans op een terroristische aanslag verminderen, maar ook andere bedrijfsrisico's zoals criminaliteit beperken.

Overheden en adviesbureaus delen maatregelen verschillend in. In deze handreiking hanteren we de indeling van de veiligheidsketen uit paragraaf 4.4. Daarbij besteden we aandacht aan maatregelen die gericht zijn op objecten en diensten, personeel en informatie.

### **Praktijk: handboek korps regiopolitie Amsterdam-Amstelland**

Het korps regiopolitie Amsterdam-Amstelland bracht in 2005 een handboek uit over de maatregelen die bedrijven kunnen nemen tegen terrorisme en criminaliteit. De brochure bevat praktische tips en adviezen die grote en kleine bedrijven kunnen helpen in de ontwikkeling, herziening of uitbreiding van hun veiligheidsbeleid. De preventieve maatregelen zijn gerangschikt op aandachtspunten voor beveiliging: gebouwen, personeel en informatie.

In 2006 selecteerde het korps regiopolitie enkele bedrijven die extra aandacht nodig hebben, zoals hotels. Het korps regiopolitie legt bedrijfsbezoeken af en brengt bedrijven in contact met de buurtregisseurs. Het korps regiopolitie treedt op als bemiddelaar en stimuleert bedrijven om zich bewust te worden van de risico's. Amsterdam-Amstelland adviseert individuele bedrijven niet over specifieke maatregelen. Hiervoor kunnen bedrijven professionele bedrijven inhuren.

Het handboek is te downloaden op [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)

Elk bedrijf is uniek. De risico's waarmee bedrijven te maken krijgen, zijn dus ook uniek. Dat betekent dat elk bedrijf ook zijn eigen afweging moet maken over de maatregelen die het gaat nemen. We raden u aan u daarbij te laten adviseren. De politie kan u algemene adviezen geven. Voor advies over specifieke bedrijfsmaatregelen kunt u contact opnemen met particuliere beveiligingsadviesbureaus. Dit voorkomt een investering in dure, ineffectieve en onnodige maatregelen. De effectiviteit van maatregelen stijgt als u verschillende maatregelen tegelijk neemt. Maatregelen die zich richten op de objecten zijn effectiever als ze in samenhang worden genomen met activiteiten die zich richten op het personeel.

#### **Meer informatie over beveiligingsmaatregelen**

- Handboek Terrorisme Tegenhouden. Drempelverhogende maatregelen voor bedrijven - Korps regiopolitie Amsterdam-Amstelland. Dit handboek kunt u vinden op [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)
- Protecting against terrorism - Britse veiligheidsdienst MI5. Deze brochure kunt u downloaden op [www.mi5.gov.uk](http://www.mi5.gov.uk)

Voor advies over specifieke beveiligingsmaatregelen voor uw bedrijf kunt u terecht bij particuliere beveiligingsadviseurs.

### **5.3 PROACTIEVE MAATREGELEN**

Proactieve maatregelen voorkomen structurele oorzaken van onveiligheid of nemen deze weg. Daarmee verdwijnt ook de dreiging of het risico. De dreiging voor een bedrijf heeft te maken met het aantrekkelijkheidsprofiel dat terroristen lijken te hanteren. Dit profiel bestaat uit verschillende bedrijfseigenschappen om te bepalen of een bedrijf aantrekkelijk kan zijn voor een terroristische activiteit. Het aantrekkelijkheidsprofiel bestaat uit elementen als de kans op veel slachtoffers, grote economische schade, grote calamiteiten, maatschappelijke onrust en aantasting van specifieke maatschappelijke waarden (zie paragraaf 2.3).



Via proactieve maatregelen kunt u proberen deze factoren te beïnvloeden voorzover dat in een open maatschappij als Nederland mogelijk is. Terroristische dreigingen kunnen we nooit helemaal uitsluiten. Daarom is het niet reëel om aan bedrijven te vragen risicovolle bedrijfsactiviteiten af te stoten. U kunt wel de risico's op een andere manier verminderen. Probeer uw bedrijf op een weinig risicovolle locatie te vestigen.

#### **Praktijk: Clean area rondom stadion**

'De voetbalwedstrijden uit de UEFA- en Champions Leaguecompetitie zijn in honderden landen live op televisie te zien. Daarna besteden voetbaljournals diverse malen op een dag aandacht aan de hoogtepunten. Veel politici en captains of industry wonen de finales bij. De enorme media aandacht en de aanwezigheid van hoogwaardigheidsbekleders maken zulke wedstrijden aantrekkelijk voor terroristen. Daarom nemen we terrorismebestrijding serieus. Laatst ontvingen we ruim 35.000 bezoekers in het stadion. Honderden politiemensen, stewards en particuliere beveiligers controleerden de bezoekers in een voor de gelegenheid gecreëerde clean area rondom het stadion. We hadden het hele gebied met hekken afgezet. Een ingrijpende maar noodzakelijke maatregel.'

*Frank Wijnveld, veiligheidsmanager van PSV*

65

## **5.4 PREVENTIEVE MAATREGELEN**

Preventieve maatregelen voorkomen directe oorzaken van onveiligheid en beperken de gevolgen van eventuele inbreuken daarop. Deze maatregelen zorgen ervoor dat uw bedrijf een minder makkelijk doelwit is voor terroristen. De maatregelen richten zich op objecten en diensten (en eventueel processen), personeel en informatie. Met het beveiligen van uw objecten en diensten, zorgt u ook voor de beveiliging van uw personeel en informatie. Maar ook aanvullende personele maatregelen zijn nodig. Dure beveiligingsmaatregelen hebben weinig zin als uw werknemers ze gemakkelijk kunnen ondermijnen. Veel preventieve maatregelen kan uw bedrijf al hebben genomen om criminaliteit te voorkomen.

### **5.4.1 OBJECTEN EN DIENSTEN**

Kijk eens naar uw objecten en diensten door de ogen van terroristen. Zij zullen er alles aan doen om te voorkomen dat anderen hun voorbereidende handelingen opmerken. Dat beperkt immers de kans op een succesvolle aanslag. Stel uzelf dan ook de vraag of onbevoegden het gebouw makkelijk kunnen binnenkomen en of veel processen en diensten routinematig zijn. En denk bij de beveiliging van uw bedrijf aan de ruimten in het gebouw, de deuren, ramen en muren en de directe en ruimere bedrijfsomgeving van het bedrijf.

#### **Vergroting zichtbaarheid**

Veel bedrijven nemen al maatregelen om de veiligheid onder normale omstandigheden zeker te stellen. Veel van deze maatregelen hebben te maken met goed 'huisvaderschap', zoals het schoonhouden en onderhouden van de publieke en gemeenschappelijke ruimten in en rond uw bedrijf. Dit vergroot de kans dat verdachte zaken of ongebruikelijke objecten sneller opvallen.



Andere voorbeelden van maatregelen die de zichtbaarheid vergroten zijn:

- beperken van bijvoorbeeld het aantal meubelen in gemeenschappelijke ruimten;
- weghalen van obstakels of voorwerpen die het zicht op uw bedrijf belemmeren;

- regelmatig legen van vuilnisbakken of gebruik van doorzichtige vuilniszakken;
- sluiten van kasten en lege kantoren;
- schoonhouden van de omgeving van het bedrijf, zoals de parkeerplaatsen;
- vasthouden aan een vaste plaats voor bepaalde zaken.

Deze maatregelen zorgen ervoor dat u weet hoe de normale situatie eruit ziet. Afwijkingen zijn dan makkelijk te constateren.

### **Bouwtechnische maatregelen**

Bouwtechnische of bouwkundige maatregelen hebben met het object zelf te maken. Soms zijn deze activiteiten effectief om terroristen buiten uw bedrijf te houden. U vergroot er in ieder geval de weerbaarheid van uw bedrijf mee. Bovendien zijn deze maatregelen ook effectief tegen criminelen.

Voorbeelden van bouwtechnische maatregelen zijn:

- kogelwerende of slagvaste beglazing;
- goed hekwerk;
- stevig hang- en sluitwerk op hekken, deuren en ramen;
- goede verlichting.

67

### **Openings- en sluitingsprocedure en toegangsbeleid**

U kan terroristen helpen als uw bedrijf of bedrijfsterrein gemakkelijk toegankelijk is. Om het hen moeilijk te maken om toegang tot uw bedrijf te krijgen, kunt u bouwtechnische maatregelen nemen. Ook kunt u aandacht besteden aan procedures voor de opening en sluiting van uw bedrijf en het toegangsbeleid.

Bij het openen en sluiten van uw bedrijf moet u erop bedacht zijn dat terroristen zich kunnen laten insluiten. Controleer dus van tevoren of er nog ramen open zijn. Tijdens de opening- en sluitingsprocedure doet u er goed aan ook de omgeving te controleren. Informeer de plaatselijke politie bij ongeregelheden.

