Beheersing van criminaliteitsrisico's door het bedrijfsleven

Jan Terpstra

Het bedrijfsleven wordt steeds meer gevraagd verantwoordelijkheid te nemen in de aanpak van onveiligheid. Maar wat doet het bedrijfsleven in de praktijk op dit punt? Voor drie bedrijfstakken (transport, banken en muziekindustrie) is nagegaan welke strategieën het bedrijfsleven hanteert ten aanzien van risico's van georganiseerde criminaliteit. Onderscheid wordt gemaakt in drie categorieën strategieën, namelijk strategieën gericht op beïnvloeding van randvoorwaarden voor criminaliteitsreductie, preventieve strategieën en reactieve strategieën. Tot slot wordt ingegaan op factoren die van invloed zijn op de mate waarin het bedrijfsleven zich met de aanpak van deze veiligheidsrisico's bezighoudt en komt de verhouding bedrijfsleven–overheid op dit terrein kort aan bod.

1 Inleiding

Sinds ongeveer twee decennia zijn de heersende opvattingen over veiligheidszorg sterk in verandering. De zorg voor veiligheid wordt niet meer gezien als alleen een taak van overheid, politie en justitie. Ook van bedrijven wordt verwacht dat zij bijdragen aan het voorkomen en bestrijden van onveiligheid. Een nieuwe verantwoordelijkheidsverdeling is ontstaan met andere verhoudingen tussen partijen. Met deze nieuwe 'governance of security' (Johnston & Shearing 2003) zijn ook de posities van politie en overheid veranderd. De overheid zou slechts op afstand opereren (Rose & Miller 1992), vooral sturen waar anderen het eigenlijke werk doen (Osborne & Gaebler 1992) of één van de vele 'knopen' zijn in een complex van netwerken (Wood & Shearing 2007).

Deze ontwikkelingen roepen vele vragen op. Van bedrijven worden bijdragen verwacht in de veiligheidszorg, maar wat doet het bedrijfsleven in de praktijk hieraan? Deze vraag staat hier centraal. Daarbij concentreert de aandacht zich op de wijze waarop het bedrijfsleven omgaat met risico´s van georganiseerde criminaliteit. Deze risico's zijn vaak complex, kunnen langdurig optreden, grote schade veroorzaken en zijn moeilijk aan te pakken. Juist hier kan zicht worden verkregen op de wijze waarop het bedrijfsleven met deze verantwoordelijkheden voor veiligheid omgaat. Tot slot komt kort aan bod hoe de aanpak van het bedrijfsleven zich verhoudt tot de inbreng van de overheid.

De risico's van georganiseerde criminaliteit voor het bedrijfsleven kunnen worden onderverdeeld in drie categorieën. Ten eerste kan een bedrijf direct slachtoffer zijn, zoals bij diefstal, oplichting of productvervalsing. Ten tweede kan sprake zijn van 'institutioneel misbruik' van een bedrijf. Criminele groepen maken daarbij misbruik van informatie, deskundigheid, faciliteiten of reputatie van een bedrijf voor de eigen illegale doelen. Het bedrijf moet daarbij schijnbaar

'normaal' blijven functioneren. Een bedrijf kan zo dienen als *facilitator* of *front* voor illegale activiteiten. Ten derde kunnen bedrijven in een corrupte omgeving opereren. Dit kan ertoe leiden dat zij praktijken en normen overnemen die daar gelden. Daarbij kunnen legale en illegale activiteiten binnen een bedrijf door elkaar gaan lopen.

Dit artikel is gebaseerd op een analyse van strategieën ten aanzien van risico's van georganiseerde criminaliteit gehanteerd door het bedrijfsleven in het goederentransport (over de weg en in de Rotterdamse haven), banken en muziekindustrie. Deze sectoren zijn gekozen omdat zij met uiteenlopende risico's worden geconfronteerd en verschillen in structuur en marktcondities. Bij de analyse is gebruikgemaakt van documenten, interviews met sleutelpersonen, aangevuld met literatuur.[1]

2 Risico's en risicobesef

Afhankelijk van de bedrijfstak heeft in Nederland 25 tot 45% van de bedrijven jaarlijks te maken met criminaliteit. De financiële schade daarvan voor het bedrijfsleven zou jaarlijks € 569 miljoen bedragen (WODC 2006). Hoe groot het aandeel georganiseerde criminaliteit hierin is, is onbekend.

