Nationaal Coördinator
Terrorismebestrijding en Veiligheid
*Ministerie van Veiligheid en Justitie*

# Handreiking terrorismebestrijding voor bedrijven

# VOORWOORD

## Dick Schoof

Jihadstrijders, mensen die naar Syrië en Irak reizen om te vechten, terrorismedreiging. U leest erover in de krant en hoort erover op radio en televisie. Ook uw bedrijf of uw medewerkers kunnen ermee te maken krijgen. Bijvoorbeeld wanneer terroristen uw bedrijf als doelwit op het oog hebben. Ook indirect kunt u de consequenties van een terroristische aanslag ondervinden, omdat uw bedrijf naast of in de omgeving van een doelwit staat. Daarnaast kunnen terroristen producten van uw bedrijf misbruiken, zoals informatie.

Deze handreiking is bedoeld voor grote én kleine bedrijven. Of u nu eigenaar of werknemer bent van een groot of klein bedrijf: het is goed dat ook u er zich bewust van bent dat u kwetsbaar kunt zijn voor terroristische dreigingen of aanslagen. En dat u weet wat u kunt of moet doen in geval van een dreiging of vermoeden van een dreiging.

Met behulp van deze handreiking kunt u nadenken hoe uw bedrijf om zou kunnen én willen gaan met terroristische dreigingen. In de volgende hoofdstukken vindt u aanknopingspunten om terrorismebestrijding in uw reguliere bedrijfsvoering of het bestaande veiligheidsbeleid in te passen.

Aandacht voor terrorisme brengt mogelijk extra maatregelen voor u mee. Gelukkig betekent dit niet altijd extra werk of extra kosten. De maatregelen verbeteren de organisatie en efficiëntie van uw bedrijf. U heeft al een belangrijke stap gezet wanneer uw personeel alert is op ongebruikelijke of verdachte activiteiten en signalen doorgeeft aan de verantwoordelijke binnen uw bedrijf. In de handreiking komen ook andere maatregelen aan de orde om de kans op een terroristische aanslag te verminderen.

Wanneer u denkt te maken te hebben met een mogelijke terroristische aanslag, of u ziet signalen die duiden op een terroristische dreiging, dan hoort de overheid dit graag. U kunt altijd contact opnemen met de plaatselijke politie. Niet alleen uw bedrijf en personeel hebben belang bij de maatregelen die u neemt. Ook voor de overheid brengt dit voordelen met zich mee. De signalen die u doorgeeft aan de politie, verbeteren de informatiepositie van de overheid. Hierdoor kan de overheid ook beter optreden bij een dreiging.

Over terrorisme en terrorismebestrijding is veel informatie beschikbaar. Aanvullende en actuele informatie kunt u vinden op de website www.nctv.nl. Natuurlijk kunt u ook altijd contact opnemen met uw brancheorganisatie.

**Dick Schoof**
*Nationaal Coördinator Terrorismebestrijding en Veiligheid*

# Inhoudsopgave


**Voorwoord** 3

**1 Inleiding** 7
1.1 Inhoud handreiking 7
1.2 Voor wie is de handreiking? 8
1.3 Nut van terrorismebestrijding door bedrijven 8
1.4 Wat mogen overheden en bedrijven van elkaar verwachten? 10

**2 Risico's en dreigingen** 13
2.1 Inleiding 13
2.2 Dreigingsbeeld Terrorisme Nederland 13
2.2.1 Dreigingsbeeld 13
2.2.2 Diffuus profiel van jihadisten en (potentiële) terroristen 14
2.2.3 Doelwitselectie 15
2.2.4 Beveiliging CBRN-stoffen 15
2.2.5 Verantwoorde verkoop chemische producten 16
2.2.6 Conclusie 17
2.3 Potentiële en concrete dreigingen 17
2.4 Herkennen van potentiële dreigingen en activiteiten 19
2.4.1 Bedrijf als potentieel doelwit 19
2.4.2 Bedrijf als potentieel middel 23
2.4.3 Kwetsbaarheid van bedrijf 24
2.5 Herkennen van concrete dreigingen 24
2.5.1 Verdachte handelingen, tijdstippen en locatie 24
2.5.2 Herkennen van radicalisering als veiligheidsrisico 26

**3 Wat kunnen bedrijven van de overheid verwachten?** 29
3.1 Inleiding 29
3.2 Landelijk 29
3.2.1 De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) 29
3.2.2 Het algemene dreigingsbeeld 32
3.2.3 Dreiging tegen een sector 33
3.3 Lokaal 36
3.3.1 Algemeen 36
3.3.2 Dreiging tegen personen, objecten of diensten 36

**4 Risicomanagement** 41
4.1 Methodiek risicoanalyse 41
4.2 Afhankelijkheidsanalyse 44
4.3 Dreigingsanalyse 45
4.4 Kwetsbaarheidsanalyse 45
4.5 Risicoanalyse 47
4.6 Kosten- en batenanalyse 49

**5 Maatregelen door bedrijven** 51
5.1 Inleiding 51
5.2 Hoe komt u tot maatregelen? 51
5.3 Welke maatregelen moet u nemen? 53
5.4 Pro-actieve maatregelen 54
5.5 Preventieve maatregelen 55
5.5.1 Inleiding 55
5.5.2 Objecten en diensten 55
5.5.3 Personeel 58

Bijlage I: verklarende woordenlijst 60
Bijlage II: afkortingenoverzicht 64
Bijlage III: relevante websites 65
Bijlage IV: dreigingsniveaus Nederland 69
Belangrijke telefoonnummers 70


Terrorisme is het uit ideologische motieven dreigen met, voorbereiden of plegen van op mensen gericht ernstig geweld, dan wel daden gericht op het aanrichten van maatschappij-ontwrichtende zaakschade, met als doel maatschappelijke veranderingen te bewerkstelligen, de bevolking ernstige vrees aan te jagen of politieke besluitvorming te beïnvloeden.

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.

# 1 Inleiding

## 1.1 Inhoud handreiking

Deze handreiking biedt een overzicht van de organisatie en het beleid van terrorismebestrijding in Nederland. De handreiking geeft ook aan hoe bedrijven aan terrorismebestrijding kunnen bijdragen.

### Doel handreiking

- inzicht geven in potentiële terroristische dreigingen voor bedrijven;
- inzicht geven in de organisatie en het beleid van terrorismebestrijding door de overheid;
- inzicht bieden in de bijdrage die bedrijven kunnen leveren aan terrorismebestrijding;
- inzicht bieden in waar bedrijven terecht kunnen met signalen en vragen.

Deze handleiding start met een hoofdstuk over de terroristische dreigingen waarmee bedrijven te maken kunnen krijgen (hoofdstuk 2). In hoofdstuk 3 komen de organisatie en het beleid van terrorismebestrijding door de internationale, Europese, nationale en lokale overheid aan de orde. Hoofdstuk 4 behandelt de wijze waarop bedrijven hun eigen risico's kunnen inschatten. Hoofdstuk 5 gaat vervolgens in op de maatregelen die bedrijven kunnen nemen om terroristische dreigingen het hoofd te bieden.

Alle onderdelen van deze handreiking zijn afzonderlijk leesbaar. Het is mogelijk te starten met hoofdstuk 2 over de dreigingen en meteen door te gaan naar hoofdstuk 5 over mogelijke maatregelen. Aanvullende informatie is beschikbaar op de website www.nctv.nl.

De bijlagen bij deze handreiking bevatten een overzicht van afkortingen, relevante documentatie, relevante websites en een overzicht van bij terrorismebestrijding betrokken organisaties. Ook geven de bijlagen aanvullende inhoudelijke informatie over maatregelen en de dreigingsniveaus. Terrorismebestrijding vormt een snel veranderend beleidsterrein. Actuele informatie is te vinden op de website www.nctv.nl.

## 1.2 Voor wie is de handreiking?

De handreiking is bedoeld voor alle bedrijven. Voor grotere en kleinere bedrijven kan de handreiking aanleiding zijn om na te denken over terroristische dreigingen en wat deze dreiging betekent voor hun bedrijf. Bedrijven kunnen op diverse manieren te maken krijgen met terroristische dreigingen of aanslagen. In hoofdstuk 2 komen de dreigingen voor bedrijven uitvoerig aan bod.

Het ene bedrijf loopt meer risico op een terroristische dreiging dan het andere. Sommige bedrijven die risico lopen zijn hiermee al bekend. Zij handelen daar ook naar. Dit geldt bijvoorbeeld voor bedrijven die aangesloten zijn bij het Alerteringssysteem Terrorismebestrijding (Atb, zie hoofdstuk 3) zoals de waterleidingsbedrijven, banken en vervoersbedrijven. Andere bedrijven realiseren zich niet dat zij interessant zijn voor terroristen. Juist voor hen is deze handreiking relevant. Op basis van de informatie in deze handreiking kunnen bedrijven te weten komen of zij maatregelen moeten treffen.

## 1.3 Nut van terrorismebestrijding door bedrijven

De kosten voor het bevorderen van de veiligheid van goederen, diensten en personeel zijn voor de bedrijven zelf. Bedrijven moeten zelf de afweging maken of de kosten om de risico's te beperken opwegen tegen de baten. Er zijn diverse voordelen verbonden aan het inpassen van terrorisme-bestrijding in de reguliere bedrijfsvoering of het reguliere (veiligheids) beleid van een bedrijf.

**Vijf redenen voor terrorismebestrijding door bedrijven:**

1. bedrijfscontinuïteit / voorkomen economische schade
2. verbetering imago
3. wettelijke verplichtingen
4. investeren in terrorismebestrijding = investeren in criminaliteitsbestrijding
5. betere informatievoorziening

Als uw bedrijf bedacht is op een mogelijke terroristische aanslag, dan is de kans aanwezig dat de bedrijfscontinuïteit beter is gegarandeerd. Bijvoorbeeld omdat back up-bestanden ergens anders worden bewaard. De kans op economische schade is dan ook minder. Aandacht voor terrorisme-bestrijding kan ook leiden tot een beter imago. Klanten doen waarschijnlijk sneller zaken als zij weten dat hun goederen veilig zijn. Aandacht voor terroristismebestrijding heeft niet alleen positieve gevolgen voor individuele bedrijven. Het kan ook het imago van het gehele Nederlandse bedrijfsleven versterken. Dat heeft weer positieve gevolgen voor de concurrentiepositie van individuele bedrijven. Daarnaast is het mogelijk dat sommige buitenlandse overheden of bedrijven uw onderneming verplichten tot bepaalde maatregelen. Alleen dan doen zij zaken. Aan dergelijke verplichtingen zijn ook voordelen verbonden, bijvoorbeeld een beperktere controle op de lading.

Investeren in terrorismebestrijding betekent ook investeren in criminaliteitspreventie én omgekeerd. Veel maatregelen in het kader van terrorismebestrijding liggen in het verlengde van het bestaande veiligheids-beleid of de reguliere bedrijfsvoering. Toch bestaan er ook verschillen tussen de bestrijding van criminaliteit en terrorisme. Bij terrorisme gaat het om maatschappelijke ontwrichting en niet om geldelijk gewin zoals bij criminaliteit. Bij terrorismebestrijding moet een bedrijf niet alleen letten op de kansen die er zijn voor criminelen om toe te slaan. Ook het te verwachten effect speelt een rol. U slaat dus twee vliegen in één klap.

De investering in terrorismebestrijding hoeft niet altijd kosten met zich mee te brengen. Soms levert het ook baten op. Zo leiden organisatorische of informatietechnische maatregelen tot efficiënter werken. Een laatste voordeel is de informatie¬voorziening van de overheid naar bedrijven toe. Wanneer bedrijven alert zijn op verdachte zaken en deze signaleren bij de lokale autoriteiten, ontstaat een beter beeld van dreigingen. De overheid kan daardoor bedrijven gerichter informeren en eventueel de kans op een aanslag verminderen. Dat is in het belang van iedereen.

## 1.4 Wat mogen overheden en bedrijven van elkaar verwachten?

Nederland is een risicomaatschappij; gevaren zoals terroristische dreigingen en aanslagen zijn niet uit te sluiten. Het is wel mogelijk de kans erop te verminderen. Dat vraagt om adequaat optreden van de publieke én private sector. De overheid is verantwoordelijk voor de veiligheid in het publieke domein. In hoofdstuk 3 leest u wat de overheid doet om de veiligheid in het publieke domein te waarborgen. Bedrijven zijn verantwoordelijk voor de veiligheid van hun goederen, diensten en personeel. Dat betekent dat bedrijven zelf maatregelen moeten nemen om hun eigendommen en personeel te beschermen. U kunt dit eventueel in samenspraak met de politie doen.

Er is dus sprake van een gezamenlijke verantwoordelijkheid van de publieke en private sector. Juist daarom moeten bedrijven en overheden erop kunnen vertrouwen dat de ander in geval van een dreiging ook daadwerkelijk maatregelen neemt. Op enkele gebieden, zoals vervoer, zijn bedrijven dat wettelijk verplicht. Voor de andere terreinen geldt deze verplichting niet. Toch kan de overheid bedrijven aanspreken op hun inspanning. Dat geldt zeker wanneer de overheid afhankelijk is van bedrijven om het gewenste veiligheidsniveau te bereiken. Wanneer bedrijven geen acties ondernemen bij een dreiging, kan de overheid ook de veiligheid niet garanderen. Samenwerking is daarom van belang. Op alle niveaus, maar in het bijzonder op het lokale niveau tussen bedrijven en politie. De maatregelen die bedrijven kunnen treffen, leest u in hoofdstuk 5.