Door een toegangsbeleid op te stellen voor medewerkers en externen (onder andere bezoekers), bepaalt u onder welke voorwaarden zij uw bedrijf mogen binnenkomen. Informeer uw personeel en bezoekers over uw toegangsbeleid. Geef bijvoorbeeld aan of er een toegangscontrole is. Laat zonder vooraanmelding niemand het bedrijf in, ook niet als de persoon bekend is, zoals een bekende leverancier. Onderdeel van de toegangscontrole kan een bagagecontrole of een onderzoek aan kleding zijn. Deze onderzoeken zijn toegestaan omdat bezoekers privaat terrein betreden. Weigeren bezoekers de controle dan is de enige sanctie dat zij uw bedrijf niet mogen betreden. Uw bedrijf kan de controle dus niet afdwingen. Bezoekers moeten toestemming verlenen tot de controle. Onder onderzoek aan de kleding hoort niet het onderzoek aan het lichaam in verband met de bescherming van de integriteit van het lichaam. Controle van bagage en aan kleding is ook bij personeel toegestaan. Deze controle moet dan opgenomen zijn in de arbeidsvoorwaarden, de arbeidsreglementen of huisregels van uw bedrijf.

Eventueel kunt u een (elektronisch) pasjessysteem invoeren. Dit zal niet voor alle bedrijven mogelijk én gewenst zijn. In dat geval is bezoekersregistratie een uitkomst: noteer de naam van de bezoeker, het bedrijf of de organisatie, het telefoonnummer en de aankomsttijd van de bezoeker. Vraag uw gasten ook altijd om zich te legitimeren met een geldig legitimatiebewijs. Een belangrijk onderdeel van het toegangsbeleid is de inzet van receptionisten en/of bewakingspersoneel. Instrueer ze goed en laat ze ongebruikelijke situaties doorgeven aan de beveiligingscoördinator.

Daarnaast kunt u de kans dat onbevoegden uw bedrijf betreden verminderen door het aantal toegangswegen te beperken of een sleutelplan in te stellen. Dat houdt in dat u het aantal sleutels beperkt en ervoor zorgt dat maar een paar mensen toegangscode van het bedrijf kennen.

Een andere mogelijkheid is uw personeel en bezoekers te autoriseren voor bepaalde bedrijfs-onderdelen, zodat ze zich niet meer vrij in uw bedrijf kunnen bewegen.

### **Toegangsbeleid in een hotel of warenhuis**

In hotels of warenhuizen, waar steeds mensen in en uit lopen, is het niet handig een pasjessysteem in te stellen om de toegang te beperken. Zichtbare aanwezigheid van bijvoorbeeld bewakingspersoneel is daarom belangrijk, zowel bij de ingang als binnen het bedrijf. Mensen verdienen de voorkeur boven camera's omdat camera's makkelijk te saboteren zijn.



## **Veiligheidssystemen**

Elektronische maatregelen kunnen indringers - en dus ook terroristen - ontmoedigen of vroegtijdig opmerken. U kunt een aantal veiligheidssystemen overwegen. Een geïntegreerde inzet daarvan levert de hoogste beveiliging op. Het is verstandig na te denken over de kosten en baten: beperkt de inzet van het veiligheidssysteem werkelijk de risico's van uw bedrijf? U kunt zich laten voorlichten door een particulier beveiligingsadviesbureau. Als u zelf aan de slag gaat is de kans aanwezig dat u investeert in een systeem dat niet de gewenste beveiliging oplevert.

Deze maatregelen zijn het overwegen waard:

- goede verlichting;
- inzet van bewakingspersoneel;
- indringerdetectiesystemen (alarmsystemen);
- (elektronische) systemen voor toegangscontrole;
- video-observatie.

70

De inzet van systemen heeft beperkingen. Vaak zijn systemen vooral nuttig als ze vergezeld gaan met heldere huisregels, die het personeel naleeft. Ook controle op het afgaan van een alarm is heel belangrijk. Daarnaast heeft de techniek van de systemen beperkingen. Veel camera's leveren bijvoorbeeld onvoldoende beeldkwaliteit om mensen te identificeren.

### **5.4.2 PERSONEEL**

Bedrijven kunnen ook slachtoffer worden van kwaadwillende personeelsleden die mogelijk bereid zijn terroristische activiteiten te ondersteunen door bijvoorbeeld informatie aan terroristen te overhandigen. U kunt hier iets tegen doen door uw medewerkers bewust te maken van het belang van beveiligingsmaatregelen. Andere preventieve personeelsmaatregelen richten zich op het aannemen van nieuwe medewerkers en op het inhuren van extern personeel.

### **Praktijk: Iedereen betrekken bij beveiliging**

‘Maak makkelijke doelen moeilijk en onderneem zelf actie. Dat is de crux van beveiligen tegen terroristen. Voor ons bedrijf - opslag en het vervoer van chemische stoffen - gelden stringente beveiligingsmaatregelen. Een aantal daarvan ligt erg voor de hand. Er staan hekken om ons terrein en er is cameratoezicht. Alle magazijnen en kantoren zijn afgesloten en alleen toegankelijk voor medewerkers die een op hun naam uitgeschreven badge dragen. Bovendien trainen we iedereen intern. Deze training gaat in op het omgaan met gevaarlijke stoffen en op het omgaan met veiligheid. Die opleidingen zijn toegespitst op ons bedrijf en we ontwikkelen ze zelf. Voor het bestrijden van een incident zijn we ook voor een groot deel zelfvoorzienend. De magazijnen zijn voorzien van degelijke sprinklers en van calamiteitenmaterialen. Daardoor kunnen we zelf direct ingrijpen. Ook een goede relatie met de hulpverleningsdiensten draagt bij aan de veiligheid.’

*Lucien Govaert, Safety, Health, Quality / Human Resource manager, Te Winkel & Oomes B.V.  
-Chemical Logistics, Nijmegen*

71

### **Bewustwording personeel**

Het is belangrijk dat uw personeel op de hoogte is van beveiligingsmaatregelen, omdat dit de bewustwording rond het belang van beveiliging vergroot. Bespreek de maatregelen en informeer de medewerkers als er wijzigingen zijn.

Beveiliging is een verantwoordelijkheid van alle medewerkers. Doe daar gerust een beroep op. Eventueel kunt u een bijeenkomst organiseren over de risico's die uw bedrijf loopt en op welke wijze uw bedrijf daarmee omgaat. Tijdens zulke bewustwordingstrainingen kunt u uw personeel vragen een bijdrage te leveren aan de beveiliging. Denk aan aandacht voor afgesloten bureaus, kasten en een opgeruimd bureau ('clean desk') aan het einde van elke werkdag. Vanzelfsprekend vertelt u ook wie wat moet doen in bepaalde situaties: wat zijn de procedures van uw bedrijf? U kunt deze instructies in een checklist vastleggen.

Het is erg belangrijk dat medewerkers weten bij wie ze terecht kunnen als ze ongebruikelijke handelingen of situaties signaleren. Ook moeten ze erop kunnen vertrouwen dat de beveiligingscoördinator actie onderneemt naar aanleiding van hun signalen.

Werknemers die al bij u werken kunt u tijdens functionerings- en beoordelingsgesprekken wijzen op het belang van beveiliging. Daarbij kunt u ook aangeven welke sancties volgen als zij niet volgens de voorschriften handelen. Eventueel kunt u een gedragscode opstellen.

Het is mogelijk dat personeel dat al bij u in dienst is radicaliseert. Het is belangrijk om vast te stellen of de radicalisering dermate ver is gevorderd dat het personeelslid ook terroristische activiteiten wil ondersteunen. Neem in zo'n geval contact op met de plaatselijke politie. Gezamenlijk kunt u de beste aanpak bespreken. U kunt een gesprek aangaan met het personeelslid of de persoon eventueel overplaatsen naar een ander bedrijfsonderdeel. Ook kan het voorkomen dat de politie vraagt niets te ondernemen in het belang van lopende onderzoeken. Het is niet nodig de plaatselijke politie te informeren als personeelsleden bijvoorbeeld strikter in hun geloof worden. Het gaat echt alleen om potentiële terroristen.

72

### **Nieuw personeel aannemen**

Bedrijven kunnen geradicaliseerde medewerkers aannemen die een terroristische aanslag willen plegen of ondersteunen, alhoewel de kans daarop klein is. Het is daarom belangrijk dat u aandacht besteed aan de integriteit van de sollicitant.

De mogelijkheid om medewerkers door de AIVD te laten screenen is zeer beperkt. Meestal doet de dienst dat alleen voor vertrouwensfuncties bij bedrijven die behoren tot de vitale infrastructuur. Deze functies zijn erkend door een ministerie.



Een andere mogelijkheid is om een Verklaring omtrent Gedrag (VOG) van nieuwe medewerkers te vragen. Een onderdeel van Justitie, de dienst Justis, verleent een VOG als de kandidaat geen strafbare feiten of overtredingen heeft begaan. Het gaat hierbij dan om strafbare feiten die een relatie met de uit te oefenen functie hebben. De dienst Justis heeft met diverse bedrijfssectoren voor die specifieke sector een profiel met bepaalde delicten opgesteld. Als een sollicitant één van de delicten heeft begaan, wordt geen VOG afgegeven. Door de relatie tussen de functie en het delict is het bereik van het VOG (bewust) beperkt. Voor meer informatie zie [www.justitie.nl](http://www.justitie.nl) U kunt zoeken op 'Justis' of 'Verklaring omtrent Gedrag'.