Risico's van georganiseerde criminaliteit verschillen deels per bedrijfstak. Deze hangen samen met de specifieke kwetsbaarheid van economische sectoren, de gelegenheid die zij bieden voor criminaliteit en hun criminele aantrekkingskracht. Geïnterviewden veronderstellen vaak dat de schade veroorzaakt door georganiseerde criminaliteit voor het bedrijfsleven de laatste decennia sterk is toegenomen. Bij gebrek aan betrouwbare data bestaat hierop echter geen nauwkeurig zicht. Wel is vermoedelijk de aard van deze risico's veranderd. Zo waren in de jaren vijftig en begin jaren zestig kluiskrakers het grootste criminaliteitsrisico voor Nederlandse banken. Vanaf eind jaren zestig tot midden jaren tachtig werden bankovervallen het grootste probleem, terwijl de traditionele kluiskraker geleidelijk uit beeld verdween. Veranderingen in beveiliging van banken en in dienstverlening, waardoor bankfilialen minder contant geld in voorraad kregen, leidden ertoe dat bankovervallen in belang afnamen. Onder invloed van de opbloeiende drugseconomie kregen banken vanaf eind jaren tachtig te maken met nieuwe problemen, zoals witwassen en criminele groeperingen die probeerden via banken illegaal verkregen geld te investeren in de reguliere economie.

Op basis van deze studie kan niet worden vastgesteld in hoeverre het bedrijfsleven voldoende investeert in preventie en bestrijding van risico's van georganiseerde criminaliteit. Uit de interviews kan worden afgeleid dat sinds midden jaren negentig zich hierin belangrijke veranderingen hebben voorgedaan. In elk van de onderscheiden bedrijfstakken lijkt het algemeen risicobesef te zijn toegenomen.

1 Een deel van de informatie is verzameld binnen het IKOC-project. Uitgebreidere verantwoording en beschrijving van resultaten vindt plaats in latere publicatie over dit project.

Op velerlei manieren is sinds die tijd samenwerking ontstaan tussen bedrijven, politie en overheid rond de aanpak van onveiligheid. Voorbeeld hiervan is het Actieplan Veilig Ondernemen waaraan ministeries, OM, politie, werkgeversorganisaties, VNG en brancheorganisaties deelnemen. Dit startte in 2004 en loopt voorlopig door tot 2010. Vele projecten rond uiteenlopende veiligheidsproblemen maken hier onderdeel van uit, zoals het convenant Aanpak Criminaliteit Wegtransport of Veiligheid van Kleinere Bedrijven.

De afgelopen jaren wordt vanuit (inter)nationale overheden meer druk uitgeoefend op bedrijven om veiligheidsmaatregelen te treffen en aan hogere securitynormen te voldoen. De 'War on Terrorism' heeft sinds 2001 in korte tijd tot een sterke toename geleid van de beveiligingseisen aan bedrijven in diverse sectoren (George & Whatford 2007). Deze worden ook ingezet tegen (georganiseerde) criminaliteit. Een voorbeeld hiervan is de *International Ship and Port Facility Security* (ISPS)-code, in 2002 ingevoerd door de International Maritime Organization (IMO) en grotendeels overgenomen door de EU. Met deze code moeten havenbedrijven en rederijen voldoen aan nieuwe, striktere beveiligingsmaatregelen. Met de invoering van de ISPS-code moeten bedrijven in de Rotterdamse haven vanaf 2004 een *Port Facility Security Plan* kunnen overleggen. Indien bedrijven niet over een dergelijk goedgekeurd plan beschikken, kunnen zij worden uitgesloten van handel met de VS

Afgaande op de interviews verschillen bedrijven en bedrijfstakken sterk in de mate van beveiliging en risk management. Veel banken en grote internationale ondernemingen beschikken over gespecialiseerde afdelingen, met deskundigheid rond risk en security management. Daarentegen voldoen kleine bedrijven, bijvoorbeeld in het weggoederentransport, vaak niet aan tamelijk simpele beveiligingseisen.