**Wat mogen overheid en bedrijfsleven van elkaar verwachten?**

Het bedrijfsleven mag van de overheid verwachten:
- dat de overheid bedrijven voorziet van voldoende informatie (algemene en concrete dreigingen);
- dat de overheid ondersteuning levert door onder meer te zorgen voor goede infrastructuur;
- in geval van een terroristische dreiging of aanslag: dat crisismanagementsystemen en (crisis) besluitvormingsprocessen effectief en efficiënt werken.

De overheid mag van het bedrijfsleven verwachten:
- dat zij een bijdrage levert aan het bevorderen van veiligheid, inclusief het treffen van maatregelen als daarvoor een noodzaak is;
- dat bedrijven signalen doorgeven aan de lokale autoriteiten wanneer sprake is van verdachte handelingen of activiteiten.

Sinds het afgelopen decennium is de terroristische dreiging in Nederland afkomstig van jihadisten: extremistische gelovigen die gericht geweld bepleiten en inzetten om hun doelen te bereiken.


# 2 Risico's en dreigingen

## 2.1 Inleiding

In dit hoofdstuk komt het dreigingsbeeld voor Nederland aan de orde en leest u hoe u terroristische dreigingen en activiteiten kunt herkennen.

Het dreigingsbeeld van Nederland wordt elk kwartaal vastgesteld in het Dreigingsbeeld Terrorisme Nederland (DTN, zie paragraaf 2.2).
De onderstaande paragrafen geven een korte schets van de trends en ontwikkelingen in de terroristische dreiging. Dit is ook relevant voor bedrijven, want het helpt u om mogelijk terroristische dreigingen en activiteiten in een bredere context te plaatsen.

In het tweede gedeelte van dit hoofdstuk staan de aantrekkelijkheid en kwetsbaarheid van bedrijven voor terrorisme centraal. De aantrekkelijkheid van een bedrijf voor terrorisme hangt mede af van de mate waarin terroristen door een aanslag hun doelen kunnen bereiken. De kwetsbaarheid is onder meer afhankelijk van de wijze waarop een bedrijfspand is gebouwd (intrinsieke weerstand), zoals een sterk betonnen gebouw met weinig glas. Daarnaast is de beveiliging van invloed op de kwetsbaarheid. Aan de hand van de aantrekkelijkheid en de kwetsbaarheid is het mogelijk een inschatting te maken van de potentiële dreiging. In paragraaf 2.3 wordt hierop nader ingegaan.

## 2.2 Dreigingsbeeld Terrorisme Nederland

### 2.2.1 Dreigingsbeeld

Het algemene dreigingsniveau voor terrorisme in Nederland staat sinds maart 2013 op het niveau *substantieel* [1]. 'Substantieel' betekent dat de kans reëel is dat in Nederland een aanslag zal plaatsvinden. Deze kans op een aanslag is niet gelijkmatig gespreid over Nederland, en is ook niet zonder meer te specificeren naar een gebied of locatie.

1 IJkdatum***

De belangrijkste vorm van terroristische dreiging waar Nederland mee te maken heeft, is het *jihadisme* (als vorm van politiek-religieus terrorisme). Sinds het afgelopen decennium is de terroristische dreiging in Nederland afkomstig van jihadisten: extremistische gelovigen die gericht geweld bepleiten en inzetten om hun doelen te bereiken.

De verhoogde terrorismedreiging komt door enkele belangrijke nationale én internationale ontwikkelingen. Ten eerste is er de grote stijging in het aantal 'jihadgangers'. Vanaf eind 2012 signaleerden de AIDV en andere veiligheidsdiensten dat steeds meer – vooral jonge – moslims naar landen in het Midden-Oosten en Afrika trokken om zich daar aan te sluiten bij jihadistische strijdgroepen. De vrees bestaat dat zij met hun ideologische gedrevenheid en praktische gevechtservaring bij terugkeer ingezet kunnen worden voor het plegen van aanslagen. Ook kunnen zij in Nederland anderen radicaliseren en aanzetten tot jihadgang. Daarnaast zijn er nog altijd signalen dat kleine groepen jongeren in Nederland in snel radicaliseren. Ook blijft Nederland in de ogen van jihadisten een legitiem doelwit, omdat ons land wordt gezien als bondgenoot van de Verenigde Staten en Israël. De recente Nederlandse deelname aan de militaire missie tegen ISIS in Irak (2014) draagt naar alle waarschijnlijkheid verder aan dit beeld van ons land bij.

### 2.2.2 Diffuus profiel van jihadisten en (potentiële) terroristen

Inmiddels zijn er al ongeveer honderdvijftig mensen uit Nederland vertrokken om in het Midden-Oosten of Afrika te vechten voor de jihad. Sommigen zijn gedood in de strijd, enkele tientallen keerden terug. Hoewel niet van elke teruggekeerde jihadist een dreiging uitgaat, moeten we ermee rekening houden dat dergelijke personen niet alleen zijn geradicaliseerd, maar ook getraumatiseerd en in hoge mate bereid zijn tot geweld. Daarnaast kan ook van tegengehouden jihadreizigers een dreiging uitgaan. De huidige groep jihadisten bestaat grotendeels uit jonge mannen en vrouwen van verschillende nationaliteiten. Zij zijn meestal tussen de 16-35 jaar oud en vaak in Nederland geboren. Het gaat om tweede en derde generatie islamitische allochtonen én bekeerlingen. Hun (zelf) radicalisering vindt vaak plaats op het internet, zonder directe individuele aansturing van anderen. Hierdoor zijn veel van de bestaande jihadistische individuen en netwerken anarchistisch van aard. Deze huidige generatie jihadisten richt zich nadrukkelijker dan eerdere generaties (buitenlandse) jihadisten tegen Nederland.

### 2.2.3 Doelwitselectie

Traditionele doelwitten voor jihadisten zijn objecten die symbool staan voor een specifiek land of regering die zij als 'anti-islamitisch' zien, zoals ambassades en regeringsgebouwen. Dit zijn de zogenaamde 'hard targets'. In de afgelopen jaren zijn ook 'soft targets' in toenemende mate doelwit. Dit zijn locaties en objecten die een publieke functie hebben en daardoor moeilijk te beveiligen zijn, zoals, musea, hotels en stations. Met aanslagen op dergelijke doelwitten treffen terroristen de burgerbevolking die zij medeverantwoordelijk houden voor de vermeend anti-islamitische daden van hun regering. Daarnaast zijn ook delen van de vitale infrastructuur, zoals bruggen en tunnels, doelwit van terrorisme. Tot slot richten terroristen hun aandacht ook op individuele personen.

### 2.2.4 Beveiliging CBRN-stoffen

Chemische, biologische, radiologische en nucleaire (CBRN) stoffen zijn voor jihadisten en andere kwaadwillenden interessante middelen om een aanslag mee te plegen. Een grote CBRN-aanslag is niet waarschijnlijk, maar ook een weinig effectieve aanslag met CBRN-stoffen of een poging daartoe kan leiden tot grote maatschappelijke onrust. Denk hierbij aan poederbrieven of verspreiding van giftige stoffen.

Daarom is het belangrijk dat CBRN-stoffen goed beveiligd zijn en dat signalen die wijzen op kwaadwillende bedoelingen herkend worden. Bedrijven en publieke instellingen die werken met CBRN-stoffen, zoals zorginstellingen, universiteiten of chemische industrie, spelen hierin een grote rol. Zij zijn namelijk verantwoordelijk voor een goede beveiliging en veiligheidsbewustzijn binnen hun eigen organisatie.

De NCTV en de betrokken ministeries hebben samen met een groot aantal instellingen een pakket instrumenten ontwikkeld om CBRN-instellingen te ondersteunen bij het nemen van maatregelen om hun weerstand te verhogen, van planning tot en met evaluatie. Het gaat om de volgende instrumenten: ·

- Beveiliging op de agenda zetten
- Beveiliging analyseren en maatregelen voorbereiden

- Medewerkers screenen
- Security awareness vergroten
- Beveiliging beoefenen en evalueren

**Meer informatie ondersteuning CRBN-instellingen**

- De instrumenten, extra achtergronddocumenten en nuttige links vindt u op de site van de NCTV: http://www.nctv.nl/onderwerpen/tb/Tools/beveiligingcbrnstoffen/
- Wilt u meer informatie of in contact komen met instellingen die al beveiligingsmaatregelen genomen hebben? Neem dan contact op met de NCTV via cbrn@nctv.minvenj.nl.

### 2.2.5 Verantwoorde verkoop chemische producten

Sommige producten met chemicaliën kunnen, naast hun normale toepassingen, ook misbruikt worden door criminelen. Terroristen gebruiken deze stoffen bijvoorbeeld om zelf explosieven te maken. Het is dus belangrijk deze stoffen op een verantwoorde wijze te verkopen.

Op http://www.nctv.nl/onderwerpen/tb/Tools/index/ vindt u uitgebreide informatie over de nieuwe regels rond verkoop van chemische producten. Ook is op de website een folder en poster beschikbaar. Hieronder kunt u de hoofdlijnen lezen over de regels rond verkoop van chemische producten.

**Verdachte transacties melden**

- U kunt in Nederland 24/7 per telefoon verdachte transacties, verdwijningen en diefstal van chemische producten melden bij het Meldpunt Verdachte Transacties Chemicaliën via: 088 154 00 00
- Maandag t/m vrijdag 9.00-17.00 kunt u ook melden via precursoren@belastingdienst.nl. Bij dit meldpunt kunt u ook terecht voor meldingen van verdachte transacties van grondstoffen voor drugs en chemische wapens.



### 2.2.6 Conclusie

De jihadistische dreiging is complex. Zij kan vanuit vele hoeken komen en zich richten tegen vele doelwitten. Bovendien maken terroristen gebruik van veel verschillende middelen. Deze complexiteit maakt het lastig om een dreiging jegens individuele objecten in te schatten. Bovendien willen terroristen verrassen. Zij doen hun best om op een ongebruikelijke manier toe te slaan en beveiligingsmaatregelen te omzeilen.

Voor bedrijven betekent dit dat het goed is om steeds op de hoogte te blijven van de actuele, algemene dreiging. Dat geldt ook voor de dreigingen die specifiek gericht zijn op bedrijven. De volgende paragraaf gaat daarop in.

## 2.3 Potentiële en concrete dreigingen

Soms zijn er aanwijzingen dat een bedrijf daadwerkelijk geconfronteerd wordt met terroristische dreigingen. Er is dan sprake van een concrete dreiging. Een *concrete* dreiging heeft doorgaans betrekking op het bedrijf als *doelwit*. Het kan ook zijn dat het bedrijf dient als *middel* dat misbruikt kan worden. In dat geval is de precieze intentie van terroristen vastgesteld of zijn voorbereidende terroristische handelingen geconstateerd. Als dergelijke aanwijzingen niet aanwezig zijn, maar beredeneerd kan worden dat een bedrijf wel *aantrekkelijk* is voor terroristen, dan is sprake van een potentiële dreiging.

Naast het scenario waarbij een bedrijf een *doelwit* of *middel* is van terroristen, kan een bedrijf ook op andere manieren te maken krijgen met terrorisme. Zo kan een bedrijf worden getroffen door *uitstralingseffecten* van een terroristische aanslag of *radicaliserend personeel* in dienst hebben.

**Bedrijven kunnen op vier manieren te maken krijgen met een dreiging van terrorisme:**

- **Doelwit:** een bedrijf wordt doelbewust getroffen door een aanslag omdat het aan bepaalde eigenschappen voldoet.
- **Middel/misbruik:** sommige bedrijven beschikken over informatie, producten of diensten die terroristen kunnen gebruiken voor de voorbereiding en uitvoering van een terroristische aanslag.
- **Schadelijke uitstralingseffecten van een aanslag:** een bedrijf staat in de buurt van een doelwit van een terroristische aanslag of is (deels) afhankelijk van het bedreigde bedrijf. Dit zorgt mogelijk voor fysieke of economische nevenschade.
- **Radicaliserend personeel:** soms zijn er aanwijzingen, bijvoorbeeld door uitingen en gedrag, dat personeelsleden aan het radicaliseren zijn. Dit kan betekenen dat ze bereid zijn terroristische activiteiten goed te keuren, te ondersteunen of uit te voeren.

### Potentiële dreiging: voorstelbaar dat een dreiging bestaat

Van een potentiële terroristische dreiging voor een bedrijf is sprake als terroristen het bedrijf aantrekkelijk vinden als doelwit of middel. Om te bepalen of dat het geval is, kan een zogeheten aantrekkelijkheidsprofiel helpen om de ernst van de dreiging inzichtelijk te maken. Dat profiel is op te stellen met behulp van informatie over terroristische aanslagen uit het verleden en/of uit strategiedocumenten van terroristische groepen. Hoe duidelijker het aantrekkelijkheidsprofiel is, en hoe meer het overeenkomt met de eigenschappen van een bedrijf, hoe voorstelbaarder de dreiging van een aanslag of de mogelijkheid van misbruik.

