Economische spionage a wereldoorlog

Nederlandse instellingen en bedrijven hebben reden om zich over economische spionage zorgen te maken of er op zijn minst alert op te zijn. Er is genoeg interesse in hun reilen en zeilen, zo waarschuwt de AIVD in haar jongste jaarverslag. Toch zijn Nederlanders zich in het algemeen onvoldoende bewust van de risico's van economische spionage. Wat zijn de verschijningsvormen en wat is er tegen te doen? Paul Koedijk *

Op 16 juli 2009 sprak een Amerikaanse rechter een historisch vonnis uit. Voor het eerst werd iemand schuldig verklaard aan spionage onder de Economic Espionage Act die in 1996 in werking trad. Het betrof een voormalige medewerker van Boeing van Chinees-Amerikaanse afkomst die informatie over onder andere de space shuttle aan China heeft doorgegeven – de man ontkent overigens, evenals China. De rechter bepaalt dit najaar zijn straf.

Ook de invoering van deze wet, die onder meer bedrijven verplicht actieve maatregelen tegen spionage te nemen, had historische betekenis. De nieuwe wetgeving markeerde een omslag. In de periode tot aan het einde van de Koude Oorlog stond spionage vooral in het teken van het verkrijgen van militaire gegevens. De balans is daarna omgedraaid ten gunste van economische informatie.

Globalisering

De globalisering heeft geleid tot een mondiaal gevecht om markten en nieuwe technologieën. Sommigen spreken zelfs in termen van 'oorlog' - en dat is geen metafoor. In Frankrijk bijvoorbeeld bestaat sinds 1997 een School voor Economische Oorlogsvoering, waarin defensie en Frans bedrijfsleven openlijk samenwerken.
Met dergelijk denken en handelen in termen van 'raison d'état' (staatsbelang) heeft Nederland altijd wat moeite. In de oorspronkelijke opzet van de Algemene Inlichtingen- en Veiligheidsdienst, die de Binnenlandse Veiligheidsdienst in 2002 opvolgde, was een taak weggelegd voor het waken over 'de vitale economische belangen' van Nederland. Uiteindelijk verzamelt de AIVD alleen algemene economische informatie. Het kabinet wijzigde het voorstel na kritiek van de Europese Commissie. Die vond economische spionage een belemmering van het vrije handelsverkeer. Nederland liep in zijn volgzaamheid voorop.

Belangrijk is het inzicht dat informatie vooraleerst informatie is

Diverse critici hebben zich inmiddels afgevraagd of de Europese Unie eigenlijk wel de ruggengraat heeft om de eigen belangen te verdedigen tegen rivalen die niet terugdeinzen voor ruw spel. Omzichtigheid is troef als het gaat om het nadrukkelijk benoemen en aanklagen van inmiddels gerenommeerde boosdoeners als Rusland of China.

Gevolgen

Nederlandse instellingen en bedrijven hebben reden om zich over economische spionage zorgen te maken of er op zijn minst alert op te zijn. Er is genoeg interesse in hun reilen en zeilen, zo waarschuwt de AIVD in haar jongste jaarverslag. Dat heeft zijn redenen. Nederland vervult een knooppuntfunctie. Dat is niet alleen vanwege het lidmaatschap van Navo en EU en de aanwezigheid van internationale instanties. Volgens de jongste cijfers van de Wereldhandelsorganisatie (WTO) is Nederland opgeklommen tot de vijfde exporteur van de wereld, vóór landen als Italië, Frankrijk en het Verenigd Koninkrijk.
Eén van de sterke punten van Nederlandse bedrijven is hun aanwezigheid in lucratieve nichemarkten waarvoor zij hoogwaardige of bijzondere producten leveren. Die producten zijn vaak gebaseerd op technologische vernieuwingen waarin bedrijven (soms gesteund door de overheid) veel hebben geïnvesteerd. Voor veel van hen geldt dat het merendeel van hun marktwaarde is gebaseerd op intellectuele eigendommen. Strategische informatie is een financieel waardeerbare productie-

ls heimelijke

factor. Economische spionage raakt daarom een bedrijf het hardst. De gevolgen strekken echter verder en treffen ook een samenleving in bredere zin:
» verlies van marktaandeel aan concurrent;
» verlies aan inkomsten uit verkoop;
» verlies aan fulltime banen;
» verlies aan gelieerde werkgelegenheid;
» negatieve invloed op de handelsbalans;
» verlies aan belastinginkomsten voor de staat.

In zakelijke en psychologische zin vernietigt economische spionage de premie op innovatie en daarmee de aansporing om producten te verbeteren of nieuwe producten te ontwikkelen.

Bedreigingen

De plegers van informatiediefstal en spionage komen uit diverse hoeken. De activiteiten kunnen incidenteel en structureel plaatsvinden. Zowel in het buitenland als in Nederland zijn er voorbeelden van werknemers die op eigen initiatief vertrouwelijke informatie van hun bedrijf hebben aangeboden aan concurrenten – of aan journalisten: dat laatste is het modernste actiemiddel van een ontevreden werknemer die vroeger misschien naar de vakbond zou zijn gestapt.