3 Strategieën

De strategieën vanuit het bedrijfsleven met betrekking tot risico's van georganiseerde criminaliteit, kunnen worden onderverdeeld in drie categorieën (schema I). Ten eerste zijn er strategieën ter beïnvloeding van de randvoorwaarden voor criminaliteitsreductie. Daarnaast bestaan strategieën die meer rechtstreeks zijn gericht op het voorkomen van georganiseerde criminaliteit. Tot slot zijn er reactieve strategieën met als doel vermindering van de gevolgen van criminaliteit. Deze bestaan niet zozeer uit repressie (zoals bij reactieve werkwijzen vanuit de publieke sector), maar zijn vooral gericht op herstel of compensatie van geleden schade. In tegenstelling tot de aanpak van politie of justitie is het bedrijfsleven niet zozeer gericht in haar aanpak op *daders*, maar op *daden* (Levi & Maguire 2004). Een deel van deze strategieën wordt uitgevoerd door bedrijfstak- of werkgeversorganisaties, andere door individuele ondernemingen.

Schema 1 Strategieën van bedrijfsleven gericht op risico's van georganiseerde criminaliteit

Gericht op randvoorwaarden	**Gericht op criminaliteitspreventie**	**Reactieve strategieën**
– Op bedrijfstakniveau: • beïnvloeden politieke agenda, regelgeving en handhaving; • bevordering risicobewustzijn en deskundigheid met betrekking tot risicomanagement; • bevordering samenwerking tussen bedrijven; • bevordering samenwerking tussen private en publieke partijen op bedrijfstakniveau. – Op bedrijfsniveau: • versterking deskundigheid met betrekking tot security management; • nakomen van regels en toezichtseisen met betrekking tot veiligheid.	– Beveiligingsmaatregelen: • fysieke en techno-beveiliging; • personele beveiliging. – Screenen en selectie nieuw personeel – Controle en toezicht op werknemers – Rapportagesystemen – Aanpassingen routine-activiteiten – Aanpassing productieproces – Vaststellen betrouwbaarheid van (potentiële) klanten en opdrachtgevers – Vaststellen van beheersmatige en formele eisen aan procedures en werkprocessen (en controle op naleving daarvan) – Creëren alternatief voor illegale markten en producten	– Melding en aangifte bij politie – Opsporen gestolen goederen en voertuigen – Zoeken van verhaal, herstel of compensatie voor geleden verlies

Alvorens in te gaan op deze strategieën, twee kanttekeningen. Ten eerste: voor bedrijven kan onduidelijk of irrelevant zijn of risico's gevolg zijn van georganiseerde criminaliteit of van andere vormen van criminaliteit (Bouloukos, Farell en Laycock 2003). Ten tweede: veel strategieën zijn (deels) ingegeven door andere motieven dan criminaliteitsreductie, zoals kosten-batenoverwegingen (Levi en Maguire 2004; Challinger 2006).

Strategieën gericht op randvoorwaarden

Bedrijfstakorganisaties proberen op verschillende manieren overheden te overtuigen van de ernst van de gevolgen van georganiseerde criminaliteit voor hun bedrijfstak. Zij pleiten bijvoorbeeld voor (nieuwe) regels, maatregelen en meer toezicht. Zo heeft de internationale (lobby)organisatie van de muziekindustrie IFPI als doel overheden en handhavers over deze risico's te informeren en hen te 'beïnvloeden' (IFPI 2005).

Deze organisaties proberen ook hun achterban bewuster te maken van de risico's van georganiseerde misdaad. TNL en EVO, twee brancheorganisaties in de transportsector, hebben handboeken uitgebracht met daarin honderden concrete maatregelen voor bedrijven om deze risico's te beperken. Deze bedrijfstak-

organisaties organiseren ook cursussen en trainingen rond veiligheid en security management.

Deze organisaties trachten ook de samenwerking tussen bedrijven onderling te versterken. Een voorbeeld hiervan zijn 'zwarte lijsten' waarbij namen van 'verdachte' bedrijven en personen worden uitgewisseld. Ook wordt informatie over 'best practices' uitgewisseld, worden gemeenschappelijkke veiligheidsplannen bevorderd (zoals in de Rotterdamse haven), of maatregelen om de toegang tot een bedrijfstak te bewaken. Zo worden in het Europees wegtransport eisen gesteld aan ondernemers, niet alleen met betrekking tot financiële positie en professionele competentie, maar ook reputatie (Bucquoye, et al. 2005; KPMG 2000).