Wanneer een bedrijfsprofiel en een aantrekkelijkheidsprofiel overeenkomen, betekent dat zelden zekerheid over het risico. Het aantrekkelijkheidsprofiel is immers opgesteld op basis van informatie uit het verleden. Terroristen veranderen hun werkwijze continu. Daarnaast zijn profielen veelal tijdgebonden en kunnen plotseling wijzigen. Toch biedt een vergelijking tussen een bedrijfsprofiel en een aantrekkelijkheidsprofiel wel enig houvast. De elementen van het aantrekkelijkheidsprofiel worden in de volgende paragraaf behandeld. De elementen die de kwetsbaarheid van een bedrijf bepalen, komen in paragraaf 2.4.3 aan bod.



### Concrete dreiging: aanwijzingen dat een dreiging bestaat

Van een concrete dreiging is sprake als er informatie is die erop wijst dat terroristen daadwerkelijk van plan zijn om een aanslag te plegen of misbruik te maken van een bedrijf. Hoe duidelijker en specifieker de informatie, hoe concreter (voorspelbaarder) de dreiging. Dit vergemakkelijkt ook de keuze van de te nemen maatregelen.

Een concrete dreiging kan blijken uit informatie bij politie en inlichtingendiensten over (potentiële) aanslagplegers. Bij concrete informatie onderneemt de overheid altijd actie (zie hoofdstuk 3). Een concrete dreiging kan ook blijken uit informatie over een bepaald doelwit. Het gaat dan om signalen (gebeurtenissen, gedrag) rond een bedrijf waaruit afgeleid kan worden dat terroristen bezig zijn om een aanslag voor te bereiden. Bedrijven kunnen dergelijke aanwijzingen doorgeven aan de politie. Soms hebben de overheid en het bedrijfsleven geen duidelijke dreigingsinformatie, maar wel informatie die, bij elkaar gebracht, leidt tot bruikbare dreigingsinformatie. In hoofdstuk 3 komen de signalen aan de orde die relevant zijn om door te geven aan de politie (paragraaf 3.3.2).

## 2.4 Herkennen van potentiële dreigingen en activiteiten

Omdat de sterkste dreiging momenteel uitgaat van jihadistische terroristen, gaat hier in onderstaande paragrafen de meeste aandacht naar uit.

### 2.4.1 Bedrijf als potentieel doelwit

Bij jihadistische terroristen spelen globaal vijf elementen een rol in hun doelwitkeuze. Deze elementen hebben te maken met effecten die zij kunnen/willen bereiken: (1) het maken van zoveel mogelijk slachtoffers, (2) het veroorzaken van een zo hoog mogelijke economische schade, (3) het veroorzaken van rampzalige effecten, (4) het treffen van bepaalde maatschappelijke waarden/beleid, en (5) het veroorzaken van maatschappelijke onrust. De mate waarin deze effecten te bereiken zijn bij een aanslag op een bedrijf, geeft zicht op het aantrekkelijkheidsprofiel van dat bedrijf.

## Slachtoffers

Jihadisten waarschuwen zelden tot nooit voorafgaand aan een specifieke aanslag. Daarmee vergroten ze de kans op een groot aantal slachtoffers. Jihadisten willen hiermee een maximaal effect van afschrikking bereiken. Daarmee kunnen ze maatschappelijke en politieke processen beïnvloeden[2].
De volgende eigenschappen van bedrijven vergroten de kans op een groot aantal slachtoffers:

- **Concentraties van mensen:** denk aan winkelcentra, stadions, concerten, bioscopen, horeca, bedrijven op luchthavens en treinstations.
- **Specifieke omstandigheden die de dodelijkheid van een aanslag vergroten:** de hoogte en snelheid van doelwit (= 'crashfactor'), de aanwezigheid van veel materiaal in de omgeving dat kan branden of als rondvliegend gruis kan dienen (bijv. glas).
- **Problematische toegankelijkheid voor hulpverlening:** ondergrondse (tunnels) of hooggelegen locaties, locaties op het water of in de lucht.

## Economische schade

Het toebrengen van economische schade aan individuele bedrijven én landen als geheel is voor terroristen niet alleen een manier van wraak gericht op de westerse welvaart, maar ook een methode om de slagkracht en prioriteitstelling van landen te beïnvloeden. De aandacht verschuift dan immers naar de binnenlandse economische problemen.
De kans op economische schade stijgt als de aanslag plaatsvindt op een doelwit:

- waardoor de marktprijs van een noodzakelijke dienst of goed (zoals energie) sterk en/of langdurig stijgt;
- waardoor een goed of dienst niet beschikbaar is terwijl de samenleving daarvan afhankelijk is (bijvoorbeeld cybersecurity, of de uitval van vitale diensten en infrastructuur waarvan andere productieprocessen afhankelijk zijn);
- dat op zichzelf staand erg kostbaar is, bijvoorbeeld een aanslag op grootschalige infrastructuur.

## Calamiteuze effecten

Een calamiteus effect kan optreden wanneer een relatief kleine aanslag op een bedrijf grote gevolgen heeft voor de (directe) omgeving, bijvoorbeeld vanwege:

- 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.

## Maatschappelijke waarden en beleid

Sommige bedrijven kunnen vanwege hun bezigheden of imago rekenen op afkeuring van terroristen. Dit zijn bedrijven die in de ogen van terroristen model staan voor vermeend anti-islamitische waarden en activiteiten, zoals:

- Bedrijven met een specifieke 'nationaliteit' vanwege hun verbondenheid met het 'anti-islamitisch' beleid van een overheid. De verbondenheid kan ontstaan door (persoonlijke) banden tussen bijvoorbeeld een bedrijf en een regering, of doordat een bedrijf specifieke diensten of goederen zoals wapens levert aan die 'anti-islamitische' overheid. Een overheid kan als 'anti-islamitisch' gezien worden wanneer zij betrokken of aanwezig is bij een militair conflict in islamitische landen. De lijst van 'anti-islamitische' landen en de volgorde verandert continue. Op basis van onder meer openbare dreigementen van jihadistische groepen behoren in ieder geval de Verenigde Staten, het Verenigd Koninkrijk, Israël en Australië tot de 'anti-islamitische' landen. Hoe meer het bedrijf kan worden geassocieerd met de politiek of de leiders van deze landen, hoe hoger het aantrekkelijkheidsprofiel.
- Bedrijven die goederen of diensten produceren en/of verlenen die jihadisten als 'verboden' beschouwen. Bijvoorbeeld objecten die staan voor de consumptie en verkoop van onder andere alcohol, en goederen en diensten die in relatie staan tot de seksuele moraal.

2 Zoals de Spaanse landelijke verkiezingen in 2004 die kort na de aanslagen op de treinen plaatsvond.

**Een bedrijf heeft een hoger aantrekkelijkheidsprofiel wanneer:**

- veel slachtoffers mogelijk zijn;
- er grote economische schade kan worden veroorzaakt;
- calamiteuze effecten kunnen worden veroorzaakt;
- het wordt gezien als vertegenwoordiger of verlengstuk van (vermeende) anti-islamitische waarden en beleid;
- maatschappelijke onrust kan worden versterkt.

### Maatschappelijke onrust

Veroorzaken van maatschappelijke onrust is een van de doelen die terroristen met een aanslag op een bedrijf kunnen nastreven. Hier is overigens niet altijd een aanslag voor nodig; maatschappelijke onrust kan ook ontstaan als gevolg van een dreiging die grote angst doet ontstaan. Dit gebeurt met name als de potentiële dreigingen:

- zich richten op een doel waarbij bij voorbaat sprake is van een problematische hulpverlening, bijvoorbeeld bij moeilijk toegankelijke locaties;
- zich richten op een doel waarbij bij de slachtoffers een gevoel van afhankelijkheid/hulpeloosheid kan ontstaan omdat zij niet kunnen ontsnappen, zoals in een vliegend vliegtuig en rijdende trein;
- zich zo manifesteren dat het gevaar (aanslagmiddel) onzichtbaar is, bijvoorbeeld door het gebruik van CBRN-middelen[3], zoals een mogelijke voedselvergiftiging;
- zich richten op specifieke categorieën slachtoffers, zoals kinderen en bejaarden.

3 Chemische, Biologische, Radiologische of Nucleaire middelen.



## 2.4.2 Bedrijf als potentieel middel

Terroristen kunnen bedrijven misbruiken voor de voorbereiding en uitvoering van hun aanslagen. Het gaat daarbij om informatie, goederen of diensten die bruikbaar zijn voor de selectie en verkenning van doelwitten. Ook kunnen terroristen producten misbruiken om een aanslag te plegen (bijvoorbeeld kunstmest als grondstof voor een zelfgemaakte bom). Voor het beoordelen van het risico op gebruik en misbruik van bedrijven zijn diverse elementen van belang:

- **De locatie van het bedrijf:**
  - vlakbij een potentieel doelwit.
- **De kennis/informatie van een bedrijf over:**
  - aanslagmiddelen zoals 'recepten' voor het vervaardigen van wapens en explosieven;
  - potentiële doelwitten, zoals de adresgegevens van belangrijke politici;
  - kwetsbaarheidsgegevens, zoals de beveiliging van potentiële doelwitten.
- **De toegang tot doelwitten vanuit het bedrijf,** bijvoorbeeld het verrichten van onderhouds-, schoonmaak- of beveiligings-werkzaamheden voor potentiële doelwitten.
- **De middelen, goederen en diensten van het bedrijf die terroristen helpen bij het voorbereiden van aanslagen, zoals:**
  - **onderdak** (bijvoorbeeld (huur)woningen, hotelkamers, vakantiehuisjes en logeeradressen);
  - **financiële diensten** (bijvoorbeeld het omwisselen, ontvangen en verzenden van geld);
  - **communicatiemiddelen** (bijvoorbeeld het aanbieden van (mobiele) telefonie en internet in belhuizen en internetcafés);
  - **verkenningsmiddelen** (bijvoorbeeld survivaluitrustingen, elektronica, verrekijkers etc.);
  - **aanslagmiddelen** (bijvoorbeeld explosieven en grondstoffen daarvoor). Voor terroristen aantrekkelijke bedrijven zijn technologische centra, ziekenhuizen, chemische centra, apotheken, drogisterijen, tuincentra en bouwmarkten.

### 2.4.3 Kwetsbaarheid van bedrijf

Terroristen streven naar een zo groot mogelijke kans op succes voor hun activiteiten, met name bij aanslagpogingen en het verwerven van middelen. Beveiligingsmaatregelen die de kans op succes verkleinen, kunnen er dus toe leiden dat terroristen besluiten een bepaald doelwit niet te kiezen. Daarom zijn onder meer de volgende elementen van belang voor terroristen:

- **gemakkelijke toegankelijkheid van een doelwit,** door weinig of geen beveiliging (inclusief cybersecurity);
- **vaste routines** zoals vaste routes met vaste tijdstippen die zich verplaatsende doelwitten afleggen, waardoor terroristen veel houvast hebben bij het plannen van hun activiteiten zoals een aanslag;
- **bedrijven met veel externen waaronder bezoekers** waardoor terroristen makkelijk onopgemerkt op kunnen gaan in de massa.

## 2.5 Herkennen van concrete dreigingen

### 2.5.1 Verdachte handelingen, tijdstippen en locatie

Om signalen voor concrete dreigingen te kunnen opmerken, is het nodig te weten wat verdachte handelingen zijn. Dit zijn handelingen die niet in het normale plaatje passen. Bedrijven die heldere procedures hebben en deze naleven (orde/netheid/controle), maken het voor zichzelf makkelijker om afwijkingen te constateren. Maar voorbereidingshandelingen voor terrorisme, zoals verkennen van een doelwit, kunnen over langere periode plaatsvinden en vallen daardoor niet altijd makkelijk op.

Bij verdachte handelingen hoeft niet altijd direct sprake te zijn van voorbereidingen voor een terroristische of criminele activiteit. Er bestaan geen checklisten om de afwijking van het normale direct de juiste betekenis te geven. Hieronder leest u een indicatieve, maar niet uitputtende lijst met aanwijzingen voor (voorbereidingen) van terroristische activiteiten. Daarbij is het van belang deze steeds af te zetten tegen de normale situatie en de context te bekijken. De kans dat een signaal wijst op iets verdachts is groter als er sprake is van een combinatie van signalen. Bij mogelijke verdachte handelingen is contact met de lokale politie aan te raden.

**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.

**Verdachte handelingen:**

- Handelingen die raken aan de beveiliging van een bedrijf:
  - aandacht/interesse voor de beveiliging;
  - vastleggen van de (beveiligings)situatie van een bedrijf: fotograferen, filmen, notuleren;
  - diefstal van bedrijfslegitimatiebewijzen, -kleding en -voertuigen;
  - testen van de beveiliging
  - cybersecurity.
- Handelingen waarbij iemand zijn/haar identiteit of handelingen probeert af te schermen in contact met een bedrijf:
  - geen legitimatiemogelijkheden: legitimatie afwezig of vals;
  - geen contactgegevens van of toegang tot een persoon (zoals een telefoonnummer of een adres);
  - betalingen van (grote) bedragen in contanten, met vals geld, of met gestolen betaalkaarten.
  - Stelen van identiteit via cyber
- (Digitale) Pogingen tot het verkrijgen van kennis en goederen geschikt voor (de voorbereiding van) een aanslag:
  - interesse in dergelijke kennis en goederen;
  - aanschaf en diefstal van dergelijke kennis en goederen.

**Verdachte momenten:**

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

**Gevoelige locaties:**

- locaties in de nabijheid of met zicht op potentiële doelwitten;
- beveiligde locaties;
- locaties waar eindcontroles plaatsvinden (bijvoorbeeld in de voedings-middelenindustrie: een vergiftiging na de eindcontrole zal niet meer worden opgemerkt);
- locaties waar zich informatie of middelen bevinden die geschikt of nodig zijn bij het plegen of voorbereiden van een aanslag.