Als u meer wilt weten over de achtergrond van een sollicitant is de meest gangbare procedure het controleren van referenties en het spreken met vorige werkgevers. Vergeet niet dat met diploma's en getuigschriften makkelijk te knoeien is. Vraag dus altijd naar het origineel. Controleer de gegevens die u verstrekt worden. Het is ook verstandig om sollicitanten te vragen zich te legitimeren met een geldig legitimatiebewijs.

73

### **Praktijk: Menselijke integriteit**

'Is degene die voor je zit, de persoon die hij zegt te zijn? Dat is een cruciale vraag voor de uitzendbranche. Wij kunnen het ons niet permitteren iemand uit te zenden die bijvoorbeeld illegaal is, gokproblemen heeft of criminele of terroristische bedoelingen heeft. Daarom hanteren we strenge beveiligingseisen, vaak in nauwe samenwerking met onze klanten. Namens Vedor werk ik bijvoorbeeld voor een bank. Wij vragen van de flexwerkers een geldig legitimatiebewijs. Als de bank verder wil met een kandidaat, voeren zij een aanvullende screening uit. Onder andere een antecedentenonderzoek. Dit klinkt streng, ja. Maar niet als je beseft dat het om menselijke integriteit gaat.'

*Arianne van Vliet, vestigingsmanager van uitzendbureau Vedor*



### **Inhuur van extern personeel**

Veel bedrijven hebben extern personeel over de vloer. Bijvoorbeeld van uitzendbureaus, onderhoud-, installatie-, schoonmaak-, catering- en beveiligingsbedrijven. Daarnaast huren bedrijven adviesbureaus in die bijvoorbeeld de beschikking kunnen krijgen over belangrijke bedrijfsinformatie. Inhuur kan risico's met zich meebrengen als bedrijven zich er van tevoren niet van vergewissen wie ze binnen halen.

74

U kunt ongewenst gedrag van extern personeel ontmoedigen of beperken met:

- een gedragscode;
- een geheimhoudingsverklaring;
- procedures en voorschriften voor kwetsbare handelingen;
- beperkte toegang tot informatie en gebieden binnen het bedrijf.

U kunt ook van de bedrijven die u inhuurt een Verklaring omtrent Gedrag van een rechtspersoon aanvragen. Met deze verklaring kunnen rechtspersonen hun integriteit tonen aan overheden, partners en bedrijven. De dienst Justis van Justitie geeft de Verklaring af. Voor meer informatie zie [www.justitie.nl](http://www.justitie.nl) U kunt zoeken op 'Justis' of 'Verklaring omtrent Gedrag'.

### **5.4.3 INFORMATIE**

Terroristen kunnen bedrijfsinformatie zoals persoonsgegevens of technische informatie misbruiken. Het is dan ook belangrijk dat u de aanwezige informatie, informatiedragers en informatiestromen inventariseert. Hieronder beschrijven we enkele mogelijkheden om bedrijfsinformatie te beschermen of effectief te vernietigen.

#### **Fysieke en procedurele maatregelen**

Als u beschikt over een inventarisatie van de informatie, de informatiedragers en de informatiestromen, kunt u beoordelen of uw personeel over alle informatie moet beschikken.

Veel informatie wordt verleend op basis van het principe 'nice to know'. Als u kiest voor informatieverstrekking op basis van het principe 'need to know' kunt u gevoelige informatie voor bepaalde medewerkers afschermen. Een digitaal systeem met de mogelijkheid autorisatieniveaus en paswoorden in te stellen kan u hierbij helpen.

Met uw personeel kunt u procedures afspreken om te voorkomen dat informatie rondslingert.

Denk bijvoorbeeld aan:

- afgesloten bureaus en kasten, uitgewiste whiteboards, afgesloten kamers en een schoon en leeg bureau (clean desk);
- schermbeveiliging gebruiken op computers en voorzichtig om gaan met paswoorden;
- spreek met uw medewerkers af dat zij in principe geen informatie mee naar huis nemen;
- laat documenten en laptops niet onbeheerd achter;
- verstrek niet zomaar belangrijke informatie via de telefoon of in de trein;
- berg vertrouwelijke en bedrijfsgevoelige documenten op in een inbraakwerende en/of brandwerende kast.

Om de naleving van afspraken te ondersteunen is het handig afspraken op papier te zetten en uw personeel eventueel een geheimhoudingsverklaring te laten ondertekenen.

## IT-beveiliging

De beveiliging van IT wordt steeds belangrijker. Een goede beveiliging voorkomt economische schade en vermindert de kans dat terroristen informatie uit uw systemen gebruiken voor een aanslag. Terroristen krijgen steeds meer handigheid in het gebruik van ICT. Ze kunnen bedrijven lamleggen door binnen te dringen in een beveiligd computersysteem (hacken). Daarnaast kunnen ze kwaadwillige software toevoegen, functionaliteiten in- en uitschakelen of veranderen en bijvoorbeeld de samenstelling van producten op afstand wijzigen.



Schaf goede software van betrouwbare fabrikanten en leveranciers aan die bestand is tegen virusuitbraken en beschikt over een goede firewall. Van tijd tot tijd is het verstandig uw computersysteem te laten analyseren op risico's. Het coderen van bestanden en het werken met paswoorden kunnen bijdragen aan een betere IT-beveiliging. Daarnaast is het verstandig gebruik te maken van verschillende servers en regelmatig back-ups te maken. Besteed aandacht aan de betrouwbaarheid van het externe IT-personeel.

### **Vernietigen informatie**

U kunt informatie vernietigen door het papier te verscheuren, te verbranden of te verpulveren. Ook zure of chemische technieken zijn voor dit doel geschikt. Maak de keuze tussen het (deels) zelf vernietigen van de informatie of het laten vernietigen. In het laatste geval is het verstandig goede afspraken met het vernietigingsbedrijf te maken. U moet er zeker van zijn dat het ingehuurd bedrijf zich aan de procedures houdt en de afgesproken norm haalt.

Let op: bij het vernietigen van informatie gaat het niet alleen om papieren informatie. Ook servers en computers moeten regelmatig geschoond worden.

77

Het vernietigen van beide soorten informatie kunt u niet alleen overlaten aan medewerkers die verantwoordelijk zijn voor het beheer van ICT of faciliteiten. Ook de beveiligingscoördinator speelt hierin een rol.

## **5.5 PREPARATIEVE MAATREGELEN**

Preparatieve maatregelen hebben betrekking op het daadwerkelijk optreden door uw personeel bij een aanslag. Deze activiteiten zijn van voorbereidende aard. Preparatieve maatregelen voor een terroristische aanslag en een ramp komen grotendeels met elkaar overeen.

Het belangrijkste is dat u voorzieningen heeft om uw personeel in veiligheid te brengen als er een aanslag is gepleegd.

Voorbeelden van preparatieve maatregelen zijn:

- een ontruimingsplan opstellen;
- uw personeel informeren over het ontruimingsplan, de vluchtwegen en de ontruimingsprocedures;
- een plek aanwijzen waar medewerkers zich moeten verzamelen;
- mensen een opleiding voor bedrijfshulpverlening laten volgen;
- regelmatig ontruimingsoefeningen houden;
- regelmatig controleren of het waarschuwingssysteem werkt;
- regelmatig controleren of materiaal de vluchtwegen niet verspert;
- aangeven welke procedures medewerkers moeten volgen bij bommeldingen en verdachte pakketjes;
- veilige plekken binnen uw bedrijf aanwijzen als het niet verstandig is naar buiten te gaan. Bijvoorbeeld als er een aanslag plaatsvindt met chemische, biologische, radiologische en nucleaire wapens (CBRN-middelen);
- kijken of u uw airconditioning kunt uitzetten. Bijvoorbeeld in geval van een poederbrief of een aanslag met CBRN-middelen;
- zorgen voor voldoende middelen, zoals dekens.

78

Een belangrijk onderdeel van een ontruimingsplan is het hebben van juiste, actuele telefoonlijsten. Wie moeten wanneer gebeld worden bij een aanslag? Maak ook een lijst van telefoonnummers van hulpverleningsinstanties en de gemeente. Bij de plaatselijke politie en de overige lokale autoriteiten moet ook in ieder geval één contactpersoon van uw bedrijf bekend zijn.

Het ontruimingsplan besteedt ook aandacht aan ontruimingen in verband met een brand, het gebruik van CBRN-middelen (denk aan poederbrieven) en bommeldingen. Het is verstandig procedures vast te stellen voor het geval uw bedrijf of medewerkers geconfronteerd worden met een poederbrief of met een bommelding. Train medewerkers geregeld in het herkennen van en het reageren op verdachte brieven, pakketjes en bommeldingen.