Samenwerking met publieke partijen vormt eveneens een belangrijk aandachtspunt, ook in de strijd tegen georganiseerde misdaad (Schneider, Beare & Hill 2000). In regionale en nationale platforms voor criminaliteitsbeheersing werken publieke en private partijen samen rond de aanpak van uiteenlopende veiligheidsproblemen. Daarnaast bestaan vele lokale veiligheidsnetwerken bij bijvoorbeeld winkelcentra en industrieterreinen. Een recent voorbeeld hiervan is de Regionale Toezicht Ruimte waarin 24 uur per dag beelden en informatie worden uitgewisseld tussen politie, bedrijven en particuliere beveiligers. Ook bestaan internationale samenwerkingsverbanden, zoals in de transportsector rond het TIR-systeem of meer recente C-TPAT, ontstaan in het kader van de strijd tegen terrorisme. In beide gevallen krijgen bedrijven die voldoen aan bepaalde (veiligheids)eisen voordelen bij grensoverschrijdend verkeer.

Ook op ondernemings- en vestigingsniveau bestaan strategieën die gericht zijn op randvoorwaarden voor criminaliteitsreductie. De afgelopen twee decennia hebben banken omvangrijke afdelingen gecreëerd met specialistische deskundigheid rond de beheersing van uiteenlopende veiligheidsrisico's. Deze afdelingen stellen onder meer risicoanalyses op als basis voor 'security plans' bij uiteenlopende risico's, evenals 'veiligheidseffectrapportages.' In kleine ondernemingen, zoals in het wegtransport, ontbreekt deze deskundigheid nagenoeg geheel.

Aan bedrijven in uiteenlopende bedrijfstakken worden steeds meer eisen gesteld met betrekking tot veiligheid. Deze moeten onder meer de externe verantwoording op dit punt vergroten. Soms zijn deze eisen door overheden opgelegd, soms is sprake van (al dan niet afgedwongen) zelfregulering. De *War on terrorism* heeft deze ontwikkeling versterkt. De genoemde ISPS-code voor de internationale scheepvaart is hiervan een voorbeeld.

Preventiestrategieën

Bedrijven hanteren ook strategieën die directer gericht zijn op het voorkomen van (georganiseerde) criminaliteit. Telkens gaat het daarbij om vermindering van de gelegenheid en opbrengsten van criminaliteit en het vergroten van de daarmee gemoeide inspanningen en kosten (Clarke 1997). De volgende strategieën kunnen worden onderscheiden:

– *Beveiligingsmaatregelen*
  Naast traditionele fysieke beveiliging (zoals hekwerk, hang- en sluitwerk, kogelvrij glas, alarmsystemen) zijn er nieuwe vormen van technobeveiliging,

zoals 'driver recognition systems' ter voorkoming van diefstal van vrachtauto's (Bucquoye, et al. 2005; Albrecht 1998). Met de opmars van internet en cybercrime zijn data- en computerbeveiliging voor bedrijven belangrijk geworden. Daarnaast blijft personele beveiliging belangrijk. Niet alleen worden beveiligingsmedewerkers ingezet voor bewaking en beveiliging van gebouwen, maar bijvoorbeeld ook om colonnes van vrachtauto's naar onveilige gebieden te begeleiden en te bewaken. Deels gaat het om ingehuurde medewerkers van gespecialiseerde beveiligingsbedrijven.