### 2.5.2 Herkennen van radicalisering als veiligheidsrisico

Een radicaliserend personeelslid kan een toekomstige dreiging vormen als hij bereid is steun te verlenen aan terroristische aanslagen of deze uit te voeren. Informatie over radicalisering op de werkvloer kan leiden tot de ontdekking van activiteiten die mogelijk te relateren zijn aan de voorbereiding en uitvoering van aanslagen. Radicalisering is een proces dat heel snel, maar ook heel geleidelijk kan plaatsvinden. Medewerkers die radicaliseren, kunt u herkennen aan het volgende gedrag:

- het voorhanden hebben of opzoeken (via internet van het bedrijf) van extremistische literatuur, pamfletten, geluids- en gegevensdragers. Dit kan lastig te beoordelen zijn, zeker bij islamitische radicalisering omdat vaak sprake is van een andere taal, zoals Arabisch;
- interesse in fysieke trainingsfaciliteiten zoals gevechtssporten;
- goedkeurende signalen ten aanzien van terroristische aanslagen;
- reizen naar regio's of landen waarvan bekend is dat daar terroristische trainingskampen bestaan of waar een terroristisch conflict speelt; denk aan Syrië of Irak, Jemen, Tsjetsjenië, Kasjmir, Pakistan, Somalië etc;
- een plotselinge afkeer van 'westerse gewoonten' zoals gemengde activiteiten (man/vrouw), het drinken van alcohol etc. en onverdraagzaamheid op dit vlak tegenover anderen;
- het dragen van specifieke kleding en symbolen of juist de plotselinge wisseling van kleding.

Voor het schetsen van een accuraat beeld van terroristische dreigingen is informatie van gemeenten, politie en bedrijven nodig.

# 3 Wat kunnen bedrijven van de overheid verwachten?

## 3.1 Inleiding

Overheden proberen de kans op terroristische dreigingen en aanslagen te verminderen. Op internationaal, Europees, landelijk en lokaal niveau stellen zij wet- en regelgeving op, of maken beleid. In dit hoofdstuk komen deze overheidsactiviteiten aan de orde.

## 3.2 Landelijk

### 3.2.1 De Nationaal Coördinator Terrorismebestrijding en Veiligheid

De Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) beschermt Nederland tegen bedreigingen die de maatschappij kunnen ontwrichten. Samen met zijn partners binnen overheid, wetenschap en bedrijfsleven zorgt de NCTV ervoor dat de Nederlandse vitale infrastructuur veilig is én blijft.

Sinds de oprichting van de NCTV is er binnen de Rijksoverheid één organisatie verantwoordelijk voor terrorismebestrijding, cyber security, nationale veiligheid en crisisbeheersing. Samen met zijn partners uit het veiligheidsdomein maakt de NCTV zich sterk voor een veilig en stabiel Nederland. De focus ligt op het voorkomen en beperken van maatschappelijke ontwrichting. Daarnaast neemt de NCTV maatregelen om de gevolgen van eventuele aanslagen te beperken.

De NCTV heeft de volgende hoofdopdrachten:
- duiden en reduceren van geïdentificeerde dreigingen;
- bewaken en beveiligen van personen, objecten, diensten en evenementen, alsmede vitale sectoren;
- zorgdragen voor cyber security;
- versterken van de weerbaarheid van objecten, personen, structuren en netwerken;
- optimale crisisbeheersing en crisiscommunicatie.

De NCTV bekijkt terroristische dreigingen vanuit drie invalshoeken:
- de algemene dreiging voor Nederland;
- een dreiging tegen (vitale) bedrijfssectoren;
- een dreiging tegen een object, dienst of persoon.

Voor elke invalshoek heeft de NCTV een systeem ontwikkeld om tijdig het beleid te kunnen aanpassen of maatregelen te treffen. De eerste twee systemen worden behandeld in deze paragraaf. Het stelsel Bewaken en Beveiligen in paragraaf 3.3.

### Drie systemen om met een terroristische dreiging om te gaan

| | |
|---|---|
| Dreigingsbeeld Terrorisme Nederland (DTN) | Het DTN geeft de (potentiële) dreiging voor Nederland weer. Het DTN is bedoeld voor het formuleren van het contra-terrorismebeleid. |
| Alerteringssysteem Terrorismebestrijding (ATb) | Dit systeem is gericht op de dreiging voor (vitale) bedrijfssectoren. Op basis van dit systeem worden maatregelen genomen door bedrijfssectoren en de overheid. |
| Stelsel Bewaken en Beveiligen | Dit stelsel is gericht op een dreiging voor een object, dienst of persoon. Op basis van dit systeem neemt de overheid concrete beveiligingsmaat-regelen. |

| | Dreigingsbeeld Terrorisme Nederland | Alerteringssysteem Terrorismebestrijding | Stelsel Bewaken en Beveiligen |
|---|---|---|---|
| Doelgroep | Overheid: bestuurders en beleidsmakers | Overheid en aangesloten bedrijfssectoren | Overheid |
| Doel | Het DTN is een globale analyse van de (inter) nationale terroristi-sche dreiging tegen Nederland. | Geeft een beeld over een dreiging op een (vitale) bedrijfssector. Bedoeld om in geval van verhoogde dreiging maatregelen te kunnen nemen bij een sector. | Geeft de ernst en de waarschijnlijk van een dreiging op een object, dienst of persoon weer. Bedoeld om bij een concrete dreiging beveiligings-maat-regelen te kunnen nemen. |
| Niveaus van dreiging | • Minimaal<br>• Beperkt<br>• Substantieel<br>• Kritiek | • Basisniveau<br>• Lichte dreiging<br>• Matige dreiging<br>• Hoge dreiging | Combinatie van de waarschijnlijkheid en de ernst van de gebeurtenis. |
| Dreiging geldt voor | Nederland als geheel | Aangesloten bedrijfssectoren | Objecten, diensten en personen |
| Maatregelen | Het DTN is bedoeld voor het formuleren van contra-terrorismebeleid. | Afhankelijk van het dreigingsniveau treffen de sector én de overheid maatregelen. | Afhankelijk van het dreigingsniveau treft de overheid beveiligings-maatregelen |

### 3.2.2 Het algemene dreigingsbeeld

De NCTV stelt ten minste ieder kwartaal het *Dreigingsbeeld Terrorisme Nederland* (DTN) op. Het DTN beschrijft de (inter)nationale terroristische dreiging tegen Nederland. Het DTN is gebaseerd op onder meer (geheime) informatie van inlichtingen- en veiligheidsdiensten en informatie uit (inter) nationale openbare bronnen. De overheid gebruikt het DTN voor het formuleren van haar contra-terrorismebeleid op verschillende niveaus.

Er zijn voor Nederland vier dreigingsniveaus: minimaal, beperkt, substantieel en kritiek. De criteria van de niveaus zijn vermeld in bijlage VI. Momenteel (eind 2014) is de terroristische dreiging substantieel. Dat betekent dat de kans aanwezig is dat in Nederland een aanslag zal plaatsvinden. Deze kans is onder meer gebaseerd op het profiel van Nederland in het buitenland. Deelname aan internationale vredesoperaties en het maatschappelijk debat over de islam beïnvloeden dit profiel. Daarnaast houdt de kans op een terroristische aanslag ook verband met de aanwezigheid van binnenlandse radicalisering en netwerken (zie ook hoofdstuk 2).

Bedrijven kunnen op www.nctv.nl een samenvatting downloaden van het *Dreigingsbeeld Terrorisme Nederland* (DTN). Ook vindt u daar het actuele dreigingsniveau.

Voor het schetsen van een accuraat beeld van terroristische dreigingen is informatie van gemeenten, politie en bedrijven nodig. Bedrijven doen er goed aan signalen van ongebruikelijke handelingen of verdachte objecten door te geven aan de plaatselijke politie.

### 3.2.3 Dreiging tegen een sector

Het Alerteringssysteem Terrorismebestrijding is een waarschuwingssysteem voor overheid en bedrijfsleven. Het systeem waarschuwt professionele operationele diensten (bestuur, politie, inlichtingendiensten) en aangesloten bedrijfssectoren bij een verhoogde dreiging. Overheidsdiensten en de betrokken sector informeren elkaar en kunnen zo snel adequate maatregelen treffen.

**Aangesloten sectoren Alerteringssysteem Terrorismebestrijding**

| | |
|---|---|
| Sector Luchthavens | Sector Financiën |
| Sector Drinkwater | Sector Olie en Chemie |
| Sector Spoor (personenvervoer en stations) | Sector Telecom |
| Sector Zeehavens | Sector Tunnels en Waterkeringen |
| Sector Gas | Sector Hotels |
| Sector Elektriciteit | Sector Niet-Rijkstunnels |
| Sector Nucleair | Sector Evenementen |
| Sector Stads- en streekvervoer | |

Het Alerteringssysteem kent vier niveaus (basisniveau, lichte, matige en hoge dreiging). Elk niveau kent zijn eigen pakket van maatregelen. Bij het 'basisniveau' gelden de maatregelen die tot de reguliere bedrijfsvoering horen. Hoe hoger het alerteringsniveau, hoe zwaarder en ingrijpender de maatregelen. Bedrijfssectoren kunnen bij het Alerteringssysteem worden aangesloten, wanneer zij van vitaal belang zijn voor Nederland en/of een aantrekkelijk doelwit voor terroristen vormen. Aangesloten bedrijfssectoren en hun actuele alerteringsniveaus staan vermeld op de website www.nctv.nl.

Bij verhoging of verlaging van het alerteringsniveau worden onder meer op de hoogte gesteld:
- de betrokken bedrijfssector;
- de politie;
- het Openbaar Ministerie;
- de gemeente (waarop de dreiging betrekking heeft).

De minister van Veiligheid en Justitie besluit over verhoging of verlaging van het alerteringsniveau. Hij doet dit op basis van een risicoanalyse, opgesteld door de NCTV. Voorafgaand aan het besluit van de minister vindt overleg plaats met de meest relevante spelers, waaronder in ieder geval de politie en de sector. Zij voeren ook zelf de maatregelen uit. De bedrijven betalen zelf de kosten voor het uitvoeren van de maatregelen. De NCTV adviseert welke concrete maatregelen een bedrijf kan treffen. De verantwoordelijkheid voor de uitvoering van de overheidsmaatregelen ligt grotendeels bij het lokale bestuur. Bedrijven die niet aangesloten zijn bij het Alerteringssysteem kunnen te maken krijgen met maatregelen die aangesloten bedrijven nemen.

## Voorbeelden maatregelen van overheid en bedrijven in het Alerteringssysteem

| Niveau | Soort maatregel | Voorbeelden van maatregelen |
|---|---|---|
| Basis | Maatregelen die horen bij 'goed huisvaderschap' en de reguliere bedrijfsvoering. Waarborgt de basisveiligheid en bedrijfscontinuiteit onder normale omstandigheden. | Screenen van vertrouwensfunctionarissen, bewakingspersoneel inzetten, regulier cameratoezicht |
| 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.<br>Het gaat om extra alertheid en maatregelen gericht op reductie van het risico op een aanslag. | Verscherpt toezicht door politie, ingangscontroles, afsluiten van terreinen/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 controles grootschalige inzet van politiediensten. |

## 3.3 Lokaal

### 3.3.1 Algemeen

Op lokaal niveau werken politie en gemeenten aan het vergroten van de veiligheid. Daaronder valt ook terrorismebestrijding. De gemeente is in eerste instantie verantwoordelijk voor het 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 en/of Bevolkingszorg. Ook kunnen bedrijven te maken krijgen met de ambtenaar verantwoordelijk voor Economische Zaken.

Bedrijven hebben doorgaans met de politie te maken bij concrete dreigingssituaties. De volgende paragraaf handelt daarover. Een aantal politie-eenheden overlegt met bedrijven over structurele (preventieve) maatregelen rond terrorismebestrijding. Voor risicoanalyses en advies zal de politie bedrijven meestal doorwijzen naar commerciële beveiligingsbedrijven.

### 3.3.2 Dreiging tegen personen, objecten of diensten

De burger is in eerste instantie zelf verantwoordelijk voor de veiligheid van zijn eigen persoon of goed. Ook bedrijven zijn in eerste instantie zelf verantwoordelijk voor het treffen van maatregelen die de veiligheid van hun werknemers borgen. Soms is de dreiging zo groot, dat een werkgever zijn personeel of goederen niet meer zelf kan beschermen. Hij kan dan de hulp van de lokale overheid inroepen, waarbij de plaatselijke politie het centrale aanspreek¬punt is. De politie bekijkt samen met andere lokale autoriteiten of beveiligingsmaatregelen noodzakelijk zijn.

De beveiliging en bewaking van personen, objecten en diensten valt in principe onder de verantwoordelijkheid van de lokale overheid. Het kan voorkomen dat een persoon, object of dienst niet onder de lokale, maar onder de landelijke verantwoordelijkheid valt. De Rijksoverheid heeft namelijk een bijzondere verantwoordelijkheid voor een beperkte groep personen, objecten of diensten. Hun veiligheid en functioneren zijn van nationaal belang. In zo'n geval nemen de lokale autoriteiten contact op met de Coördinator Bewaking en Beveiliging (CBB), werkzaam bij de NCTV. Hij is belast met het onderhoud en de uitvoering van het stelsel Bewaken en Beveiligen. Bedrijven hoeven niet zelf contact op te nemen met de NCTV, want de beveiligingsmaatregelen vanuit de lokale en landelijke overheid zijn gelijk.