### **Praktijk: Actuele en realistische dreiging als basis van veiligheidsbeleid**

‘Na 11 september 2001 ontstond wereldwijd de angst dat Al Qaida pakjes rond zou sturen met giftig antraxpoeder. Dat leidde tot maatregelen bij TNT Post. Medewerkers kregen de beschikking over mondkapjes en handschoenen. Als ze in aanraking kwamen met een poeder, moesten ze direct onder de douche en een overall aantrekken. Later bleek deze angst ongegrond. Nogal wat grapjassen maakten van de gelegenheid gebruik om bijvoorbeeld waspoeder op te sturen.

De maatregelen maakten diepe indruk op onze mensen. Dit vormde de opmaat naar een veiligheidsbeleid dat gebaseerd is op actuele en realistische dreiging en op een gedegen risico-analyse: wat hebben we nodig om ons veilig te voelen? Per gebouw, locatie en materiaal hebben we de risico's in kaart gebracht.

Goede informatie is de basis. Zo wisselen we informatie met andere Europese post-bedrijven uit. Daarnaast hebben wij goede contacten met overheidsdiensten.

We hebben geen ervaring met terroristen, maar we mogen niet achterover leunen tot er wat gebeurt. We moeten wél nuchter blijven en realistische maatregelen nemen om onnodige paniek te voorkomen. Onze mensen werken nog steeds met handschoenen, maar het is vandaag de dag niet nodig om bij het eerste het beste poeder automatisch ambulance en politie in te schakelen.’

*Ab Verkaik, directeur bedrijfsveiligheid van TNT Post Nederland*

79

Ook maatregelen die de bedrijfscontinuïteit verbeteren tijdens of na een aanslag behoren tot de preparatieve maatregelen. Voorbeelden hiervan zijn het maken van regelmatige back-ups van computerbestanden en ervoor zorgen dat belangrijke documenten ook elders elektronisch of fysiek beschikbaar zijn.

### **Hoe kan een verdacht pakketje of brief eruit zien?**

- het heeft een vreemde vorm, geur en/of een ongebruikelijk gewicht;
- er staan veel fouten in het adres;
- het land of de stad van herkomst van de afzender klopt niet met het poststempel;
- de brief of het pakketje is onverwacht of van een onverwachte zender;
- de verpakking bevat vetvlekken of verkleuringen;
- het adres van de afzender is niet vermeld, onleesbaar of oncontroleerbaar;
- de brief of het pakketje is te veel gefrankeerd;
- de melding 'persoonlijk' of 'vertrouwelijk' bevindt zich op het omslag;
- de brief of het pakketje is op een vreemde manier bezorgd;
- er is vreemd of veel materiaal gebruikt, zoals touw, plakband, aluminiumfolie en metalen draden.

## **5.6 RESPONSIEVE MAATREGELEN**

80

Responsieve maatregelen hebben te maken met het bestrijden van de aanslag, het beperken van de nadelige gevolgen ervan en het verlenen van hulp. Een ander woord voor respons is 'repressie'. De maatregelen in deze categorie zijn vooral toebedeeld aan de hulpverleningsorganisaties: brandweer, politie en ambulance. Het effect van de responsieve maatregelen is ook afhankelijk van de mate waarin een getroffen bedrijf zich voorbereid heeft op rampen en incidenten. Denk aan regelmatige oefening en een goede opleiding van het personeel.

Responsieve maatregelen tijdens een terroristische aanslag komen grotendeels overeen met de maatregelen tijdens een ramp of andere crisis. Toch zijn er ook verschillen. Dat is ook de reden dat de landelijke overheid in oktober 2006 is gestart met een landelijke campagne onder de titel 'Denk vooruit'. Deze campagne benadrukt dat elke crisis andere maatregelen verlangt. In de campagne staat centraal wat u kunt doen bij een grote brand, bij langdurige uitval van stroom, gas, water of telefoon, bij een overstroming, bij het vrijkomen van gevaarlijke stoffen en bij een terroristische aanslag.



Bij een terroristische aanslag is het van belang dat uw medewerkers alert zijn en informatie doorgeven aan de plaatselijke politie. Deze informatie kan helpen de daders op te sporen.

Op de website [www.crisis.nl](http://www.crisis.nl) vindt u de basale maatregelen voor de verschillende crises. Algemene informatie over crisismanagement en crisisbeheersing is te vinden op [www.veiligheid.minbzk.nl](http://www.veiligheid.minbzk.nl)

#### Tips om met verdachte pakketjes om te gaan

- raak het pakketje niet aan, maar bekijk het wel zorgvuldig;
- verlaat de plaats waar het pakketje zich bevindt en voorkom trillingen;
- sluit de plaats waar het pakketje zich bevindt af;
- informeer de beveiligingscoördinator (en via hem eventueel de politie);
- gebruik nooit een gsm, palm top of IPAQ;
- in geval van een mogelijke poederbrief: de brief niet schudden. Stop hem in een plastic zak. Zet eventuele ventilatie uit en zorg dat niemand direct in contact komt met de poeder.

81



### Tips om met telefonische bommeldingen om te gaan

- blijf kalm en luister naar het bericht;
- probeer zoveel mogelijk informatie van de beller te verkrijgen. Stel vragen als:
  - waar is de bom geplaatst?
  - hoe ziet de bom eruit?
  - wanneer gaat de bom af?
  - hoe groot zal de explosie zijn?
  - wie heeft de bom geplaatst?
- probeer het gesprek op te nemen als dat mogelijk is;
- probeer te achterhalen van waar de beller belt;
- stel direct de beveiligingscoördinator op de hoogte (die de politie inlicht en eventueel tot ontruiming overgaat);
- probeer zoveel mogelijk notities op te stellen voor de politie, zoals:
  - het geslacht van de beller;
  - eventueel de naam, leeftijd en nationaliteit van de beller;
  - gesproken taal (accent);
  - achtergrondgeluiden;
  - toon van beller (nasaal, gehaast, kalm, hysterisch).



### **Wat moet u doen bij een bomaanslag?**

- bescherm uzelf tegen rondvliegend of vallend materiaal;
- als u zelf niet ernstig gewond bent, help dan zoveel mogelijk anderen;
- ga zo snel mogelijk naar een open plek, uit de buurt van grote gebouwen vanwege instortingsgevaar;
- ga niet in groepen staan. Er kan nóg een bom ontploffen;
- blijf uit de buurt van ramen omdat ze kunnen breken en geparkeerde auto's omdat ze kunnen ontploffen;
- doe wat politie, beveiligingspersoneel of hulpverleners zeggen;
- gebruik de telefoon kort en niet voor onnodige gesprekken;
- gebruik geen lucifers of aanstekers in verband met de kans op een gas-ontploffing;
- geef informatie die kan helpen bij het opsporen van de daders door aan de politie, zoals signalementen en een beschrijving van een auto;
- geef foto's die u gemaakt heeft, bijvoorbeeld met uw mobiele telefoon, aan de politie;
- ga niet kijken op de plek van de aanslag;
- kijk bij een aanslag regelmatig naar de televisie, luister naar de radio, of kijk op [www.nederlandtegenterrorisme.nl](http://www.nederlandtegenterrorisme.nl) voor meer informatie.

83

### **5.7 NAZORGSMATREGELEN**

Nazorgsmaatregelen zijn activiteiten om de gevolgen van een aanslag te verhelpen en herhaling te voorkomen. Deze maatregelen zorgen voor een terugkeer naar de 'normale' situatie. Als u veel aandacht heeft besteed aan preparatieve maatregelen om de bedrijfscontinuïteit te bevorderen, komt dit de nazorg ten goede. Dat zou kunnen betekenen dat u heeft gezorgd voor een goede uitwijkmogelijkheid voor uw bedrijf als u niet meer in uw gebouw kunt werken. Ook kunt u maatregelen hebben genomen voor het behoud van informatie en gegevens. U heeft misschien uw servers ook buiten uw pand laten draaien en heeft voldoende back-ups gemaakt.

Uw personeel is waarschijnlijk voor u het belangrijkste. Het is dan ook aannemelijk dat u van tevoren goede verzekeringen heeft afgesloten, zodat uw werknemers niet de dupe van een aanslag op uw bedrijf worden (bijvoorbeeld door ziekte). U kunt medewerkers ook psychische hulp aanbieden. Het is raadzaam met uw verzekeraar uw polis te bespreken om te kijken of u voldoende verzekerd bent.



## **5.8 CHECKLIST VOOR BEDRIJVEN**

In deze handreiking hebben we u veel tips gegeven om op structurele wijze een goede bedrijfsbeveiliging op te zetten tegen terroristische dreigingen en aanslagen. We zetten de suggesties nog eens op een rij.