– *Screening en toezicht*
  Vaak wordt het belang van screening van nieuwe werknemers benadrukt om risico's van georganiseerde criminaliteit te voorkomen. Zo wordt in het wegtransportverkeer een verklaring van goed gedrag vereist. In de praktijk gebeurt dat niet altijd, onder meer omdat in deze sector veel tijdelijke of inhuurkrachten worden gebruikt. Vooral grotere ondernemingen hebben gedragscodes als onderdeel van integriteitsprogramma's, mede met als doel criminaliteitsrisico's tegen te gaan. De effectiviteit van deze codes wordt soms betwijfeld (vgl. Levi 2006), mede omdat verantwoording en toezicht op de naleving daarvan soms worden overgelaten aan informele en persoonlijke initiatieven van directe leidinggevenden. Ook op allerlei andere manieren wordt toezicht gehouden op werknemers, onder meer via toegangscontrole (ook met biometrische vormen van identificatie) of (bij vrachtwagenchauffeurs) via een digitale tachograaf.
– *Rapportagesystemen*
  Om risico's tegen te gaan, wordt werknemers de mogelijkheid geboden gesignaleerde regelovertredingen te melden, zonder dat zij bang hoeven te zijn voor repercussies. Dit kan door het instellen van een 'vertrouwenspersoon'. Ervaringen met klokkenluiderprocedures suggereren dat dit in de praktijk niet onproblematisch is. Ook al stelt de bedrijfsleiding zich open voor dergelijke signalen, directe collega's of leidinggevenden kunnen een 'verklikker' toch negatief behandelen.
– *Aanpassingen routine-activiteiten en productieproces*
  Bedrijven proberen criminaliteit tegen te gaan door aanpassingen van de dagelijkse, deels vanzelfsprekende gedragspatronen van werknemers. Dit past bij de routine-activiteitentheorie (Felson, 1998). Voorbeelden hiervan zijn lijsten met praktische tips voor vrachtwagenchauffeurs om de gelegenheid tot diefstal van hun vracht te verminderen.[2] Nog verder gaan aanpassingen in producten of productieprocessen om de kans op criminaliteit te verminderen. Zo hebben banken sinds de jaren zestig vele aanpassingen aangebracht om de telkens veranderende risico's tegen te gaan waarmee zij werden geconfronteerd. In eerste instantie ging de aandacht vooral uit naar betere beveiliging van kluizen. Toen bankovervallen vanaf eind jaren zestig een groeiend probleem werden, werd beveiliging gezocht in gesloten balies en kogelvrij glas. Begin jaren negentig besloten de banken tot koerswijziging en te streven naar

2 Zie *Transport en Logistiek*, 2004/10, 8-9.

zo weinig mogelijk contant geld aan hun balies. Daarom werd gekozen voor massale invoering van betaalautomaten. In de muziekindustrie probeert men al jarenlang (met overigens weinig succes) met behulp van technologische oplossingen de cd-piraterij tegen te gaan en zo te komen tot productbescherming (Brunelli & Vettori 2005).

– *Vaststellen betrouwbaarheid*
  Ook het vaststellen van de betrouwbaarheid van klanten, partners en opdrachtgevers kan van groot belang zijn. Deze screening kan zich richten op financiële betrouwbaarheid of eventuele illegale praktijken. Hierbij wordt soms gebruikgemaakt van externe informatie, van branchegenoten, soms ook van bedrijven die gespecialiseerd zijn in het verzamelen en verstrekken van dergelijke informatie (als *World-Check*). Soms worden aan partners formele eisen gesteld ten aanzien van maatregelen tegen fraude en corruptie.
– *Administratieve en formele eisen*
  Om risico's van georganiseerde criminaliteit te verminderen, leggen overheden uiteenlopende regels op aan bedrijven. Sinds de jaren negentig eisen verschillende Europese landen van financiële instellingen dat zij mogelijk risicovolle transacties rapporteren. In Nederland bestaat de verplichting tot melding van ongebruikelijke transacties. In 2005 werden ruim 180.000 meldingen gedaan, maar deze krijgen weinig follow-up. Jaarlijks komt het slechts in ongeveer 130 gevallen tot een rechtszaak (Adviescommissie Informatiestromen 2007).
– *Creëren legale alternatieven*
  Eén van de manieren om criminaliteit tegen te gaan is door de (potentiële) beloning van handel in illegale goederen te verminderen. Dit kan door alternatieve markten te creëren waar consumenten legale goederen kunnen kopen voor een prijs die concurreert met het illegale aanbod. Deze strategie volgt de muziekindustrie bij haar strijd tegen cd-piraterij: *music on demand*.

Reactieve strategieën

Drie categorieën reactieve strategieën kunnen worden onderscheiden. Ten eerste, melding van criminaliteit door bedrijven bij de politie. Bedrijven zijn hier soms tamelijk terughoudend mee. Slechte ervaringen met de politie, gebrek aan vertrouwen in de opbrengst van die stap en vrees voor reputatiebeschadiging spelen daarbij een rol (Van Dijk et al. 1999; Johnston et al. 1994; Hardie & Hobbs 2002). In de muzieksector verricht de Stichting Brein zelf opsporingsonderzoek naar gevallen van cd-piraterij en -plagiaat. Op basis hiervan kunnen civielrechtelijke zaken worden gestart of wordt informatie aangeleverd bij de FIOD-ECD in de hoop dat dit leidt tot strafrechtelijke stappen.