Bedrijven die melding of aangifte doen bij de plaatselijke politie van dreigingen, ongebruikelijke handelingen of verdachte objecten, krijgen waarschijnlijk te maken met de portefeuillehouder Conflict- en Crisisbeheersing (CCB) van de politie. Hij behandelt dreigingsmeldingen en voorziet de andere lokale autoriteiten van informatie. Dreigingsmeldingen kunnen ook via andere kanalen binnenkomen, zoals de landelijke overheid. De portefeuillehouder CCB beoordeelt de concrete dreiging (zie hoofdstuk 2). Soms brengt hij ook potentiële dreigingen in kaart.

Op basis van informatie van de portefeuillehouder CCB wegen de burgemeester, de (hoofd)officier van justitie en de politiechef (gezamenlijk de driehoek) de ernst en waarschijnlijkheid van de dreiging. De driehoek bepaalt of beveiligingsmaatregelen nodig zijn en zo ja, welke. Hoe hoger de ernst en waarschijnlijkheid, hoe zwaarder het maatregelenpakket.

**De burgemeester is verantwoordelijk voor:**

- treffen van veiligheidsmaatregelen indien de openbare orde in het geding is;
- objectbeveiliging gericht op handhaving van de openbare orde en veiligheid.

**De (hoofd)officier van justitie is verantwoordelijk voor:**

- treffen van veiligheidsmaatregelen (bijvoorbeeld persoonsbeveiliging) bij vrees voor het leven van personen, hun fysieke integriteit of voor andere ernstige delicten;
- objectbeveiliging gericht op de strafrechtelijke handhaving van de rechtsorde.

## Voorbeelden van overheidsmaatregelen binnen het stelsel Bewaken en Beveiligen

| | |
|---|---|
| Extra aandacht in de reguliere surveillance van politie | Verscherpt rijdend toezicht |
| Gecombineerd rijdend toezicht | Permanent toezicht, bewakingscontainer |
| Persoonsbegeleiding | Persoonsbeveiliging |
| Routeverkenning | Safe-house |
| Bouwtechnisch advies | Explosievenschouw |
| Technische beveiliging van woning of werkplek | Technische beveiliging van het voertuig |
| Pasjesregeling | Accreditatie |
| Poortjes | Pantservoertuigen |
| Inzet bijzondere bijstandseenheden | Wegafsluiting |

De lokale autoriteiten onderhouden contact met de bedreigde persoon, de instelling of het bedrijf over de getroffen beveiligingsmaatregelen. De plaatselijke politie voert deze maatregelen uit. Zij kunnen daarbij gebruikmaken van faciliteiten van de Rijksoverheid. Zo is ondersteuning voor persoonsbeveiliging door de Dienst Bewaken en Beveiligen (DBB) mogelijk. Bedrijven treffen zelf ook maatregelen en stellen de politie daarvan in kennis. Zij kunnen over maatregelen die passen bij de aard van het bedrijf, advies inwinnen bij een (commerciële) veiligheidsadviseur of navraag doen bij hun brancheorganisatie (zie hoofdstuk 5).

Door belangen, dreigingen en weerstand in onderlinge samenhang te bekijken kunnen risico's van een organisatie – en dus ook van een bedrijf – worden benoemd.

# 4 Risicomanagement

## 4.1 Methodiek risicoanalyse

Mensen en organisaties zijn voortdurend in de weer om de risico's van alledag te beheersen. Vaak gebeurt dat intuïtief en zonder een expliciete aanpak of methodiek. Er zijn echter ook bedrijfssectoren en vakgebieden waar het analyseren en het managen van risico's een bijzonder specialisme is geworden. Een voorbeeld hiervan is de financiële sector met het beheersen van investeringsrisico's, verzekeringsrisico's en beleggingsrisico's. De chemische industrie richt zich juist op de beheersing van ongevalsrisico's.

Een ander soort risicomanagement is het beheersen van risico's veroorzaakt door mensen die kwaad willen, ook wel aangeduid als bewust menselijk handelen. Hiervoor zijn specifieke risicoanalysemethoden ontwikkeld. Deze methodieken bestaan meestal uit een combinatie van drie verschillende analyses: een afhankelijkheidsanalyse, een dreigingsanalyse en een kwetsbaarheidsanalyse.

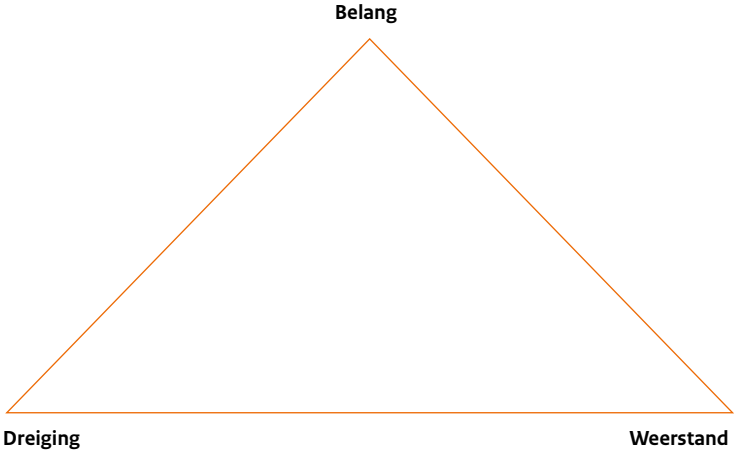
**In de afhankelijkheidsanalyse** staan de kroonjuwelen van de organisatie centraal: vitale bedrijfsprocessen en cruciale onderdelen van de organisatie. Deze *belangen* behoeven bescherming om ernstige bedrijfseconomische of maatschappelijke schade te voorkomen (zie paragraaf 4.2).

**In de dreigingsanalyse** worden de mensen die kwaad willen en hun activiteiten onderzocht. Hier staat de waarschijnlijkheid van de *dreiging* centraal. In deze handreiking wordt naast de criminele dreiging vooral aandacht gevraagd voor de terroristische dreiging (zie paragraaf 4.3).

**In de kwetsbaarheidsanalyse** wordt de *weerstand* van een organisatie onderzocht. Daar waar de weerstand tekortschiet kan de organisatie kwetsbaar zijn (zie paragraaf 4.4).

De risicoanalyse brengt de cruciale belangen, de waarschijnlijk geachte potentiële dreigingen en de weerstand van een organisatie met elkaar in verband. Door belangen, dreigingen en weerstand in onderlinge samenhang te bekijken kunnen risico's van een organisatie – en dus ook van een bedrijf – worden benoemd. Voor het maken van een goede risicoanalyse is kennis en informatie nodig over de organisatie, over concrete en potentiële dreigingen én over weerstandsverhogende maatregelen. Het doel van een risicoanalyse is te kunnen inspelen op ernstige risico's van nu en in de nabije toekomst.

## Figuur: Onderdelen van een risicoanalyse




Verschillende organisaties, commerciële instellingen of adviesbureaus hanteren diverse methoden voor het opstellen van risicoanalyses. Ook zijn er risicoanalysemethoden in omloop die specifiek gericht zijn op het evalueren van beveiligingsmaatregelen. Deze handreiking spreekt geen voorkeur uit voor één van deze methodieken, maar geeft wel aan welke elementen in een risicoanalyse thuishoren.

De uitvoering van een risicoanalyse kan op verschillende manieren. Het is mogelijk een adviesbureau in te schakelen, wat voor bedrijven die veel risico denken te lopen of grotere bedrijven aanbeveling verdient. Ook kunnen bedrijven uit dezelfde branche een gezamenlijke analyse (laten) uitvoeren. Belangrijk is in ieder geval een beproefde methodiek te hanteren en deskundigen te betrekken bij de verschillende onderdelen van de analyse. Voor kleinere bedrijven is een extern bureau inschakelen niet altijd mogelijk. Het volgende schema kan ook behulpzaam zijn bij een minder omvangrijke risicoanalyse. In dit schema zijn de opeenvolgende stappen bij het opstellen van een risicoanalyse aangegeven.

## Schema: proces risicoanalyse

Stap 1. Bepaal het domein van de risicoanalyse
(bijvoorbeeld: een sector, een cluster bedrijven of een bepaald bedrijf)

→ Stap 2. Afhankelijkheidsanalyse (zie 4.2)
Stap 3. Dreigingsanalyse (zie 4.3)
Stap 4. Kwetsbaarheidsanalyse (zie 4.4) ←

→ Stap 5. Risicoanalyse (zie 4.5)

→ Stap 6. Kosten- en batenanalyse van (aanvullende) maatregelen (zie 4.6)

Bovenstaande afbeelding illustreert een cyclus voor risicomanagement. Aan de hand van de zes stappen van deze cyclus kunnen de risico's van een bedrijf worden benoemd en gerangschikt. Op basis hiervan besluit een bedrijf (aanvullende) maatregelen ter vermindering van die risico's te onderzoeken.

## 4.2 Afhankelijkheidsanalyse

In een afhankelijkheidsanalyse staan de belangen van een bedrijf centraal, belangrijke waarden die kunnen worden aangetast. Belangen van een organisatie zijn bijvoorbeeld mensen, belangrijke bedrijfsprocessen, cruciale bedrijfselementen, grondstoffen, objecten of locaties. Hieronder volgen enkele invalshoeken om de belangen en de afhankelijkheden van een bedrijf te duiden.

- **Mensen en hun veiligheid** zijn van het grootste belang voor iedere organisatie. Waarborging van de fysieke en psychische gezondheid van mensen is daarom bij iedere organisatie noodzakelijk.
- **Informatie** kan uniek, kostbaar, imagogevoelig, vertrouwelijk of cruciaal voor de continuïteit of concurrentiepositie van de organisatie zijn. De beschikbaarheid, vertrouwelijkheid of de integriteit van de informatie moet dan worden zeker gesteld.
- **Bedrijfsprocessen** zijn vaak cruciaal voor de bedrijfscontinuïteit of concurrentiepositie van een bedrijf. Deze processen mogen niet of zo min mogelijk worden verstoord.
- **Productiemiddelen, grondstoffen, producten en diensten** kunnen kostbaar en attractief voor criminelen zijn. De beschikbaarheid en integriteit hiervan moeten worden gewaarborgd.

Een goede afhankelijkheidsanalyse geeft inzicht in welke belangen het bedrijf onderkent en wat hun omvang is. Ook geeft de analyse aan waarvan die belangen afhankelijk zijn. Mede hierdoor wordt inzicht verkregen in de mogelijke schade – in aard en omvang – bij een ernstig incident, ook wel het effect of de ernst van een incident genoemd. Deze schade kan van bedrijfs¬economische of meer maatschappelijke aard zijn. Een categorisering en rangschikking van de ernst van de mogelijke schades vormt de basis voor de risicoanalyse.

## 4.3 Dreigingsanalyse

Na definiëring en rangschikking van belangen en afhankelijkheden volgt een systematisch onderzoek naar mogelijke dreigingen. Wie zouden een bepaald belang kunnen schaden en hoe gaan zij dan te werk?

In hoofdstuk 2 stond de inventarisatie van de terroristische dreiging centraal. Daar is al aangegeven dat een dreigingsanalyse zich uitspreekt over potentiële dreigingen. Bij een dreigingsanalyse is het verstandig eerst de mogelijke mensen die kwaad willen in kaart te brengen. Wie heeft de kennis, kunde en intentie om specifieke bedrijven schade toe te brengen? Vervolgens moet worden vastgesteld met welke middelen en methoden zij te werk kunnen of zullen gaan.

Bij het opstellen van een dreigingsanalyse over de terroristische dreiging kunnen bedrijven gebruikmaken van de informatie uit hoofdstuk 2. Aanvullende informatie hierover is te vinden via de website van de AIVD: www.aivd.nl. Momenteel bekijken overheid en private sector of verbetering van informatie-uitwisseling over de terroristische dreigingen mogelijk is. Voor een inschatting van de dreiging die uitgaat van bijvoorbeeld criminelen, vandalen en eigen medewerkers, zullen andere bronnen en deskundigen moeten worden geraadpleegd.

Een categorisering en inschatting van de waarschijnlijkheid van acties of incidenten door mensen die kwaad willen (waarschijnlijk geachte potentiële dreigingen) is de tweede bouwsteen voor de risicoanalyse.

## 4.4 Kwetsbaarheidsanalyse

Welk bedrijf een terrorist kiest voor zijn kwaadwillende activiteiten en of hij daarin slaagt, hangt af van een groot aantal factoren. In hoofdstuk 2 is al ingegaan op de motivatie van terroristen en hun keuze van doelen; niet alle bedrijven zijn even geschikt of aantrekkelijk. De kwetsbaarheidsanalyse onderzoekt de kwetsbaarheid van bedrijven voor bepaalde activiteiten van mensen die kwaad willen. Deze analyse legt een relatie tussen de methode en de middelen van de mensen die kwaad willen versus de weerstand daartegen van het bedrijf. De methoden en middelen die terroristen kunnen of zullen gebruiken, vloeien voort uit de dreigingsanalyse van

paragraaf 4.3. De weerstand van een bedrijf is te onderzoeken en eventueel te verbeteren aan de hand van de vijf schakels van de veiligheidsketen: pro-actie, preventie, preparatie, respons en nazorg.

