

# WAT DOET DE OVERHEID AAN TERRORISMEBESTRIJDING?

**U wilt meer weten over het antwoord op bovenstaande vraag. Hieronder volgt eerst de tekst van de website, daarna vindt u uitgebreidere informatie. Deze informatie is gebaseerd op de *'Handreiking voor bedrijven. Wat kan uw bedrijf ondernemen tegen terrorisme?'*, paragrafen 3.1, 3.2 en 3.3. De handreiking kunt u downloaden of bestellen op [www.nederlandtegenterrorisme.nl/bedrijven](http://www.nederlandtegenterrorisme.nl/bedrijven)**

## **Wat doet de lokale overheid?**

Op lokaal niveau werken politie en gemeenten samen om de veiligheid te vergroten. De gemeente is in eerste instantie verantwoordelijk voor de ontwikkeling en uitvoering van het lokale veiligheidsbeleid. Daaronder valt ook terrorismebestrijding.

De lokale politie is het eerste aanspreekpunt voor meldingen van dreiging van bedrijven of voor meldingen van verdachte handelingen of objecten.

Elke Nederlander is verantwoordelijk voor de veiligheid van zichzelf en zijn goederen. Ook bedrijven zijn zelf verantwoordelijk voor de beveiliging van hun terrein, gebouw en werknemers. Soms is de dreiging zo groot dat personen, organisaties of bedrijven zichzelf onvoldoende kunnen beveiligen. Deze kunnen hiervan melding maken bij de plaatselijke politie. Dan kunnen de politie, burgemeester en (hoofd)officier van justitie bepalen of en welke beveiligingsmaatregelen van de zijde van de overheid nodig zijn.

## **Wat doet de landelijke overheid?**

De landelijke overheid doet veel om de kans op terroristische dreigingen te verkleinen. Op 1 januari 2005 is de Nationaal Coördinator Terrorismebestrijding (NCTb) ingesteld. De NCTb coördineert de terrorismebestrijding in Nederland.

De NCTb bekijkt de dreiging vanuit verschillende invalshoeken: de algemene dreiging voor Nederland, de dreiging tegen vitale

bedrijfssectoren en de dreiging tegen een object, dienst of persoon. Voor elke invalshoek heeft de NCTb een systeem ontwikkeld om tijdig het beleid aan te passen of maatregelen te nemen. Meer informatie over de NCTb is te vinden op [www.ncbt.nl](http://www.ncbt.nl)

## **Wat gebeurt er op Europees en internationaal niveau?**

Veel bedrijven hebben te maken met internationale of Europese regelgeving over terrorisme en/of beveiliging. Deze regelgeving is volop in beweging. De Europese en internationale gemeenschap ontwikkelen regels op het gebied van:

- bescherming van Europese vitale infrastructuur met grensoverschrijdende effecten. Kijk voor actuele informatie op [www.ec.europa.eu/justice\\_home/funding/epcip/funding\\_epcip\\_en.htm](http://www.ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm)
- beveiliging van havens en zeeschepen. Kijk voor praktische tips op [www.portsecuritytoolkit.com](http://www.portsecuritytoolkit.com), [www.portfacilitysecurity.nl/criminaliteit](http://www.portfacilitysecurity.nl/criminaliteit) en <http://ec.europa.eu/transport/maritime>.
- bescherming van de luchtvaart tegen terroristische aanslagen. Meer informatie is te vinden op [www.ec.europa.eu/transport/air\\_portal](http://www.ec.europa.eu/transport/air_portal) en [www.ncbt.nl](http://www.ncbt.nl)
- verbetering van de beveiliging van bevoorradingsketens. Voor meer informatie zie [www.ec.europa.eu/dgs/energy\\_transport/security](http://www.ec.europa.eu/dgs/energy_transport/security) en [www.ec.europa.eu/transport](http://www.ec.europa.eu/transport)
- veiligheidseisen ten behoeve van douanecontroles. Voor meer informatie zie [www.ec.europa.eu/dgs/taxation\\_customs](http://www.ec.europa.eu/dgs/taxation_customs), [www.eur-lex.europa.eu/nl](http://www.eur-lex.europa.eu/nl) en [www.minfin.nl](http://www.minfin.nl)

## **1. LOKAAL**

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

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

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

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

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

Het korps regiopolitie Kennemerland realiseerde zich dat er in de regio meer bedrijven doelwit of middel kunnen zijn voor terroristen. Daarom organiseerde de politie in juni 2006 een conferentie voor bedrijven en lokale autoriteiten om de bewustwording over risico's te versterken.

Ook stelde de politie een contactpunt in bij het veiligheidsbureau Kennemerland die bedrijven op weg helpt als ze vragen hebben over terrorismebestrijding. Het veiligheidsbureau zet bovendien een platform op voor bedrijven waarin best practices uitgewisseld kunnen worden.