Ten tweede proberen bedrijven soms gestolen spullen op te sporen. In het goederenwegtransport wordt met satellietnavigatie, *positioning systems* en G(R)PS de locatie van vrachtauto's bepaald. Dit systeem wordt ook gebruikt om te achterhalen waar een gestolen vrachtauto of oplegger is. Gespecialiseerde bedrijven leveren deze *tracking and tracing services*. Naar schatting één op de drie Nederlandse wegtransportbedrijven maakt hiervan gebruik. Ook 'taggingsystemen', bekend uit kledingzaken, worden door transportbedrijven gebruikt om gestolen

waar te achterhalen. Tot slot proberen bedrijven schade veroorzaakt door criminaliteit op uiteenlopende wijzen te herstellen, te compenseren of te verhalen.

4 Belemmeringen

Verschillende factoren kunnen ertoe bijdragen dat binnen het bedrijfsleven de ontwikkeling van preventie- en controlemaatregelen tegen (georganiseerde) criminaliteit belemmerd wordt. Deze factoren kunnen per bedrijfstak en bedrijf verschillen. Deels bij wijze van hypothese worden hier de (vermoedelijk) belangrijkste factoren op een rij gezet.

a Ten eerste kan er onvoldoende besef zijn van de risico's van georganiseerde criminaliteit voor bedrijf of bedrijfstak. Het belang van veiligheidsmaatregelen wordt lang niet altijd ingezien (Challinger 2006). Soms worden deze maatregelen primair gezien als verantwoordelijkheid van overheid of politie (Chamard 2006).

b Ook kan betrouwbare informatie ontbreken, bijvoorbeeld over de financiële gevolgen van (deze) criminaliteit. Gebrek aan deskundigheid met betrekking tot veiligheidszorg kan hierbij een rol spelen. Vooral banken en grote internationale ondernemingen hebben de afgelopen jaren veel geïnvesteerd in professionalisering van hun security management.

c Bedrijven zijn terughoudend met veiligheidsmaatregelen als zij veronderstellen dat deze het normale productieproces zullen verstoren en tot financiële last zullen zijn. Vaak worden veiligheidsmaatregelen alleen geaccepteerd als zij de concurrentiepositie niet schaden of ook gelden voor concurrerende bedrijven. In de Rotterdamse haven wordt daarom nauwlettend gevolgd hoe 'Antwerpen' en 'Hamburg' omgaan met nieuwe veiligheidseisen opgelegd door internationale regelgeving.

d Zolang een onderneming in staat is de financiële gevolgen van (georganiseerde) criminaliteit af te schuiven op een andere ondernemer (bijvoorbeeld toeleverancier), verzekeringsmaatschappij of overheid, functioneert dit als negatieve prikkel voor beveiliging of security management (Levi, Morgan & Burrows 2003).

e Veel strategieën van bedrijven bij de aanpak van onveiligheid zijn gebaseerd op samenwerking met andere partijen. Samenwerking tussen bedrijven kan moeilijk zijn als deze ook elkaars concurrenten zijn (Hardie & Hobbs 2002). Samenwerking tussen bedrijfsleven en publieke instanties (politie of justitie) wordt soms belemmerd door verschillen in visie, cultuur of belangen.

f Ook sectorspecifieke omstandigheden kunnen hier een rol spelen, zoals de complexiteit van de risico's waarmee bedrijven worden geconfronteerd en de mogelijkheden die bedrijven hebben om hierop een antwoord te vinden. De structuur van de bedrijfstak en betreffende markt kan hierbij relevant zijn. Voor een sector die bestaat uit kleine, onderling sterk concurrerende bedrijven kan het moeilijk zijn collectief veiligheidsmaatregelen te realiseren. Dat lukt vaak pas door interventie van een derde. Vaak zal dat de overheid zijn, maar strikte eisen door een grote afnemer of verzekeringsmaatschappij kun-

nen een vergelijkbaar effect hebben. Soms is een derde partij nodig om freerider gedrag te vermijden of de angst weg te nemen van verstoring van een 'level playing field'.

5 Slot

Bij door het bedrijfsleven gehanteerde strategieën met betrekking tot risico's van georganiseerde criminaliteit bestaan nog vele onbeantwoorde vragen. Zo is er nauwelijks informatie over de uitvoering van deze strategieën en de ervaringen die daarmee zijn opgedaan. Geldt ook hier, net als in de publieke veiligheidszorg, dat vaak sprake is van een aanzienlijk verschil tussen maatregelen op papier en in de praktijk? Ook is weinig (systematische) empirische informatie beschikbaar over de effecten van deze strategieën.