**De veiligheidsketen kent vijf schakels van veiligheidsmaatregelen:**
**Pro-actie:** 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 daadwerkelijk optreden bij een aanslag.
**Respons:** bestrijden van de aanslag, beperken van de nadelige gevolgen van een aanslag en het verlenen van hulp. Soms wordt voor respons ook 'repressie' gebruikt.
**Nazorg:** activiteiten gericht op verhelpen van gevolgen van een aanslag en de terugkeer naar de 'normale' situatie.

Hieronder wordt de aard van de maatregelen per schakel in de veiligheidsketen omschreven. In hoofdstuk 5 komen meer voorbeelden van maatregelen aan de orde.

- **Proactieve maatregelen:** deze moeten voorkomen dat kwetsbaarheden ontstaan. Een bedrijf kan bijvoorbeeld bedrijfsonderdelen naar een minder risicovolle locatie verplaatsen.
- **Preventieve maatregelen:** deze verkleinen de kwetsbaarheid en dus de kans op een incident. Preventieve maatregelen in relatie tot mensen die kwaad willen, worden vaak 'beveiligingsmaatregelen' genoemd. Een bedrijf kan beveiligingsmaatregelen treffen zoals het aanbrengen van goed hang- en sluitwerk, het instellen van toegangscontrole en het gebruik van virusscanners.
- **Preparatieve maatregelen:** deze zijn gericht op een goede voorbereiding op incidenten. Een bedrijf kan bijvoorbeeld een vluchtplan opstellen voor het personeel en deze periodiek oefenen.
- **Responsieve maatregelen:** deze moeten de directe nadelige gevolgen van een incident beperken. Denk hierbij aan het inzetten van blus-middelen, het organiseren van de eerste hulp en het managen van de crisis.
- **Nazorgmaatregelen**: deze moeten de bedrijfscontinuïteit en de overgang naar 'back-to-normal' bevorderen. Denk daarbij aan het maken van back-ups en het regelen van een uitwijklocatie.

## 4.5 Risicoanalyse

In de risicoanalyse komen de belangen, dreigingen en weerstand bij elkaar. Deze analyse maakt inzichtelijk welke risico's de organisatie loopt, welke risico's acceptabel zijn en tegen welke risico's maatregelen nodig zijn.

De risicoanalyse maakt de ernst van het effect van de meest waarschijnlijke acties van mensen die kwaad willen duidelijk, rekening houdend met de bestaande weerstand van de organisatie. In deze analyse worden de resultaten van de vorige analyses betrokken:

- de waarschijnlijk geachte activiteiten door mensen die kwaad willen (waarschijnlijk geachte potentiële dreigingen);
- de weerstand van de organisatie op die specifieke activiteiten of dreigingen;
- de ernst van de schade die de incidenten bij de bestaande weerstand alsnog veroorzaken.

De waarschijnlijkheid van de incidenten uit de dreigingsanalyse wordt concreter in het licht van de bestaande én ontbrekende weerstand uit de kwetsbaarheidsanalyse. Sommige incidenten blijken bij nader inzien minder aannemelijk door reeds aanwezige maatregelen.

De waarschijnlijkheid dat een organisatie te maken krijgt met een terroristische aanslag is doorgaans vele malen lager dan bijvoorbeeld de kans op diefstal door criminelen. Daar staat echter tegenover dat de ernst van de mogelijke schade door een terroristische aanslag veel groter kan zijn dan de schade door criminaliteit.
In de risicoanalyse wordt de waarschijnlijkheid (ook wel de kans genoemd) daarom gerelateerd aan de ernst van de schade die daaruit kan voortkomen; ook wel effect genoemd. Het resultaat is een waardering van het risico. Een veel gebruikte formule hiervoor is:

*Risico = Kans X Effect*

Na rangordening van de risico's geeft de organisatie aan welke risico's acceptabel zijn en tegen welke risico's (aanvullende) maatregelen noodzakelijk zijn.

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

| Type analyse | Focus | Leidt tot |
|---|---|---|
| Afhankelijkheidsanalyse | Aard en omvang van de bedrijfsbelangen | Inschatting van de schade bij een incident (= effect van incident) |
| Dreigingsanalyse | • potentiële dreiging<br>• mensen die kwaad willen<br>• middelen en methode | Inschatting van waarschijnlijkheid van acties of incidenten (= waarschijnlijk geachte potentiële dreiging). |
| Kwetsbaarheidsanalyse | • weerstand<br>• maatregelen | Inschatting van de weerstand van de organisatie |
| Risicoanalyse | • belangen<br>• potentiële dreiging<br>• weerstand | Inschatting van de ernst van de schade die incidenten bij bestaande weerstand alsnog veroorzaken |

## 4.6 Kosten- en batenanalyse

Deze analyse onderzoekt welke bijdrage, ook wel baten, eventuele (aanvullende) maatregelen kunnen hebben op het verlagen van de geconstateerde risico's. Worden de risico's echt verlaagd door de voorgestelde maatregelen?

Deze baten moeten worden afgezet tegen de kosten van de desbetreffende maatregelen. Staan de kosten in een acceptabele verhouding tot de baten? Hieruit volgt welke maatregelen het meest kosteneffectief zijn. De organisatie is zelf verantwoordelijk voor deze afweging van kosten en baten.

Het veiligheidsbeleid moet een duidelijke plaats krijgen in de reguliere bedrijfsvoering.


# 5 Maatregelen door bedrijven

## 5.1 Inleiding

In dit hoofdstuk komen de maatregelen aan de orde die bedrijven kunnen nemen om hun weerstand tegen (terroristische) dreigingen te vergroten.

Er zijn verschillende soorten indelingen van maatregelen, zoals:

- een indeling langs de elementen personeel, gebouwen en informatie.
- een indeling langs de elementen organisatorisch, (bouw)technisch, elektronisch en ICT. De beveiligingsbranche gebruikt deze indeling, ook wel OBE genoemd, veelvuldig.
- een indeling bestaande uit basismaatregelen (fysieke en personele beveiliging), reactieve maatregelen (risicoanalyse, beveiligings- en risicomanagement), preventieve maatregelen (beveiligingsportefeuille in managementteam, geavanceerde informatiebeveiliging) en geavanceerde maatregelen (ketensamenwerking, beveiligingsstrategie). een indeling langs de lijnen van de veiligheidsketen: pro-actie, preventie, preparatie, respons en nazorg.

Dit hoofdstuk hanteert zoveel mogelijk de indeling van de veiligheidsketen, waarbij de aandacht uitgaat naar maatregelen gericht op objecten en diensten (fysieke veiligheid), personeel en informatie.

## 5.2 Hoe komt u tot maatregelen?

Hoofdstuk 4 behandelde de wijze waarop bedrijven kunnen komen tot een goede risicoanalyse. Bij het opstellen van deze analyse maken bedrijven ook een kwetsbaarheidsanalyse. Onderdeel van de kwetsbaarheidsanalyse is een inventarisatie van de maatregelen die een bedrijf heeft genomen om de kans op incidenten te verminderen. De risicoanalyse maakt inzichtelijk tegen welke risico's aanvullende maatregelen nodig zijn. Het is dan nog niet geheel duidelijk om welke maatregelen dit gaat.

In een veiligheidsplan is het mogelijk de concrete maatregelen te bepalen. Veel bedrijven beschikken al over een dergelijk plan; de aandacht voor veiligheid maakt deel uit van de reguliere bedrijfsvoering. Indien aanwezig kan het onderdeel terrorismebestrijding opgenomen worden in het bestaande (veiligheids)beleid. Wanneer een bedrijf nog niet beschikt over een veiligheidsbeleid en een veiligheidsplan, is het verstandig dit wel vast te stellen.

Wie het veiligheidsbeleid opstelt en vastlegt verschilt per bedrijf. Binnen grote bedrijven zijn vaak security managers aanwezig. Kleinere bedrijven zullen iemand anders met het veiligheidsbeleid belasten, zoals de eigenaar of directeur. Een duidelijk aanspreekpunt voor het veiligheidsbeleid is in ieder geval raadzaam. De verantwoordelijke kan de volgende taken op zich nemen:

- opstellen van een risicoanalyse;
- opstellen van een veiligheidsplan waarin aandacht uitgaat naar risicomanagement en bedrijfscontinuïteit;
- implementatie en zo nodig testen en oefenen van de maatregelen;
- opstellen van een ontruimingsplan als onderdeel van het veiligheidsplan;
- aanwijzingen hoe te handelen bij verdachte objecten, personen en handelingen, en bommeldingen (als onderdeel van het veiligheidsplan);
- 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 en de maatregelen.

Het is van groot belang dat de verantwoordelijke voor het veiligheidsbeleid steun krijgt van de directie of het managementteam. Wanneer de directie het veiligheidsbeleid en -plan goedgekeurd heeft, het belang ervan uitdraagt en ook zelf de maatregelen naleeft, neemt de kans op een breed draagvlak bij de werknemers toe. Bij het opstellen van het veiligheidsbeleid en -plan is het verstandig ook de verschillende afdelingen te raadplegen binnen uw bedrijf, als deze er zijn. Het veiligheidsplan beschrijft onder meer wie wat in bepaalde situaties moet doen. Maak dus een checklist van de maatregelen en instructies die werknemers moeten nemen in bepaalde situaties.



De volgende stappen zijn essentieel voor een goede veiligheid in en rond het bedrijf:

1. Maak een risicoanalyse (zie hoofdstuk 4).
2. Ontwikkel veiligheidsbeleid en laat dit goedkeuren door de directie of het managementteam.
3. Stel een veiligheidsplan op en laat dit goedkeuren door de directie of het managementteam.
4. Communiceer het plan en de maatregelen naar de medewerkers of werknemers.
5. Oefen de plannen regelmatig en pas deze zo nodig aan.

## 5.3 Welke maatregelen moet u nemen?

De activiteiten van bedrijven liggen vooral op het gebied van ‘pro-actie’ en ‘preventie’ van de veiligheidsketen. Deze maatregelen zorgen ervoor dat een bedrijf een minder makkelijk doelwit is voor terroristen. Bij preventieve maatregelen gaat het bijvoorbeeld om het instellen van toegangsregels. Maar ook preparatieve maatregelen zijn van belang voor bedrijven. Bijvoorbeeld het opstellen van een goed vluchtplan voor personeel, zoals in paragraaf 5.2 al aan de orde kwam.

De volgende paragrafen beschrijven diverse maatregelen aan de hand van de vijf schakels van de veiligheidsketen. Deze maatregelen zijn niet alleen gericht op terrorismebestrijding, maar kunnen ook de kans op criminaliteit verminderen. De genoemde maatregelen hebben steeds betrekking op objecten en diensten (fysieke veiligheid), personeel en informatie.

Veelal is al sprake van goed ‘huisvaderschap’ bij bedrijven. Binnen de reguliere bedrijfsvoering worden maatregelen getroffen om de basis-veiligheid en bedrijfscontinuïteit onder normale omstandigheden zeker te stellen. Denk bijvoorbeeld aan het schoonhouden van het bedrijf en zijn directe omgeving. Ook goede verlichting en regulier cameratoezicht horen hiertoe.

In de kwetsbaarheidsanalyse zijn naar alle waarschijnlijkheid alle maatregelen rondom de reguliere bedrijfsvoering naar voren gekomen. Of aanvullende maatregelen nodig zijn, hangt af van de dreigingen

waarmee individuele bedrijven te maken hebben. Een kosten- en baten-analyse is daarbij van groot belang om dure investeringen in ineffectieve en onnodige maatregelen te voorkomen.

De effectiviteit neemt toe bij verschillende typen maatregelen. Maatregelen gericht op de objecten zijn bijvoorbeeld effectiever in combinatie met maatregelen gericht op het personeel.

Over de maatregelen kunnen bedrijven contact leggen met de plaatselijke politie. De politie heeft veelal expertise in huis over beveiligings-maatregelen rond objecten (en diensten). Minder gangbaar is dat de politie ook over kennis beschikt rond andere maatregelen. Hiervoor is het mogelijk professionele bedrijven in te huren. Vaak kunnen deze ook een risico-analyse uitvoeren.

## 5.4 Pro-actieve maatregelen

Pro-actieve maatregelen voorkomen structurele oorzaken van onveiligheid of nemen deze weg. Een bedrijf kan echter maar weinig pro-actieve maatregelen nemen, zowel ten aanzien van objecten en diensten, als personeel en informatie. Het afstoten van een risicovolle bedrijfsactiviteit is meestal geen optie, vaak gaat het om de corebusiness van een bedrijf. Soms is het wel mogelijk om een bedrijfsonderdeel naar een minder risicovolle locatie te plaatsen. Een bedrijf met giftige gassen dicht tegen een woonwijk aan, kan aanzienlijk meer schade voor de omgeving opleveren dan een bedrijf op een afgelegen plaats.
Wat betreft personeel is het mogelijk contracten van geradicaliseerde werknemers niet te verlengen. Géén personeel in dienst nemen dat mogelijk ontvankelijk is voor terrorisme is geen optie: er bestaat geen zekerheid of iemand ook daadwerkelijk radicaliseert. Factoren die duiden op radicalisering zijn moeilijk te geven.
Ook voor informatie zijn nauwelijks pro-actieve maatregelen te nemen. Bescherming van gegevens is mogelijk, maar dat valt onder preventieve maatregelen.