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

Elke Nederlander is verantwoordelijk voor de veiligheid van zijn eigen persoon en goederen. Zo moet iedereen zelf zorgen

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

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

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

Op basis van de informatie van de afdeling Conflict- en Crisisbeheersing wegen de burgemeester, de (hoofd)officier van justitie en de korpschef - die gezamenlijk de zogenoemde driehoek vormen - de ernst en waarschijnlijkheid van de dreiging. De driehoek bepaalt of en welke beveiligingsmaatregelen van de zijde van de overheid nodig zijn. Hoe ernstiger en waarschijnlijker een dreiging is, hoe zwaarder het maatregelenpakket. De politie voert de beveiligingsmaatregelen uit.

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

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

De lokale autoriteiten onderhouden het contact met de bedreigde persoon, instelling of bedrijf over de genomen beveiligingsmaatregelen. De plaatselijke politie voert deze maatregelen uit en kan daarbij gebruikmaken van faciliteiten van de landelijke overheid. Zo kan de Dienst Koninklijke en Diplomatieke Beveiliging (DKDB) van het Korps Landelijke Politiediensten (KLPD) worden gevraagd om persoonsbeveiliging. Daarnaast nemen bedrijven ook zelf maatregelen en stellen de politie daarvan in kennis. Bedrijven kunnen bij een (particuliere) veiligheidsadviseur advies inwinnen over maatregelen die passen bij de aard van het bedrijf of navraag doen bij hun brancheorganisatie.

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

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

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

## **2. LANDELIJK**

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

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

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

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

De NCTb bekijkt terroristische dreigingen vanuit drie invalshoeken:

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

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

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

## **2.2 HET ALGEMENE DREIGINGSBEELD**

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

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

Er zijn in Nederland vier dreigingsniveaus: minimaal, beperkt, substantieel en kritiek. Sinds voorjaar 2007 is de terroristische dreiging 'beperkt'. Dat betekent dat de kans gering is dat er in ons land een aanslag zal plaatsvinden. Helemaal uit te sluiten is een aanslag niet. Het dreigingsbeeld is onder meer gebaseerd op het beeld dat terroristen hebben van ons land. Deelname aan internationale vredesoperaties en het maatschappelijk debat over de islam kunnen dit beeld beïnvloeden. Binnenlandse radicalisering en de aanwezigheid van netwerken beïnvloeden eveneens de kans op een terroristische aanslag.

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

## **2.3 DREIGING TEGEN EEN SECTOR**

Het Alerteringsysteem Terrorismebestrijding is een waarschuwingssysteem voor overheden en bedrijven. Het waarschuwt ministeries, provincies en gemeenten, politie, inlichtingendiensten en de aangesloten bedrijfssectoren als er een verhoogde dreiging is. Overheidsdiensten en betrokken bedrijfssectoren kunnen zo snel adequate maatregelen nemen als er een verhoogde dreiging is.

### **Aangesloten bedrijfssectoren Alerteringsysteem Terrorismebestrijding (vanaf 1 juli 2007)**

- |                         |                              |
|-------------------------|------------------------------|
| 1. Luchthavens          | 8. Stads- en streekvervoer   |
| 2. Zeehavens            | 9. Financiële sector         |
| 3. Drinkwatersector     | 10. Oliesector               |
| 4. Spoorsector          | 11. Chemiesector             |
| 5. Gassector            | 12. Hotelsector              |
| 6. Elektriciteitssector | 13. Evenementensector        |
| 7. Nucleaire sector     | 14. Tunnels en waterkeringen |

Het Alerteringssysteem heeft vier niveaus: het basisniveau en een lichte, matige en hoge dreiging. Elk niveau en elke sector heeft zijn eigen maatregelenpakket. Bij het 'basisniveau' zijn dit maatregelen die tot de reguliere bedrijfsvoering horen. Hoe hoger het alerteringsniveau, hoe zwaarder en ingrijpender de maatregelen zijn.

De NCTb sluit bedrijfssectoren aan bij het Alerteringssysteem als ze van vitaal belang zijn voor Nederland en/of een aantrekkelijk doelwit zijn voor terroristen. De alerteringsniveaus van de aangesloten bedrijfssectoren staan vermeld op

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

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

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

De minister van Justitie besluit in overleg met de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) over de verhoging of verlaging van het alerteringsniveau. Hij doet dit op basis van een dreigingsanalyse die de NCTb opstelt.

Voordat de minister een besluit neemt vindt overleg plaats met de meest relevante partijen. In ieder geval met de politie en de bedrijfssector. Zij formuleren samen met de NCTb een advies over de maatregelen die een bedrijf kan nemen. De bedrijven voeren de maatregelen vrijwillig uit en betalen de kosten ervan. Het lokale bestuur is grotendeels verantwoordelijk voor de uitvoering van de overheidsmaatregelen. Maatregelen die aangesloten sectoren bij een verhoogde dreiging nemen, kunnen merkbaar zijn voor niet aangesloten bedrijven en het publiek.