Toch zijn enkele algemene conclusies mogelijk. De door het bedrijfsleven gehanteerde strategieën zijn zeer divers. Zij verschillen onder meer naar bedrijfstak, soort bedrijf, aard van de risico's en naar niveau (bedrijf of bedrijfstak). Duidelijk is dat het geheel van door het bedrijfsleven gehanteerde strategieën veel breder is dan wat vaak onder 'corporate security' wordt verstaan (Challinger 2006). Het gaat niet alleen om door afzonderlijke bedrijven gehanteerde instrumentele maatregelen om risico's te verminderen en opgelopen schade te reduceren. De veiligheidszorg door het bedrijfsleven vindt plaats in een telkens veranderend veld, waarin het ook gaat om aanzien en invloed, om autonomie en om de vraag wie de rekening betaalt van veiligheidsrisico's en van maatregelen daartegen. Tot de strategieën behoren ook het mobiliseren van partijen, het lobbyen bij de overheid, het druk uitoefenen om anderen het voortouw te laten nemen of hun veiligheidszorg beter op orde te laten brengen.

De veiligheidszorg door het bedrijfsleven laat een pluriform, gedifferentieerd, maar ook gefragmenteerd beeld zien. De verhoudingen daarbij tussen publieke en private partijen zijn niet aan de hand van één model te typeren. In veel strategieën blijft een belangrijke positie bestaan voor overheid en politie. Het model van een 'nodal security' (Johnston en Shearing 2003; Wood en Shearing 2007) doet hieraan onvoldoende recht. Politie en overheid zijn in de veiligheidzorg niet 'one node among many', zoals Crawford (2003, 162) terecht concludeert. In sommige gevallen blijft de overheid de centrale partij (symbolisch en/of feitelijk), een situatie waar banken bijvoorbeeld over klagen als zij merken dat zij door publieke opsporingsdiensten als slechts een verlengstuk worden behandeld (Adviescommissie Informatiestromen 2007, 47). In andere gevallen proberen bedrijven of bedrijfstakorganisaties politie en overheid voor hun karretje te spannen, waar ook sommige lobbypraktijken op dit terrein op wijzen. Soms lijkt de rol van publieke partijen in de aanpak van veiligheidsrisico's marginaal en speelt de overheid in directe zin nauwelijks een rol van betekenis. Andere private maatregelen lijken slechts mogelijk omdat de overheid op de achtergrond aanwezig blijft en eventueel dwangmiddelen kan inzetten. Al met al is hier sprake van een complex, gefragmenteerd beeld, waarin vele relaties en modellen in de verhouding publiek–privaat door en naast elkaar bestaan (Crawford 2006, 466-467).

De hier in grote lijnen geschetste veiligheidszorg door het bedrijfsleven kent vele tegenstellingen. Er wordt wel samengewerkt tussen publieke en private partijen (en vermoedelijk steeds meer), dit veld blijft gefragmenteerd. Terwijl de overheid het bedrijfsleven aanmoedigt de eigen verantwoordelijkheden te nemen en bedrijven uitnodigt tot samenwerking, bestaat bij de politie soms de neiging zich terug te trekken en weer meer te geloven in eigen middelen en oplossingen (Adviescommissie Informatiestromen 2007). Crawford (2004) heeft het tegenstrijdige karakter van de nieuwe veiligheidszorg getypeerd als 'joined-up but fragmented', en de rol van overheid en politie ten opzichte van private partijen als 'at arm's length but hands on'. De verbrokkeling en complexiteit gaan echter verder. 'Joined-up' én fragmentatie, 'op afstand' én direct sturend, komen naast en door elkaar voor, afhankelijk van situatie en context. De prijs is onoverzichtelijkheid in de veiligheidszorg, op termijn vermoedelijk een weinig geruststellende gedachte.

Literatuur

Adviescommissie Informatiestromen Veiligheid (2007) *Data voor daadkracht*. Den Haag: BZK.

Albrecht, J. (1998) 'Security strategies for cargo companies'. *Security Management*, 42 (4), 28-32.

Bouloukos, A., G. Farell & G. Laycock (2003) 'Transnational organised crime in Europe and North America: Towards a framework for prevention'. In K. Aromaa (ed.), *Crime and criminal justice in Europe and North America 1995-1997: report on the sixth United Nations Survey on Criminal Justice Systems*. Helsinki: EICPCJ, 176-192.