## 5.5 Preventieve maatregelen

### 5.5.1 Inleiding

Preventieve maatregelen voorkomen de *directe* oorzaken van onveiligheid en beperken de gevolgen van eventuele inbreuken op die veiligheid. Deze maatregelen richten zich niet alleen op de beveiliging van objecten en diensten, maar ook van personeel en informatie. Het heeft immers weinig zin te investeren in dure beveiligingsmaatregelen als werknemers deze gemakkelijk kunnen ondermijnen. Investering in afspraken en het naleven van regels door medewerkers is dan ook van groot belang. Een integrale aanpak, die alle facetten van de bedrijfsvoering onder de loep neemt, is daarom essentieel.

Hieronder staan preventieve maatregelen beschreven die bedrijven in overweging kunnen nemen.

### 5.5.2 Objecten en diensten

Wanneer bedrijven hun objecten en diensten beveiligen, zorgen zij ook voor de veiligheid van personeel en informatie. Het is raadzaam om eens door de ogen van terroristen naar objecten en diensten te kijken. Is het terrein open toegankelijk? Kunnen onbevoegden gemakkelijk het gebouw binnenkomen? Hoe kan de meeste schade aan het gebouw worden toegebracht? De volgende maatregelen zijn mogelijk:

#### Schoon en onderhouden

Onder goed ‘huisvaderschap’ behoort eigenlijk al het schoonhouden en onderhouden van de publieke en gemeenschappelijke ruimten in en om uw bedrijf. Een schone omgeving doet verdachte zaken sneller opvallen. Met een beperkt aantal meubelen in publieke en gemeenschappelijke ruimten vergroot u bovendien het overzicht. Ook obstakels of posters die de inkijk op uw bedrijf belemmeren, kunt u beter weghalen.
Maatregelen die uw bedrijf kunt treffen zijn onder meer het regelmatig legen van vuilnisbakken, het vasthouden aan een vaste plaats voor bepaalde zaken, het sluiten van kasten en lege kantoren.
Vanzelfsprekend geldt dat ook de omgeving van het bedrijf onderhoud verdient. De parkeerplaatsen moeten er goed bij liggen en de vegetatie rond het bedrijf – vooral dicht bij ingangen – moet regelmatig worden gesnoeid.

## Bouwtechnische maatregelen

Bouwtechnische maatregelen zijn maatregelen die met het object zelf te maken hebben. Soms zijn bouwkundige maatregelen effectief om mensen die kwaad willen buiten uw organisatie te houden. Voorbeelden zijn:

- slagwerende beglazing;
- goed hekwerk;
- goed hang en sluitwerk;
- goede verlichting;
- beveiliging van deuren en ramen.

## Toegangswegen en toegangsbeleid

Het helpt zowel criminelen als terroristen wanneer uw bedrijf of bedrijfsterrein gemakkelijk toegankelijk is. Zorg daarom voor maatregelen die de toegang tot uw bedrijf bemoeilijken. Naast allerlei bouwtechnische maatregelen, gaat het om aandacht voor het openen en sluiten van uw bedrijf, het toegangsbeleid en de veiligheid van de receptie.

Bij de opening en sluiting dient u er altijd op bedacht te zijn dat terroristen zich hebben kunnen insluiten, of dat bepaalde ramen nog open zijn. Controleer daarom voor uw openings- en sluitingsprocedure altijd de omgeving. Bij een verdachte situatie is het verstandig de politie te waarschuwen.

Het verdient aanbeveling het toegangsbeleid op papier te zetten. Bepaal wie onder welke voorwaarden uw organisatie mag betreden en maak dat bekend aan personeel en bezoekers. Overweeg toegangscontrole, zonering, sleutelbeheer, autorisatie van personeel tot bepaalde bedrijfsonderdelen en -systemen. Een sleutelplan kan deel uitmaken van uw toegangsbeleid. Beperk het aantal sleutels dat in omloop is en zorg ervoor dat een zeer beperkt aantal mensen toegangscodes tot het bedrijf kent. Het toegangsbeleid omvat ook een efficiënt ontvangstbeleid. Niet voor alle bedrijven zal een elektronisch pasjessysteem mogelijk zijn. Noteer wel altijd namen, bedrijf of organisatie, telefoonnummer en aankomsttijd van de bezoekers. Zo heeft u zicht op wie er in huis is.

**Toegangsbeleid in een hotel of warenhuis**

Het is niet altijd mogelijk om met pasjessystemen te werken om de toegang te krijgen tot een bedrijf. Denk aan een hotel en een warenhuis, waar elke dag steeds opnieuw mensen in en uit lopen.

In zo'n geval is zichtbare aanwezigheid van belang. Zowel bij de toegang van uw bedrijf als in het bedrijf. Bij de toegang is het verstandig bewakingspersoneel in te zetten. Dat maakt meer 'indruk' dan camera's die mogelijk uit te schakelen zijn. Bij ongeregeldheden die met de camera worden opgemerkt, is het verstandig altijd bewakingspersoneel te sturen.

## Veiligheidssystemen

Elektronische maatregelen kunnen indringers en dus ook terroristen ontmoedigen of vroegtijdig opmerken. Het is daarom goed om een aantal elektronische systemen te overwegen. Een geïntegreerde inzet van deze systemen levert de hoogste veiligheid op. Sommige systemen zijn prijzig; bedenk dan ook altijd vooraf of de inzet van het systeem echt nuttig is. Elektronische maatregelen hebben overigens weinig nut als zij niet gepaard gaan met heldere huisregels, die het personeel ook naleeft.

De volgende maatregelen zijn het overwegen waard:

- goede verlichting, zie ook bouwtechnische maatregelen;
- inzet van bewakingspersoneel;
- alarmsystemen;
- (elektronische) toegangscontrolesystemen, zie ook Toegangswegen en toegangsbeleid;
- camera's (CCTV).

### 5.5.3 Personeel

Een bedrijf kan ook te maken krijgen met kwaadwillende personeelsleden. Maatregelen zijn gericht op bewustwording van uw personeel en op het aannemen van nieuw personeel. Daarnaast is het mogelijk maatregelen te treffen die de dreiging van binnenuit de organisatie kunnen verminderen.

#### Bewustwording personeel

Het veiligheidsbeleid moet een duidelijke plaats krijgen in de reguliere bedrijfsvoering. Dat betekent dat de veiligheid en de getroffen maatregelen een regelmatig thema zijn in besprekingen met het personeel. Het kan nuttig zijn een dag of training te besteden aan de risico's die het bedrijf loopt. Maak tijdens trainingen helder wie wat moet doen in bepaalde situaties en behandel een checklist met de bijbehorende maatregelen en instructies. Ook zijn zogenaamde 'awareness-acties' aan te bevelen, zoals aandacht voor afgesloten bureaus, kasten en een clean desk-beleid.

Voor personeelsleden moet duidelijk zijn bij wie ze terechtkunnen als zij ongebruikelijke handelingen of situaties tegenkomen.

#### Aanname van nieuw personeel

De kans dat bedrijven geradicaliseerd personeel aannemen of in dienst hebben, is niet heel groot. Nederland heeft te maken met verschillende radicale netwerken, maar slechts een beperkt aantal geradicaliseerden wil overgaan tot gewelddadig handelen. Toch kan het geen kwaad om bij het aannemen van nieuw personeel aandacht te besteden aan de achtergrond van de sollicitant. Slechts in beperkte gevallen is het mogelijk om personeel te laten screenen door de AIVD. Het gaat daarbij om vertrouwensfuncties die erkend zijn door een ministerie.

Bedrijven hebben twee andere opties die veel gangbaarder zijn:

- opvragen van een Verklaring Omtrent Gedrag (VOG). Voor het VOG-onderzoek wordt gekeken in het centraal justitieel documentatieregister waarin gegevens over de afwikkeling van strafbare feiten en overtredingen staan vermeld, van onherroepelijke veroordelingen tot sepots en transacties. Ook kunnen in het onderzoek politieregistergegevens worden betrokken en kunnen inlichtingen worden ingewonnen bij het Openbaar Ministerie en de Reclassering. Probleem bij de VOG is dat er altijd een relatie tussen de delicten en de functie moet zijn. Verschillende sectoren hebben een screeningsprofiel.
- natrekken van referenties en het spreken van vorige werkgevers.

Personeel dat al bij u werkt kunt u tijdens functionerings-, beoordelings- en exitgesprekken wijzen op de onderwerpen risico's en beveiliging. Daarbij geeft u bijvoorbeeld aan welke sancties volgen indien werknemers niet volgens de voorschriften handelen. Eventueel kunt u een gedragscode opstellen.

#### Contractanten en extern personeel

Veel bedrijven hebben extern personeel over de vloer of te maken met contractanten. Het gaat bij extern personeel om de inhuur van bedrijven zoals installatie-, schoonmaak-, catering- en beveiligingsbedrijven. Outsourcing kan risico's met zich meebrengen als bedrijven vooraf niet precies bekijken wie zij binnenhalen. Met een gedragscode, een geheimhoudingsverklaring, een concurrentiebeding en procedures en voorschriften voor kwetsbare handelingen is het mogelijk om het gedrag van contractanten te beïnvloeden. Ook kunnen regels gesteld worden over informatie die de contractanten ontvangen en de gebieden binnen het bedrijf waar zij mogen komen.

Een laatste mogelijkheid is om aan contractanten een Verklaring Omtrent Gedrag van een rechtspersoon te vragen. Dat maakt meteen duidelijk of de contractant een betrouwbaar bedrijf is.

# Bijlage I: verklarende woordenlijst

| Begrip | Omschrijving |
|---|---|
| Afhankelijkheidsanalyse | In een afhankelijkheidsanalyse staan de vitale bedrijfsprocessen en cruciale onderdelen van een bedrijf centraal. Deze belangen van de organisatie behoeven bescherming om ernstige bedrijfseconomische en maatschappelijke schade te voorkomen. |
| Alerteringsniveau | Het Alerteringssysteem Terrorismebestrijding kent 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. |
| Bedrijfssectoren | De bedrijfstakken (sectoren) die zijn aangesloten bij het Alerteringssysteem Terrorismebestrijding (negen sectoren) en/of het project Bescherming Vitale Infrastructuur (twaalf sectoren). Deze sectoren vertegenwoordigen de bedrijven uit de betreffende sector in het overleg met de overheid. |
| Beveiligingsmaatregelen | Maatregelen door bedrijven en overheid gericht op de beveiliging van een goed, dienst of persoon. De maatregelen moeten de kans op een aanslag en het effect van een eventuele aanslag verminderen. Soms worden ook de termen veiligheids-maatregelen of maatregelen gebruikt. Naast beveiligings-maatregelen gaat het dan ook om bijv. organisatorische of informatietechnische maatregelen. |
| CBB | Coördinator Bewaking en Beveiliging valt onder de verantwoor-delijkheid van de NCTV. De CCB is belast met het onderhoud en de uitvoering van het stelsel Bewaken en Beveiligen. |
| Contra-terrorismebeleid | Beleid dat gericht is op het tegengaan van terrorisme. |
| Dreigingsanalyse | In een dreigingsanalyse worden de mensen die kwaad willen en hun activiteiten onderzocht. Gekeken wordt naar de potentiële dreigingen. De waarschijnlijkheid van de dreiging staat centraal. Dreigingsanalyses maken deel uit van risicoanalyses. |

| Begrip | Omschrijving |
|---|---|
| Dreigingsbeeld | Het Dreigingsbeeld Terrorisme Nederland wordt opgesteld door NCTV. Het is een analyse van de (inter)nationale terroristische dreiging tegen Nederland. |
| Dreigingsniveaus | Een dreigingsniveau geeft de ernst en waarschijnlijkheid van de dreiging weer. Het Dreigingsbeeld Terrorisme Nederland kent vier dreigingsniveaus: minimaal, beperkt, substantieel en kritiek. |
| Driehoek | De driehoek bestaat uit de burgemeester, de (hoofd)officier van justitie en de korpschef. Zij bespreken gezamenlijk het lokale openbare orde en veiligheidsbeleid. |
| Ketenveiligheid | Het principe waarbij elke schakel in bijv. een vervoersketen of voedselketen de eigen veiligheid moet kunnen garanderen tegenover de partners in diezelfde keten. |
| Kwetsbaarheidsanalyse | In een kwetsbaarheidsanalyse wordt de weerstand van een organisatie of bedrijf tegen bijv. een terroristische aanslag onderzocht. De kwetsbaarheid van een bedrijf hangt af van de aantrekkelijkheid van dat bedrijf voor terroristen en de maatregelen die een bedrijf heeft getroffen. |
| NCTV | De Nationaal Coördinator Terrorismebestrijding (NCTV) coördineert de samenwerking tussen de bij terrorismebestrijding betrokken instanties. De coördinator is verantwoordelijk voor de beleidsontwikkeling, de analyse van (inlichtingen)informatie en de regie over maatregelen bij de bestrijding van terrorisme. |
| Objectbeveiliging | Het beveiligen van een object d.m.v. bijvoorbeeld camera's, surveillance en fysieke maatregelen (o.a. hekwerk, sloten, overzichtelijke omgeving). |
| Portefeuillehouder CCB | De portefeuillehouder Conflict- en Crisisbeheersing is binnen de politie het centrale aanspreekpunt. Hier komen de meldingen van bedrijven die melding of aangifte doen van dreiging van hun bedrijf of medewerkers of ongebruikelijke handelingen of verdachte objecten terecht. |