### **Checklist beveiligingsmaatregelen:**

1. Stel u op de hoogte van de terroristische dreiging voor Nederland en bekijk welke eigenschappen een bedrijf aantrekkelijk maken voor terroristen.
2. Sta regelmatig stil bij de vraag welke specifieke risico's op uw bedrijf afkomen. Maak periodiek een risicoanalyse. Probeer uw bedrijf eens door de ogen van terroristen te bekijken.
3. Bekijk of aanvullende beveiligingsmaatregelen de risico's effectief kunnen terugdringen. Maak een afweging tussen de kosten en de baten (effecten).
4. Stel een veiligheidsplan op.
5. Stimuleer het bewustzijn rond beveiliging van uw medewerkers.
6. Oefen regelmatig het veiligheidsplan en de beveiligingsmaatregelen. Pas het plan zonodig aan.
7. Zorg ervoor dat medewerkers tijdig verdachte en ongebruikelijke omstandigheden signaleren en deze bij de beveiligingscoördinator melden. Die neemt zonodig contact op met de lokale politie.
8. Zorg voor zichtbaarheid in en om uw bedrijf door de ruimten en omgeving schoon te houden.
9. Stel een goed toegangsbeleid in en een goede toegangscontrole.
10. Zorg voor een goede beveiliging van uw pand om terroristen af te schrikken. Voorbeelden zijn goed hang- en sluitwerk, alarmsystemen, goede verlichting en video-observatie.
11. Controleer de referenties bij het aannemen van nieuw personeel. Zorg ervoor dat u te maken hebt met betrouwbare bedrijven als u extern personeel inhuurt.
12. Schenk voldoende aandacht aan het beschermen en vernietigen van bedrijfsgevoelige informatie en aan het beveiligen van uw ICT-systemen.
13. Zorg voor goede procedures voor bommeldingen, bomaanslagen en verdachte pakketjes.
14. Stel een ontruimingsplan op en houd regelmatig ontruimingsoefeningen.
15. Zorg dat u maatregelen heeft genomen zodat de bedrijfscontinuïteit van uw bedrijf niet in gevaar komt bij een eventuele aanslag.

# BIJLAGEN

## BIJLAGE I: VERKLARING VAN WOORDEN

| Begrip                           | Omschrijving                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Aantrekkelijkheidsprofiel</b> | Profiel van een bedrijf dat bestaat uit diverse eigenschappen die terroristen lijken te hanteren bij de selectie van hun doelwit of middel voor een aanslag.                                                                                                                                                                                                                            |
| <b>Afhankelijkheidsanalyse</b>   | Hierin staan de vitale bedrijfsprocessen en cruciale onderdelen van een bedrijf centraal. Deze belangen en afhankelijkheden van de organisatie moeten beschermd worden om ernstige bedrijfseconomische en maatschappelijke schade te voorkomen. Afhankelijkheidsanalyses zijn onderdeel van risicoanalyses.                                                                             |
| <b>Alerteringsniveau</b>         | Het Alerteringssysteem Terrorismebestrijding bevat vier niveaus. Het basisniveau, en drie alerteringsniveaus bij oplopende dreiging: lichte, matige en hoge dreiging. Elk niveau en elke sector kent zijn eigen pakket van maatregelen. Hoe hoger het niveau, hoe zwaarder en ingrijpender de maatregelen.                                                                              |
| <b>Bedrijfssectoren</b>          | Bedrijfssectoren zijn in deze handreiking de negen bedrijfstakken die zijn aangesloten bij het Alerteringssysteem Terrorismebestrijding en/of de twaalf bedrijfstakken die zijn aangesloten bij het project Bescherming Vitale Infrastructuur.                                                                                                                                          |
| <b>Beveiligingscoördinator</b>   | Persoon binnen het bedrijf die verantwoordelijk is voor het beveiligingsbeleid. Hij stelt onder meer het beveiligingsplan op.                                                                                                                                                                                                                                                           |
| <b>Beveiligingsmaatregelen</b>   | Maatregelen van bedrijven en overheden die gericht zijn op de beveiliging van een object, product, dienst of persoon. Deze maatregelen moeten de kans op en het effect van een eventuele aanslag verminderen, ook wel security maatregelen genoemd. Soms wordt ook de term veiligheidsmaatregelen gebruikt. Het gaat dan ook om maatregelen om natuurrampen en dergelijke te voorkomen. |
| <b>Beveiligingsplan</b>          | Strategie van het bedrijf voor bedrijfscontinuïteit en veiligheid (safety en security). Het plan bevat onder andere het risicomanagementsysteem van het bedrijf, de te treffen beveiligingsmaatregelen, de in acht te nemen procedures en een ontruimingsplan.                                                                                                                          |
| <b>Concrete dreiging</b>         | Aanwijzingen dat een bedrijf daadwerkelijk een doelwit is voor een terroristische aanslag of als middel door terroristen misbruikt gaat worden. De precieze intentie of voorbereidingshandelingen zijn geconstateerd.                                                                                                                                                                   |
| <b>Contra-terrorismebeleid</b>   | Beleid dat terrorisme tegengaat.                                                                                                                                                                                                                                                                                                                                                        |

|                                                  |                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Coördinator Bewaking en Beveiliging (CBB)</b> | De Coördinator Bewaking en Beveiliging valt onder de verantwoordelijkheid van de NCTb en is belast met het onderhoud en de uitvoering van het Stelsel van Bewaking en Beveiliging.                                                                                                                                                             |
| <b>Dreigingsanalyse</b>                          | Een (terroristische) dreigingsanalyse onderzoekt terroristen en hun activiteiten en kijkt naar potentiële dreigingen. De kans van de dreiging staat centraal. Dreigingsanalyses zijn onderdeel van risicoanalyses.                                                                                                                             |
| <b>Dreigingsbeeld Terrorisme Nederland</b>       | De NCTb stelt het Dreigingsbeeld Terrorisme Nederland op. Dit is een periodieke analyse op hoofdlijnen van de (inter)nationale terroristische dreiging tegen Nederland.                                                                                                                                                                        |
| <b>Dreigingsniveaus</b>                          | Een dreigingsniveau geeft de ernst en de kans op een dreiging weer. Het Dreigingsbeeld Terrorisme Nederland onderscheidt vier dreigingsniveaus: minimaal, beperkt, substantieel en kritiek.                                                                                                                                                    |
| <b>Driehoek</b>                                  | De driehoek bestaat uit de burgemeester, de (hoofd)officier van justitie en de korpschef van de politie. Zij bespreken de lokale openbare orde en het veiligheidsbeleid.                                                                                                                                                                       |
| <b>Ketenbeveiliging</b>                          | Met ketenbeveiliging wordt bedoeld dat elke schakel in een keten de veiligheid moet kunnen garanderen tegenover de andere schakels. De vervoersketen is hier een voorbeeld van.                                                                                                                                                                |
| <b>Kwetsbaarheidsanalyse</b>                     | In deze analyse wordt de weerbaarheid van een bedrijf tegen bijvoorbeeld een terroristische aanslag onderzocht. De kwetsbaarheid van een bedrijf hangt af van de aantrekkelijkheid van het bedrijf voor terroristen en de maatregelen die een bedrijf heeft getroffen.                                                                         |
| <b>Potentiële dreiging</b>                       | Als de eigenschappen van een bedrijf overeenkomen met het aantrekkelijkheidsprofiel dat terroristen hanteren, spreken we van een potentiële dreiging. Een bedrijf is dan een aantrekkelijk doelwit of middel voor een aanslag, maar er zijn nog geen concrete aanwijzingen voor een op handen zijnde aanslag. De dreiging is dan voorstelbaar. |
| <b>Radicalisme</b>                               | Een geesteshouding, waarbij iemand bereid is om de uiterste consequentie uit een denkwijze te aanvaarden en die in daden om te zetten.                                                                                                                                                                                                         |
| <b>Radicalisering</b>                            | Toenemende bereidheid om diep ingrijpende veranderingen in de samenleving na te streven of te ondersteunen die op gespannen voet staan met de democratische rechtsorde en/of waarbij ondemocratische middelen worden ingezet.                                                                                                                  |