Brunelli, M. & B. Vettori (2005) 'European music sector'. In T. Vander Beken (ed.), *Organised crime and vulnerability of economic sectors. The European transport and music sector,* Antwerp: Maklu, 194-308.

Bucquoye, A. et al. (2005) 'European road transport of goods'. In T. Vander Beken (ed.), *Organised crime and vulnerability of economic sectors. The European transport and music sector.* Antwerpen: Maklu, 57-193.

Clarke, R.V. (1997) *Situational crime prevention: successful case studies*. Albany: Harrow and Heston.

Challinger, D. (2006) 'Corporate security: a cost or contributor to the bottom line?' In M. Gill (ed.), *The Handbook of Security*. Houndmills: Palgrave, 586-609.

Chamard, S. (2006) *Partnering with businesses to address public safety problems*. Washington: U.S. Department of Justice.

Crawford, A. (2003) 'The pattern of policing in the U.K.: policing beyond the police'. In T. Newburn (ed.), *Handbook of Policing.* Cullompton: Willan Publishing, 136-168.

Crawford, A. (2004) 'The governance of urban safety and the politics of insecurity'. In K. van der Vijver & J. Terpstra (eds.), *Urban safety. Problems, governance and strategies*. Enschede: IPIT, 65-85.

Crawford, A. (2006) 'Networked governance and the post-regulatory state?' *Theoretical Criminology*, 10 (4), 449-479.

Dijk, Th. van, et al. (1999) *Bewust van de gevaren van criminaliteit: een inventarisatie van kwetsbaarheden, die in de logistieke keten en daarmee ook in de Rotterdamse haven voorkomen*. Rotterdam: Sanders Instituut.

Felson, M. (1998) *Crime and everyday life*. Thousand Oaks: Pine Forge.

George, B. & N. Whatford (2007) 'Regulation of transport security post 9/11'. *Security Journal*, 20 (3), 158-170.

Hardie, J. & B. Hobbs (2002) *Partners against crime: The role of the corporate sector in tackling crime*. Londen: IPPR.

IFPI (2005) *Music piracy. Serious, violent and organised crime* (from http: //www.ifpi.org/site-content/library/music-piracy-organised-crime.pdf, maart 2005).

Johnston, V. et al. (1994) 'Crime, business and policing on industrial estates'. In M. Gill (ed.), *Crime at work. Studies in security and crime prevention*. Leicester: Perpetuity, 102-123.

Johnston, L. & C. Shearing (2003) *Governing security. Explorations in policing and justice*. London: Routledge.

KPMG Forensic Accounting (2000) *Proefproject doorlichting transportsector. Een verkenning in het kader van het programma Preventie Georganiseerde Criminaliteit*. Den Haag: Ministerie van Justitie.

Levi, M. (2006) 'Combating white-collar and organized economic crimes: some reflections on the role of security'. In M. Gill (ed.), *The Handbook of Security*. Houndmills: Palgrave, 261-280.

Levi, M. & M. Maguire (2004) 'Reducing and preventing organised crime: an evidence-based critique'. *Crime, Law & Social Change*, 41, 397-469.

Levi, M., J. Morgan & J. Burrows (2003) 'Enhancing business crime reduction: UK directors' responsibilities to review the impact of crime on business'. *Security Journal*, 16 (4), 7-27.

Osborne, D. & T. Gaebler (1992) *Reinventing Government. How the entrepreneurial spirit is transforming the public sector*. New York: Penguin.

Rose, N. & P. Miller (1992) 'Political power beyond the state: problematic of government'. *British Journal of Sociology*, 43 (2), 173-205.

Schneider, S., M. Beare & J. Hill (2000) *Alternative approaches to combating transnational crime*. Toronto: KPMG/ Nathanson Centre.

WODC (2006) *Monitor Criminaliteit Bedrijfsleven 2006*. Den Haag: WODC.

Wood, J. & C. Shearing (2007) *Imagining Security*. Cullompton: Willan.

Dr. ir. J.B. Terpstra is werkzaam bij het Criminologisch Instituut, Sectie Strafrecht en Strafprocesrecht, Faculteit der Rechtsgeleerdheid, Radboud Universiteit, Nijmegen. Contactadres: Th. v. Aquinostraat 6, Postbus 9049, 6500 KK Nijmegen. E-mailadres: j.terpstra@jur.ru.nl.