| Begrip | Omschrijving |
|---|---|
| Radicalisering | Een proces van groeiende bereidheid om niet-democratische middelen te gebruiken om politieke of godsdienstige opvattingen aan anderen op te leggen. |
| Risicoanalyse | a In de risicoanalyse worden de cruciale belangen, de waarschijnlijk geachte potentiële dreigingen en de weerstand aan elkaar gerelateerd. Door belangen, dreigingen en weerstand in onderlinge samenhang te bekijken kunnen risico's van een bedrijf worden benoemd. Op basis van de risicoanalyse kunnen maatregelen worden genomen die de risico's zelf wegnemen of verminderen, of de gevolgen ervan beperken. |
| Rijk | Het Rijk of de Rijksoverheid wordt gebruikt om de hoogste bestuurslaag van het land aan te geven. De andere bestuurslagen zijn de provincies en gemeenten. Meestal wordt met het Rijk de ministeries bedoeld. |
| Terrorisme | Terrorisme is het plegen van of dreigen met geweld door burgers of groepen burgers, het ontwrichten van de samenleving of het toebrengen van grote economische zaakschade, met als doel maatschappelijke veranderingen te bewerkstellingen of politieke besluitvorming te beïnvloeden. |
| Terrorismebestrijding | 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. |
| Terroristische dreiging | De mate waarin er sprake is van een dreiging van een terroristische aanslag. |
| Veiligheidsketen | De veiligheidsketen kent vijf schakels van veiligheidsmaatregelen:<br>*Pro-actie:* voorkomen of wegnemen van structurele oorzaken van onveiligheid.<br>*Preventie:* voorkomen van directe oorzaken van onveiligheid en beperken van de gevolgen van eventuele inbreuken op die veiligheid.<br>*Preparatie:* voorbereiden op daadwerkelijk optreden bij een aanslag.<br>*Respons:* 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>*Nazorg:* activiteiten gericht op verhelpen van gevolgen van een aanslag en de terugkeer naar de 'normale' situatie. |



| Begrip | Omschrijving |
|---|---|
| Vitale infrastructuur | Producten, diensten en processen behoren tot de vitale infrastructuur als deze bij uitval grootschalige maatschappelijke ontwrichting kunnen veroorzaken. Bij grote economische schade, als herstel lang duurt of als er geen alternatieven voorhanden zijn, kan sprake zijn van grootschalige maatschappelijke ontwrichting. |
| Weerstand | De weerstand van een bedrijf heeft betrekking op de mate waarin het bedrijf zich tegen een aanslag of dreiging kan verweren. De weerstand van een bedrijf is te verbeteren aan de hand van de vijf schakels van de veiligheidsketen. |

# Bijlage II: afkortingenoverzicht

*NB: Afkortingen betreffen niet alleen de hoofdtekst maar ook de bijlagen.*

| | |
|---|---|
| **AIVD** | Algemene Inlichtingen- en Veiligheidsdienst |
| **BZK** | Binnenlandse Zaken en Koninkrijksrelaties |
| **CBB** | Coördinator Bewaking en Beveiliging |
| **CBRN** | Chemisch, Biologisch, Nucleair, Radiologisch |
| **CCB** | (Portefeuillehouder) Conflict- en Crisisbeheersing |
| **CCV** | Centrum voor Criminaliteitspreventie en Veiligheid |
| **CEN** | (European) Committee for Standardization |
| **C-TPAT** | Customs Trade Partnership Against Terrorism |
| **DB&B** | Dienst Bewaken en Beveiligen |
| **DTN** | Dreigingsbeeld Terrorisme Nederland |
| **DB3** | Directie Bewaken, Beveiliging en Burgerluchtvaart |
| **EOD** | Explosieven Opruimingsdienst |
| **EU** | Europese Unie |
| **EVO** | Eigen Vervoerders Organisatie |
| **IMO** | International Maritime Organization |
| **ISPS-Code** | International Ship and Port Facility Security Code |
| **KvK** | Kamer(s) van Koophandel |
| **MIVD** | Militaire Inlichtingen- en Veiligheidsdienst |
| **MKB** | Midden- en Kleinbedrijf |
| **NCTV** | Nationaal Coördinator Terrorismebestrijding en Veiligheid |
| **NDL** | Nederland Distributieland |
| **OM** | Openbaar Ministerie |
| **RFID** | Radio frequency identification |
| **TAPA** | Technology Asset Protection Association |
| **TLN** | Transport en Logistiek Nederland |
| **UCTA** | Unit Contraterrorisme en -activisme |
| **VPb** | Vereniging van Particuliere Beveiligingsorganisaties |
| **VvBO** | Verbond van Beveiligingsorganisaties |
| **WCO** | World Customs Organisation |



# Bijlage III: relevante websites

## Binnenland

| Site | Uitleg |
|---|---|
| www.aivd.nl | Site van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Deze site biedt inzicht in de organisatie en taken van de AIVD. De site bevat ook publicaties over terrorisme, AIVD- jaarverslagen en publicaties over bijv. veiligheidsrisico's. |
| www.evo.nl | Site van de Eigen Vervoerders Organisatie (EVO). Leden van 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. |
| www.hetccv.nl | Site van Centrum voor Criminaliteitspreventie en Veiligheid (CCV). Het 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 een thema 'ondernemen' opgenomen op de website. |
| www.justitie.nl | Site van het ministerie van Justitie. Op deze site wordt onder het thema 'criminaliteit' aandacht besteed aan terrorisme. |
| www.kvk.nl | Site van de Kamers van Koophandel (KvK). Op deze site wordt onder het thema 'wetten en regels' aandacht besteed aan 'veilig ondernemen'. Ook terrorisme komt aan de orde. |
| www.meldmisdaadanoniem.nl | 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. |
| www.meldpuntcybercrime.nl | 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 actie door politie, Justitie of opsporings- en inlichtingendiensten. |

| Site | Uitleg |
|---|---|
| www.mkb.nl | Site van MKB-Nederland. Op deze site is informatie over terrorismebestrijding te vinden bij de nieuwsberichten. Informatie over veilig ondernemen is beschikbaar onder ‘projecten’. |
| www.minbzk.nl | Site van het ministerie van BZK. Op deze site wordt onder het thema ‘veiligheid’ aandacht besteed aan terrorisme. Onder het thema ‘veiligheid’ is ook informatie beschikbaar over crisisbeheersing, bescherming vitale infrastructuur en de AIVD. |
| www.nctv.nl | Site van de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). De site verschaft o.a. informatie over het huidige dreigingsniveau en het Alerteringssysteem. De site bevat overheidsdocumentatie over terrorismebestrijding. |
| www.ndl.nl | Site van Nederland Distributieland (NDL). Op deze site wordt onder het thema ‘projecten / thema 1: Europese Logistieke Netwerken’, ingegaan op het project PROTECT. Diverse verslagen en publicaties zijn te downloaden. |
| www.om.nl | Site van het Openbaar Ministerie. Het OM is verantwoordelijk voor de opsporing en vervolging van strafbare feiten. De site bevat een dossier ‘terrorisme’. Daarnaast is het via het ‘thema’ parketten mogelijk door te klikken naar het Landelijk Parket. Dit Parket houdt zich bezig met de aanpak van o.a. terrorisme. |
| www.politie.nl | Site van Politie Nederland met informatie over de korpsen en het Nederlands Politie Instituut. Onder het thema ‘Politie ABC’ gaat ook de aandacht uit naar terrorisme. |
| www.tln.nl | Site van Transport en Logistiek Nederland (TLN). Op deze site komen onder het thema ‘visie / milieu en veiligheid’ onderwerpen verwant aan terrorisme aan de orde. |
| www.transumo.nl | Site van TRansition SUstainable MObility (Transumo), een platform van bedrijven, overheden en kennis¬instellingen die kennis ontwikkelen op het gebied van mobiliteit. Onder ‘projecten’ is informatie aanwezig over het project PROTECT. |
| www.veiligheid.minbzk.nl | Site van het ministerie van BZK over veiligheid. Op deze site wordt geen aandacht besteed aan terrorisme, maar onder ‘projecten’ wel aan aanverwante onderwerpen. |
| www.vno-ncw.nl | Site van VNO-NCW. Op deze site komt onder het thema ‘dossiers’ criminaliteitsbeheersing aan de orde. Hier worden nieuwsberichten ed. over terrorisme geplaatst. |



| Site | Uitleg |
|---|---|
| www.vvbo.nl | Site van het Verbond van Beveiligingsorganisaties (VvBO). Via deze site kunt u doorklikken naar alle aangesloten leden van VvBO, zoals de Vereniging van Particuliere Beveiligingsorganisaties (VPB). |

## Buitenland

| Site | Uitleg |
|---|---|
| www.cabinetoffice.gov.uk | Site van het kabinet van het Verenigd Koninkrijk. Onder ‘Security, Intelligence and Resilience’ is informatie beschikbaar verwant aan terrorisme. |
| www.cityoflondon.police.uk | Site van de City of London Police. Onder ‘Countering Terrorism’ is informatie beschikbaar over terrorisme. |
| www.cbp.gov | Site van U.S. Customs and Border Protection waarop aandacht voor C-TPAT: Customs Trade Partnership Against Terrorism. |
| www.dhs.gov/dhspublic | 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. |
| www.ec.europa.eu | 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. |
| www.homeoffice.gov.uk | 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. |
| www.mi5.gov.uk | Site van MI5: de veiligheidsdienst van het Verenigd Koninkrijk. Op deze is informatie beschikbaar over dreigingen, veiligheidsadviezen, te nemen maatregelen ed. Ook kunnen diverse brochures gedownload worden. |
| www.imo.org/home.asp | Site van International Maritime Organization, waarop uitgebreide informatie beschikbaar is over de IPS-Code. |
| www.iso.org | Site van ISO: International Organization for Standardization. Via het thema ‘products and services’ kunnen verschillende standaarden gevonden worden, zoals ook 28000. |
| www.niscc.gov.uk | Site van National Infrastructure Security Co-ordination Centre (NISCC). Site behandelt dreigingen tegen de vitale infrastructuur en geeft adviezen over een betere beveiliging. |

| Site | Uitleg |
|---|---|
| www.portsecuritytoolkit.com | 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. |
| www.ready.gov/business | 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. |
| www.security.homeoffice.gov.uk | Site van ministerie van Binnenlandse Zaken van het Verenigd Koninkrijk, specifiek gericht op 'security' en 'counter-terrorism strategy'. |
| www.tapaemea.com | Site over: Technology Asset Protection Association (TAPA). De site is ook in het Nederlands. |
| www.vbo-feb.be | Site van de Vereniging van Belgische ondernemingen. Op deze site is de handreiking Terrorisme en extremisme. *Welke maatregelen kunnen de bedrijven nemen?* te downloaden. |

# Bijlage IV: dreigingsniveaus Nederland

| Dreigingsniveaus in het Dreigingsbeeld Terrorisme Nederland | |
|---|---|
| **Niveau** | **Voorbeelden van criteria** |
| Minimaal | • Er is amper aanwezigheid van nationale en internationale terroristische netwerken.<br>• Het is niet waarschijnlijk dat aanslagen worden gepland.<br>• De open samenleving en het risicokarakter van een moderne samenleving houden dit niveau in stand. |
| Beperkt | • Er worden geen nieuwe trends of fenomenen onderkend.<br>• Aanslagen blijken te kunnen worden voorkomen.<br>• Nederland wordt niet of nauwelijks genoemd in verklaringen van serieus te nemen terroristische netwerken. |
| Substantieel | • Er worden nieuwe trends en fenomenen waar dreiging van uitgaat ontdekt.<br>• De kans dat een aanslag in Nederland zal plaatsvinden is reëel.<br>• Aanslagen vinden plaats in andere, met Nederland vergelijkbare landen.<br>• Radicalisering en rekrutering vinden op aanzienlijke schaal plaats.<br>• Nederland wordt geregeld genoemd in verklaringen van serieus te nemen terroristische netwerken. |
| Kritiek | • Er zijn zeer sterke aanwijzingen dat een aanslag in Nederland zal plaatsvinden.<br>• In Nederland heeft een aanslag plaatsgevonden en vervolgaanslagen zijn zeer waarschijnlijk.<br>• Nederland wordt vaak genoemd in zeer serieus te nemen verklaringen van terroristische netwerken en specifieke doelen worden daarbij serieus bedreigd. |

# Belangrijke telefoonnummers

| Situatie in kwestie | Telefoon | Bijzonderheden |
|---|---|---|
| Meldingen van verdachte of ongebruikelijke handelingen | Plaatselijke politie: 0900-8844 | Lokaal gesprekstarief |
| Anonieme meldingen | Meld Misdaad Anoniem: 0800-7000 | Van 08.00 tot 24.00 uur |
| Meldingen levensbedreigende situaties en heterdaad-meldingen van misdrijven | 112 | Alleen in spoedeisende gevallen |
| Advies over (structurele) maatregelen | Beveiligingsbureaus: zie www.vvbo.nl Plaatselijke politie: 0900-8844 | De politie heeft vooral kennis van maatregelen in het kader van criminaliteitsbestrijding. Meer specialistische kennis hebben beveiligingsbureaus. |
| Uitvoeren risicoanalyse | Beveiligingsbureaus: www.vvbo.nl | |
| Algemene informatie over terrorismebestrijding en bedrijven | Nationaal Coördinator Terrorismebestrijding en Veiligheid: www.nctv.nl 070-7515050 | |

**Uitgave**
Nationaal Coördinator Terrorismebestrijding en Veiligheid
Den Haag

*Meer informatie*
www.nctv.nl
info@nctv.minvenj.nl

November 2014