|                                 |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Risicoanalyse</b>            | In deze analyse worden de cruciale belangen, de kans op dreigingen en de weerbaarheid van een bedrijf aan elkaar gerelateerd. Door belangen, dreigingen en weerbaarheid in hun onderlinge samenhang te bekijken kunnen risico's van een bedrijf worden benoemd. Op basis van de risicoanalyse kunnen bedrijven maatregelen nemen die de risico's wegnemen of verminderen, of de gevolgen ervan beperken.                                                                                                                                                                                                                                                                                           |
| <b>Risicomanagement-systeem</b> | Systeem waarin aangegeven is hoe een bedrijf risico's beperkt en zijn continuïteit zeker probeert te stellen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Safety-beleid</b>            | Beleid om onveiligheid die veroorzaakt wordt door natuurlijke afwijkingen, rampen, systeem- of procesfouten of menselijk falen te voorkomen en te bestrijden.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Security-beleid</b>          | Beleid om onveiligheid die veroorzaakt wordt door opzettelijk menselijk handelen, zoals criminaliteit en terrorisme, te voorkomen en te beperken.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Security-maatregelen</b>     | Zie beveiligingsmaatregelen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Terrorisme</b>               | Terrorisme is het op mensenlevens gerichte plegen van of dreigen met geweld door individuen of groepen, het ontwrichten van de samenleving of het toebrengen van ernstige schade, met als doel maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden.                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Terrorismebestrijding</b>    | Terrorismebestrijding is het verkleinen van de kans op een terroristische aanslag of dreiging, het beperken van de gevolgen van aanslagen en het opsporen en vervolgen van terroristen.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Terroristische dreiging</b>  | De mate waarin er sprake is van een dreiging van een terroristische aanslag.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Veiligheidsketen</b>         | De veiligheidsketen bevat vijf schakels van veiligheidsmaatregelen:<br><b>Proactie:</b> voorkomen of wegnemen van structurele oorzaken van onveiligheid.<br><b>Preventie:</b> voorkomen van directe oorzaken van onveiligheid en beperken van de gevolgen van eventuele inbreuken op die veiligheid.<br><b>Preparatie:</b> voorbereiden op daadwerkelijk optreden bij een aanslag.<br><b>Respons:</b> bestrijden van de aanslag, beperken van de nadelige gevolgen van een aanslag en het verlenen van hulp. Soms wordt voor respons ook 'repressie' gebruikt.<br><b>Nazorg:</b> activiteiten gericht op het verhelpen van de gevolgen van een aanslag en de terugkeer naar de 'normale' situatie. |



|                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Vitale infrastructuur</b> | Producten, diensten en de onderliggende processen behoren tot de vitale infrastructuur die, als zij uitvallen, maatschappelijke ontwrichting kunnen veroorzaken. Van maatschappelijke ontwrichting is sprake als er veel slachtoffers zijn en grote economische schade is toegebracht. Ook bij langdurig herstel of bij afwezigheid van reële alternatieven terwijl de samenleving deze producten en diensten niet kan missen, is er sprake van maatschappelijke ontwrichting. |
| <b>Weerbaarheid</b>          | De weerbaarheid heeft betrekking op de mate waarin een bedrijfssector of een bedrijf zich tegen een aanslag of dreiging kan verweren. De weerbaarheid van een bedrijf is te verbeteren aan de hand van de vijf schakels van de veiligheidsketen.                                                                                                                                                                                                                               |

## **BIJLAGE II: AFKORTINGEN**

|                  |                                                                |
|------------------|----------------------------------------------------------------|
| <b>AEO</b>       | Authorized Economic Operator                                   |
| <b>ATb</b>       | Alerteringssysteem Terrorismebestrijding                       |
| <b>AIVD</b>      | Algemene Inlichtingen- en Veiligheidsdienst                    |
| <b>BZK</b>       | Binnenlandse Zaken en Koninkrijksrelaties                      |
| <b>CBB</b>       | Coördinator Bewaking en Beveiliging                            |
| <b>CBRN</b>      | Chemisch, Biologisch, Radiologisch en Nucleair                 |
| <b>CCB</b>       | Conflict- en Crisisbeheersing (van de politie)                 |
| <b>CEN</b>       | (European) Committee for Standardization                       |
| <b>C-TPAT</b>    | Customs Trade Partnership Against Terrorism                    |
| <b>DKDB</b>      | Dienst Koninklijke en Diplomatieke Beveiliging (van het KLPD)  |
| <b>DTN</b>       | Dreigingsbeeld Terrorisme Nederland                            |
| <b>EBB</b>       | Eenheid Bewaking en Beveiliging (van de NCTb)                  |
| <b>EU</b>        | Europese Unie                                                  |
| <b>IMO</b>       | International Maritime Organization                            |
| <b>ISO</b>       | International Organization for Standardization                 |
| <b>ISPS-Code</b> | International Ship and Port Facility Security Code             |
| <b>KLPD</b>      | Korps Landelijke Politiediensten                               |
| <b>NCTb</b>      | Nationaal Coördinator Terrorismebestrijding                    |
| <b>NHT</b>       | Nederlandse Herverzekeringsmaatschappij voor Terrorismeschaden |
| <b>NPI</b>       | Nederlands Politie Instituut                                   |
| <b>TAPA</b>      | Technology Asset Protection Association                        |
| <b>VOG</b>       | Verklaring omtrent Gedrag                                      |
| <b>Vpb</b>       | Vereniging van Particuliere Beveiligingsorganisaties           |
| <b>VvBO</b>      | Verbond van Beveiligingsorganisaties                           |
| <b>WCO</b>       | World Customs Organization                                     |

## **BIJLAGE III: WEBSITES**

### ***Binnenland***

| Site                                                                     | Uitleg                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="http://www.aivd.nl">www.aivd.nl</a>                             | Deze site van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) biedt inzicht in de organisatie en taken van deze organisatie en bevat ook AIVD-jaarverslagen en publicaties over bijvoorbeeld terrorisme en veiligheidsrisico's.                                                                                                                    |
| <a href="http://www.evo.nl">www.evo.nl</a>                               | Leden van de verladersorganisatie (EVO) kunnen inloggen voor extra informatie. De site bevat onder het thema 'criminaliteit en security' informatie over (inter)nationale en Europese wet- en regelgeving rond terrorismebestrijding.                                                                                                                    |
| <a href="http://www.hetccv.nl">www.hetccv.nl</a>                         | Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) stimuleert samenwerking tussen publieke en private organisaties om criminaliteit integraal terug te dringen en vormt een schakel tussen beleid en praktijk. Het CCV richt zich op overheden, instellingen en brancheorganisaties. Er is ook een thema 'ondernemen' opgenomen op de website. |
| <a href="http://www.crisis.nl">www.crisis.nl</a>                         | Site van de landelijke overheid met informatie over wat men kan doen bij rampen. Bij een ramp (of terroristische aanslag) wordt de site vervangen door een site met actuele informatie over de ramp.                                                                                                                                                     |
| <a href="http://www.justitie.nl">www.justitie.nl</a>                     | Deze site van het ministerie van Justitie besteedt onder het thema 'criminaliteit' aandacht aan terrorisme en de Verklaring omtrent Gedrag.                                                                                                                                                                                                              |
| <a href="http://www.kvk.nl">www.kvk.nl</a>                               | Op deze site van de Kamers van Koophandel wordt onder het thema 'wetten en regels' aandacht besteed aan 'veilig ondernemen'. Ook terrorisme komt aan de orde.                                                                                                                                                                                            |
| <a href="http://www.meldmisdaadanoniem.nl">www.meldmisdaadanoniem.nl</a> | Via deze meldlijn van Stichting M. kunnen burgers en bedrijven anoniem melding doen van ernstige misdrijven, zoals moord en doodslag of wapenhandel. M. geeft meldingen door aan politie, Justitie of opsporings- en inlichtingendiensten, maar ook aan het Verbond van Verzekeraars.                                                                    |
| <a href="http://www.meldpuntcybercrime.nl">www.meldpuntcybercrime.nl</a> | Via het Meldpunt Cybercrime kunnen burgers en bedrijven melding maken van radicalisering, terrorisme of kinderporno op of via het internet. Deze melding kan de basis zijn voor politie, Justitie of opsporings- en inlichtingendiensten om actie te ondernemen.                                                                                         |

|                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="http://www.mkb.nl">www.mkb.nl</a>                                                                                                                                                              | Op deze site van MKB-Nederland is informatie over terrorismebestrijding te vinden bij de nieuwsberichten. Informatie over veilig ondernemen is beschikbaar onder 'projecten'.                                                                                                                                                                                                                                                          |
| <a href="http://www.minbzk.nl">www.minbzk.nl</a>                                                                                                                                                        | De site van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) besteedt onder het thema 'veiligheid' aandacht aan terrorisme. Onder het thema 'veiligheid' is ook informatie beschikbaar over crisisbeheersing, bescherming vitale infrastructuur en de AIVD.                                                                                                                                                          |
| <a href="http://www.nctb.nl">www.nctb.nl</a>                                                                                                                                                            | De site van de Nationaal Coördinator Terrorismebestrijding (NCTb) verstrekt onder andere informatie over het huidige dreigingsniveau en het Alerteringssysteem en bevat overheidsdocumentatie over terrorismebestrijding.                                                                                                                                                                                                              |
| <a href="http://www.ndl.nl">www.ndl.nl</a>                                                                                                                                                              | Site van Vereniging van Nederland Distributieland (NDL/HIDC), vereniging van en voor de logistieke sector. Onder het thema 'projecten / thema 1: 'Europese Logistieke Netwerken', gaat deze site in op het Transumo-project PROTECT. Op de site zijn diverse verslagen en publicaties te downloaden.                                                                                                                                   |
| <a href="http://www.nederlandtegen-terrorisme.nl">www.nederlandtegen-terrorisme.nl</a><br>of <a href="http://www.nederlandtegen-terrorisme.nl/bedrijven">www.nederlandtegen-terrorisme.nl/bedrijven</a> | Deze site van de landelijke overheid geeft aan wat er gedaan wordt tegen terrorisme en wat burgers en bedrijven zelf kunnen doen.                                                                                                                                                                                                                                                                                                      |
| <a href="http://www.om.nl">www.om.nl</a>                                                                                                                                                                | Het Openbaar Ministerie is verantwoordelijk voor de opsporing en vervolging van strafbare feiten. Deze site bevat een dossier 'terrorisme'. Daarnaast is het mogelijk om via het 'thema' parketten door te klikken naar het Landelijk Parket, dat zich bezighoudt met de aanpak van onder andere terrorisme.                                                                                                                           |
| <a href="http://www.politie.nl">www.politie.nl</a>                                                                                                                                                      | Site van Politie Nederland met informatie over de korpsen en het Nederlands Politie Instituut. Het thema 'Politie ABC' besteedt ook aandacht aan terrorisme.                                                                                                                                                                                                                                                                           |
| <a href="http://www.politie.nl/klpd">www.politie.nl/klpd</a>                                                                                                                                            | Via deze site van het Korps Landelijke Politie Diensten (KLPD) is het mogelijk informatie te verkrijgen over diverse onderdelen van de KLPD die een bijdrage aan terrorismebestrijding leveren, zoals de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB), de dienst Nationale Recherche Informatie (DNRI) en de dienst Nationale Recherche (DNR). Onder de laatste dienst valt ook de Unit Contraterorisme en -activisme (UCTA). |
| <a href="http://www.politie-amsterdam-amstelland.nl">www.politie-amsterdam-amstelland.nl</a>                                                                                                            | Site van de politieregio Amsterdam-Amstelland, waarop het onderwerp 'terrorisme' aan bod komt onder het thema 'in de praktijk / speerpunten'. Hier kunnen bedrijven een preventiepakket terrorisme voor ondernemers aanvragen.                                                                                                                                                                                                         |