### Lichte dreiging op het spoor

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

## 2.4 BESCHERMING VITALE INFRASTRUCTUUR

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

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

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

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

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

#### Sectoren vitale infrastructuur

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

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

voorwaarden veelal informatie over dreigingen en ondersteunt op deze wijze de uitvoering van risicoanalyses.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft samen met de vitale bedrijfssectoren, diverse ministeries, de AIVD, de NCTb en de politie in Nederland een Nationaal Adviescentrum Vitale Infrastructuur (NAVI) ingesteld. Het NAVI is op 1 april 2007 gestart. Het adviescentrum gaat een bijdrage leveren aan de structurele verhoging van de veiligheid van de vitale infrastructuur. Ook gaat het NAVI de informatie-uitwisseling op het terrein van beveiliging tussen overheden en de vitale bedrijfssectoren bevorderen. Het adviescentrum kan expertise en kennis over maatregelen en best practices bundelen. Kijk voor actuele informatie over het NAVI en de taken van deze organisatie op

[www.navi-online.nl](http://www.navi-online.nl)

### 3. INTERNATIONAAL EN EUROPEES

Veel bedrijven hebben te maken met internationale of Europese regelgeving over terrorisme en/of beveiliging. Deze regelgeving is volop in beweging. Zo ontwikkelt de Europese Unie (EU) een 'European Programme for Critical Infrastructure Protection' (EPCIP). Dit programma omvat de bescherming van Europese vitale infrastructuur met grensoverschrijdende effecten. Naar verwachting treedt het EPCIP eind 2007 in werking. Kijk voor actuele informatie op [http://ec.europa.eu/justice\\_home/funding/epcip/funding\\_epcip\\_en.htm](http://ec.europa.eu/justice_home/funding/epcip/funding_epcip_en.htm).

Mede door de vele ontwikkelingen op het gebied van logistiek, verkeer, water en luchtvaart besloten bedrijven, de landelijke overheid en kennisinstellingen samen te werken in het Transumo-project 'Protect'. Doel is te kijken hoe bedrijven en de landelijke overheid internationale goederenstromen veiliger kunnen maken. Zie voor meer informatie [www.protect.transumo.nl](http://www.protect.transumo.nl)

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

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

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

Voor het opstellen van veiligheidsplannen is ook een toolkit ontworpen. Deze toolkit en informatie over de ISPS-Code is te vinden op [www.portsecuritytoolkit.com](http://www.portsecuritytoolkit.com), [www.portfacilitysecurity.nl/criminaliteit](http://www.portfacilitysecurity.nl/criminaliteit) of <http://ec.europa.eu/transport/maritime>

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

### **3.2 KETENBEVEILIGING**

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

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

De EU heeft een verordening aan de lidstaten voorgesteld om de beveiliging van de bevoorradingketens te verbeteren en het Europese goederenvervoer beter tegen mogelijke terroristische aanslagen te beschermen. Deze conceptverordening moet het verschil tussen de beveiliging van schepen, havens en de luchtvaart én andere vervoersmodaliteiten opheffen. De bevoorradingketen omvat alle vervoershandelingen en de daarmee verbonden handelingen en processen vanaf de productielocatie tot op de plaats van bestemming van de goederen. Bedrijven die - vrijwillig - voldoen aan eisen rond fysieke veiligheid, toegangscontrole, veilige procedures, veiligheid voor het personeel, registratieprocedures, informatiebeveiliging en opleiding en bewustmaking, kunnen erkend worden als 'veilige exploitant'. Deze erkenning kan in de toekomst praktische voordelen bij veiligheidscontroles zoals douanecontroles opleveren. In december 2006 heeft de Europese Commissie besloten het voorstel voor de ketenverordening voor een periode van twee jaar te bevriezen. De Commissie heroverweegt de behoefte aan de verordening mede in het licht van de recent gewijzigde douanewetgeving (introductie van het beginsel van 'geautoriseerde marktdeelnemer').

Voor meer informatie zie [www.ec.europa.eu/dgs/energy\\_transport](http://www.ec.europa.eu/dgs/energy_transport) en [www.ec.europa.eu/transport](http://www.ec.europa.eu/transport)

Alle EU-lidstaten moeten per 1 januari 2008 het beginsel van 'geautoriseerde marktdeelnemer' (Authorised Economic Operator, AEO) in de douanewetgeving invoeren. De bedoeling is om een onderscheid te maken tussen bedrijven die investeren in beveiliging en bedrijven die dat niet doen. Het gaat bijvoorbeeld om maatregelen ter beveiliging van de automatisering en gebouwen. Een bedrijf dat deze investeringen maakt, krijgt de status van 'geautoriseerde marktdeelnemer'. Hij moet daarvoor een vergunning bij de douane aanvragen. Bedrijven met zo'n status hoeven minder informatie aan te leveren bij de douane. Ook zullen zij waarschijnlijk minder controles aan de buitengrens moeten ondergaan. Daarnaast moeten bedrijven vanaf 2009 voorafgaand aan invoer en uitvoer van goederen informatie aanleveren aan de douane. De douane kan dan een goede risicoanalyse uitvoeren. Voor meer informatie

[www.ec.europa.eu/dgs/taxation\\_customs](http://www.ec.europa.eu/dgs/taxation_customs), [www.eur-lex.europa.eu/nl](http://www.eur-lex.europa.eu/nl) en [www.minfin.nl](http://www.minfin.nl).

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

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