|                                                                              |                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="http://www.portsecuritytoolkit.com">www.portsecuritytoolkit.com</a> | Site met informatie over de ISPS-Code en een toolkit voor het ontwerpen van (haven)veiligheidsplannen.                                                                                                                                                                                                                          |
| <a href="http://www.protect.transumo.nl">www.protect.transumo.nl</a>         | TRansition SUSTainable MObility (Transumo) is een platform van bedrijven, overheden en kennis-instellingen die kennis ontwikkelen op het gebied van mobiliteit. Deze site behandelt het Transumo-project Protect. Protect bekijkt hoe bedrijven en de landelijke overheid internationale goederenstromen veiliger kunnen maken. |
| <a href="http://www.tln.nl">www.tln.nl</a>                                   | Op deze site van Transport en Logistiek Nederland (TLN) komen onder het thema 'visie / milieu en veiligheid' onderwerpen aan de orde die verwant zijn aan terrorisme.                                                                                                                                                           |
| <a href="http://www.veiligheid.minbzk.nl">www.veiligheid.minbzk.nl</a>       | De site van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) over veiligheid besteedt geen aandacht aan terrorisme, maar wel aan aanverwante onderwerpen onder 'projecten'.                                                                                                                                   |
| <a href="http://www.vno-ncw.nl">www.vno-ncw.nl</a>                           | Onder het thema 'dossiers' komt criminaliteitsbeheersing aan de orde op de site van VNO-NCW. Hier zijn onder andere nieuwsberichten over terrorisme te vinden.                                                                                                                                                                  |
| <a href="http://www.vvbo.nl">www.vvbo.nl</a>                                 | Site van het Verbond van Beveiligingsorganisaties (VvBO). Hierop kunt u doorklikken naar alle aangesloten leden van VvBO, zoals de Vereniging van Particuliere Beveiligingsorganisaties (Vpb).                                                                                                                                  |

## Buitenland

| Site                                                                       | Uitleg                                                                                                                                                                                 |
|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="http://www.cabinetoffice.gov.uk">www.cabinetoffice.gov.uk</a>     | Site van het kabinet van het Verenigd Koninkrijk. Onder 'Security, Intelligence and Resilience' is informatie beschikbaar verwant aan terrorisme.                                      |
| <a href="http://www.cityoflondon.police.uk">www.cityoflondon.police.uk</a> | Site van de City of London Police. Onder 'Countering Terrorism' is informatie beschikbaar over terrorisme.                                                                             |
| <a href="http://www.cbp.gov">www.cbp.gov</a>                               | Site van U.S. Customs and Border Protection waarop aandacht voor C-TPAT: Customs Trade Partnership Against Terrorism.                                                                  |
| <a href="http://www.dhs.gov/dhspublic">www.dhs.gov/dhspublic</a>           | Site van Homeland Security (Ministerie van Veiligheid in de Verenigde Staten). Op deze site is onder het thema 'threats and protection' informatie beschikbaar verwant aan terrorisme. |

|                                                                                    |                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="http://www.ec.europa.eu">www.ec.europa.eu</a>                             | Site van de Europese Commissie van de EU. Op deze site is informatie beschikbaar over het EU-beleid. Ook is het mogelijk bij de sites van de Directoraten-generaal en diensten informatie te zoeken over terrorisme en vitale infrastructuur. |
| <a href="http://www.homeoffice.gov.uk">www.homeoffice.gov.uk</a>                   | Site van Ministerie van Binnenlandse Zaken van het Verenigd Koninkrijk. Onder 'security' is informatie beschikbaar over het dreigingsniveau, de maatregelen die getroffen worden en wet- en regelgeving.                                      |
| <a href="http://www.mi5.gov.uk">www.mi5.gov.uk</a>                                 | Site van MI5: de veiligheidsdienst van het Verenigd Koninkrijk. Op deze site is informatie beschikbaar over dreigingen, veiligheidsadviezen, te nemen maatregelen e.d. Ook kunnen diverse brochures gedownload worden.                        |
| <a href="http://www.imo.org/home.asp">www.imo.org/home.asp</a>                     | Site van International Maritime Organization, waarop uitgebreide informatie beschikbaar is over de ISPS-Code.                                                                                                                                 |
| <a href="http://www.iso.org">www.iso.org</a>                                       | Site van ISO: International Organization for Standardization. Via het thema 'products and services' kunnen verschillende standaarden gevonden worden, zoals ook ISO 28000.                                                                    |
| <a href="http://www.niscc.gov.uk">www.niscc.gov.uk</a>                             | Site van National Infrastructure Security Co-ordination Centre (NISCC). Site behandelt dreigingen tegen de vitale infrastructuur en geeft adviezen over een betere beveiliging.                                                               |
| <a href="http://www.portsecuritytoolkit.com">www.portsecuritytoolkit.com</a>       | Site met een toolkit om de ISPS-Code te implementeren. De Toolkit voorziet in het opstellen van een risico-inschatting, een actieplan en een veiligheidsplan.                                                                                 |
| <a href="http://www.ready.gov/business">www.ready.gov/business</a>                 | Site van Homeland Security (Ministerie van Veiligheid in de Verenigde Staten). Op deze site worden bedrijven geïnformeerd over de wijze waarop zij de kans om slachtoffer te worden van een aanslag kunnen verminderen.                       |
| <a href="http://www.security.homeoffice.gov.uk">www.security.homeoffice.gov.uk</a> | Site van Ministerie van Binnenlandse Zaken van het Verenigd Koninkrijk, specifiek gericht op 'security' en 'counter-terrorism strategy'.                                                                                                      |
| <a href="http://www.tapaemea.com">www.tapaemea.com</a>                             | Site over Technology Asset Protection Association (TAPA). De site is ook in het Nederlands.                                                                                                                                                   |
| <a href="http://www.vbo-feb.be">www.vbo-feb.be</a>                                 | Site van de Vereniging van Belgische ondernemingen. Op deze site is de handreiking Terrorismen en extremisme. Welke maatregelen kunnen de bedrijven nemen? te downloaden.                                                                     |

## **BIJLAGE IV: ACHTERGRONDDOCUMENTATIE**

### ***Binnenland***

- Jaarverslag 2005, AIVD, april 2006
- 7 vragen over het Alerteringssysteem Terrorismebestrijding, NCTb, maart 2006
- De gewelddadige Jihad in Nederland: actuele trends in de islamitische-terroristische dreiging, AIVD, maart 2006
- Handreiking Terrorismebestrijding op lokaal niveau, NCTb, maart 2006
- PROTECT, Beveiliging in de logistieke keten. Een praktische aanpak, Rotterdam, december 2005
- Terrorisme tegenhouden. Drempelverhogende maatregelen voor bedrijven, Korps regiopolitie Amsterdam-Amstelland, Amsterdam, mei 2005
- Spionage en veiligheidsrisico's. Actueel, onzichtbaar en divers, AIVD en MIVD, tweede druk, juli 2005
- Leidraad Port Security, Landelijke werkgroep Post Security, maart 2005
- Communicatiehandleiding security zeehavens en zeescheepvaart, Ministerie van Verkeer en Waterstaat, augustus 2004
- Ship Security Plan, Koninklijke Vereniging van Nederlandse Reders, april 2003

95

Documenten van de landelijke overheid, zoals voortgangsrapportages aan de Tweede Kamer, kunnen via de website [www.nctb.nl](http://www.nctb.nl) worden gedownload.

### ***Buitenland***

- Terrorisme en extremisme. Welke maatregelen kunnen de bedrijven nemen? Verbond van Belgische Ondernemingen (VBO), 2005
- Protecting against terrorism, MI5 Security Service, 2005
- Every business should have a plan, Homeland Security

**BIJLAGE V: DREIGINGSNIVEAUS NEDERLAND**

| Dreigingsniveaus in het Dreigingsbeeld Terrorisme Nederland |                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Niveau                                                      | Voorbeelden van criteria                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Minimaal                                                    | <ul style="list-style-type: none"><li>• Er is amper aanwezigheid van nationale en internationale terroristische netwerken</li><li>• Het is niet waarschijnlijk dat aanslagen worden gepland</li><li>• De open samenleving en het risicokarakter van een moderne samenleving houden dit niveau in stand</li></ul>                                                                                                                                                        |
| Beperkt                                                     | <ul style="list-style-type: none"><li>• Er worden geen nieuwe trends of fenomenen onderkend</li><li>• Aanslagen blijken te kunnen worden voorkomen</li><li>• Nederland wordt niet of nauwelijks genoemd in verklaringen van serieus te nemen terroristische netwerken</li></ul>                                                                                                                                                                                         |
| Substantieel                                                | <ul style="list-style-type: none"><li>• Er worden nieuwe trends en fenomenen waar dreiging van uitgaat ontdekt</li><li>• De kans dat een aanslag in Nederland kan plaatsvinden is reëel</li><li>• Aanslagen vinden plaats in andere, met Nederland vergelijkbare landen</li><li>• Radicalisering en rekrutering vinden op aanzienlijke schaal plaats</li><li>• Nederland wordt geregeld genoemd in verklaringen van serieus te nemen terroristische netwerken</li></ul> |
| Kritiek                                                     | <ul style="list-style-type: none"><li>• Er zijn zeer sterke aanwijzingen dat een aanslag in Nederland zal plaatsvinden</li><li>• In Nederland heeft een aanslag plaatsgevonden en vervolgaanslagen zijn zeer waarschijnlijk</li><li>• Nederland wordt vaak genoemd in zeer serieus te nemen verklaringen van terroristische netwerken en specifieke doelen worden daarbij serieus bedreigd</li></ul>                                                                    |



**BIJLAGE VI: DREIGINGSSYSTEMEN**

|                      | Dreigingsbeeld Terrorisme<br>Nederland (DTN)                                                                                             | Alerteringssysteem<br>Terrorismebestrijding                                                                                                                     | Stelsel Bewaken en<br>Beveiligen                                                                                                                                          |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Doel                 | Geeft een globale analyse van de (inter)nationale terroristische dreiging tegen Nederland. De focus ligt op fenomenen en ontwikkelingen. | Geeft een beeld over een dreiging op een (vitale) bedrijfssector. Bedoeld om in geval van verhoogde dreiging maatregelen te kunnen nemen gericht op die sector. | Geeft de ernst en de waarschijnlijk van een dreiging op een object, dienst of persoon weer. Bedoeld om bij een concrete dreiging beveiligingsmaatregelen te kunnen nemen. |
| Niveaus van dreiging | <ul style="list-style-type: none"><li>• Minimaal</li><li>• Beperkt</li><li>• Substantieel</li><li>• Kritiek</li></ul>                    | <ul style="list-style-type: none"><li>• Basisniveau</li><li>• Lichte dreiging</li><li>• Matige dreiging</li><li>• Hoge dreiging</li></ul>                       | Glijdende schaal: combinatie van de waarschijnlijkheid en de ernst van de dreiging.                                                                                       |
| Dreiging geldt voor  | Nederland als geheel.                                                                                                                    | Aangesloten bedrijfssectoren.                                                                                                                                   | Personen, objecten en diensten.                                                                                                                                           |
| Maatregelen          | Het DTN is bedoeld voor het formuleren van contra-terrorismebeleid.                                                                      | Afhankelijk van het dreigingsniveau treffen de sector én de lokale en/of landelijke overheid maatregelen.                                                       | Afhankelijk van het dreigingsniveau treft de lokale en/of landelijke overheid beveiligingsmaatregelen.                                                                    |

**BIJLAGE VII: VOORBEELDEN MAATREGELN**

| Voorbeelden maatregelen van overheden en bedrijven in het Alerteringssysteem |                                                                                                                                                                                                                                                                         |                                                                                                                                                                  |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Niveau                                                                       | Soort maatregel                                                                                                                                                                                                                                                         | Voorbeelden van maatregelen door overheden en bedrijven                                                                                                          |
| Basis                                                                        | Maatregelen die horen bij 'goed huisvaderschap' en de reguliere bedrijfsvoering. Deze waarborgen de basisveiligheid en bedrijfscontinuïteit onder normale omstandigheden.                                                                                               | Bewakingspersoneel inzetten, regulier cameratoezicht, referenties van nieuw personeel natrekken.                                                                 |
| Lichte dreiging                                                              | Maatregelen die de sector en het personeel alert maken of het toezicht verscherpen en die een lichte impact hebben op de bedrijfsvoering en/of samenleving. Deze maatregelen kunnen langere tijd worden volgehouden.                                                    | Extra surveillance door politie, toezicht door eigen personeel van de sector, verhogen alertheid personeel, identificatie van bezoekers/klanten.                 |
| Matige dreiging                                                              | Deze maatregelen hebben een merkbare impact op de bedrijfsvoering en/of samenleving en kunnen een beperkte tijd worden volgehouden. Het gaat om extra alertheid en maatregelen gericht op reductie van het risico op een aanslag.                                       | Verscherpt toezicht door politie, ingangscontroles, afsluiten van terreinen en gebouwen, omleiden van verkeer, stoppen van bepaalde kritische bedrijfsprocessen. |
| Hoge dreiging                                                                | Het betreft hier zware maatregelen die een grote impact op de bedrijfsvoering en/of de samenleving hebben. Ze kunnen een korte tijd worden volgehouden. Het gaat om maatregelen die het plegen van een aanslag fysiek bemoeilijken of het effect daarvan minimaliseren. | Verbod tot betreden van bepaalde plaatsen, ontruiming, stopzetten dienstverlening, zwaar bewapende politiecontroles, grootschalige inzet van politiediensten.    |

# **COLOFON**

## **Uitgave**

Nationaal Coördinator Terrorismebestrijding (NCTb)

Den Haag

Deze handreiking is opgesteld met medewerking van onder meer AIVD, het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), Kamer van Koophandel Nederland, Nederlands Politie Instituut, Korps regiopolitie Amsterdam-Amstelland, Vereniging van Particuliere Beveiligingsorganisaties (Vpb) en Transumo/deelproject Protect, waarin deelnemen Erasmus Universiteit, TNO, Transport en Logistiek Nederland (TLN), verladersorganisatie EVO en Vereniging Nederland Distributieland (NDL/HIDC).

## **Vormgeving en ontwerp**

ARA

Rotterdam

99

## **Redactie**

Nationaal Coördinator Terrorismebestrijding (NCTb)

Toelis tekst | communicatie

Den Haag

## **Fotografie**

Ronald Koetzier

Hollandse hoogte

## **Drukwerk**

DeltaHage

Den Haag

November 2006

### **MEER INFORMATIE**

[www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)

[www.nctb.nl](http://www.nctb.nl)

### **REACTIES EN EXTRA EXEMPLAREN**

[www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)

## **BELANGRIJKE TELEFOONNUMMERS**

| Situatie in kwestie                                                        | Telefoon                                                                                       | Bijzonderheden                                                                                                                                       |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Meldingen levensbedreigende situaties en heterdaadmeldingen van misdrijven | 1-1-2                                                                                          | Alleen in spoedeisende gevallen                                                                                                                      |
| Meldingen van verdachte of ongebruikelijke handelingen                     | Plaatselijke politie:<br>0900 - 8844                                                           | Lokaal gesprekstarif                                                                                                                                 |
| Anonieme meldingen                                                         | Meld Misdaad Anoniem:<br>0800 - 7000                                                           | Van 08.00 tot 24.00 uur                                                                                                                              |
| Advies over (structurele) beveiligingsmaatregelen                          | Plaatselijke politie:<br>0900 - 8844                                                           | De politie geeft adviezen van meer algemene aard<br><br>Beveiligingsadviesbureaus kunnen bedrijven voorzien van op hun bedrijf toegespitste adviezen |
| Uitvoeren risicoanalyse                                                    | Beveiligingsadviesbureaus:<br><a href="http://www.vvbo.nl">www.vvbo.nl</a>                     |                                                                                                                                                      |
| Algemene informatie over terrorismebestrijding en bedrijven                | Nationaal Coördinator Terrorisme-<br>bestrijding: <a href="http://www.nctb.nl">www.nctb.nl</a> |                                                                                                                                                      |

**De Nationaal Coördinator Terrorismebestrijding**