Het structurele en grootste gevaar is afkomstig van concurrerende bedrijven en van buitenlandse inlichtingendiensten. In sommige gevallen, zoals Rusland en vooral China, zijn die twee nauwelijks van elkaar te onderscheiden. Dit zijn de partijen die opereren op basis van langetermijnstrategieën en die hun volle technologische en menselijke potentieel in de strijd kunnen werpen: de economische oorlog ten voeten uit. Een voorbeeld is de installatie van een trojaans paard dat gevoelige informatie verzamelde en doorzond van een groot Brits bedrijf dat in overnamebesprekingen was verwikkeld met een Chinees staatsbedrijf. Maar het gaat niet alleen om technische spionage. Diverse westerse veiligheidsdiensten hebben reeds gewezen op het gevaar van Chinese studenten en gastwetenschappers die westerse universiteiten en onderzoekslaboratoria bezoeken. Het gevaar schuilt niet langer in getrainde agenten maar in burgers die zijn opgeleid – of gedwongen – om informatie te verzamelen. Sommigen van hen zijn zogenaamde ‘slapers’, die zijn gerecruteerd voordat een specifieke informatiebehoefte was geformuleerd. Naast concurrenten en ‘state actors’ vormen ten slotte georganiseerde criminaliteit en terroristische groeperingen een groeiend risico. »

Tegenmaatregelen

De AIVD waarschuwde onlangs maar weer eens dat Nederlanders zich in het algemeen onvoldoende bewust zijn van de risico's van economische spionage. Dat komt mogelijkerwijs mede doordat maar weinig bedrijven over effectieve methoden beschikken om de waarde en kwetsbaarheid van hun intellectuele kapitaal vast te stellen. De geconstateerde toename van cybercrime richting Nederlandse bedrijven gaat daar misschien verandering in brengen. De terechte aandacht voor *cyber security* mag echter niet ten koste gaan van de aandacht voor andere bedreigingen. Nog steeds concentreren veel bedrijven zich op de fysieke aspecten van (informatie)beveiliging. In de VS is wel eens berekend dat 70 procent van de marktwaarde van een gemiddeld Amerikaans bedrijf gebaseerd is op intellectueel kapitaal. Desondanks spenderen die bedrijven zo'n 80 procent van hun beveiligingsuitgaven aan de bescherming van de overige 30 procent van hun vermogensbestanddelen. De oorzaak ligt in een onevenwichtige inschatting van risico's. Het gaat bij gevoelige informatie niet langer alleen om bijvoorbeeld patenten en blauwdrukken die in (elektronische) kluizen worden weggeborgen. Natuurlijk beschermt vrijwel ieder bedrijf zijn kroonjuwelen. Informatie is keurig gerubriceerd en bijbehorende fysieke en procedurele beveiligingsmaatregelen zijn genomen. Maar minstens zo belangrijk is het inzicht dat informatie vooraleerst *informatie* is.

Kennis staat los van de aard van de dragers of bronnen van die kennis. Informatie dient beschouwd te worden als een *product* van een proces; een product waarvan het totaal meer is dan de som der delen. Wie maar voldoende ogenschijnlijk triviale stukken informatie verzamelt en combineert, puzzelt zo toch successievelijk het mozaïek bij elkaar. Dat verloren gegane inzicht hervonden de Amerikanen door schade en schande tijdens de Vietnamoorlog. De grote verliezen aan vliegtuigen bleken niet het gevolg van diefstal van operatieplannen. De tegenstander observeerde slechts eenvoudig waarneembare routines die een patroon vertoonden dat een op handen zijnde operatie verraadde. Uit die ontdekking ontstond het concept van *operational security* (OPSEC), dat zich richt op het onderkennen en verhullen van ongerubriceerde operationele informatie. Inmiddels is het een cruciaal onderdeel van alle militaire operaties. In het bedrijfsleven is het echter nog verre van gemeengoed en dat geldt zeker voor veel Nederlandse bedrijven.

Operationele beveiliging

De officiële Amerikaanse definitie van OPSEC spreekt van een samenstel van procedures en methodes waarmee managers op kosteneffectieve wijze hun programma's en hun staf kunnen vrijwaren van exploitatie door tegenstanders. De grondgedachte is dat een onderneming verhindert dat een derde partij kritische informatie verwerft en uitbuit. Operationele beveiliging staat daarbij naast de 'gewone' beveiliging. Eén van de zaken waarnaar de aandacht van een OPSEC-auditor uitgaat, is of niet juist bepaalde beveiligingsmaatregelen indirect informatie prijsgeven die een bedrijf liever binnen de poorten houdt.
Operationele beveiliging is in de huidige geglobaliseerde informatiesamenleving geen eenvoudige opgave. De gevaren zijn velerlei en slechts enkele kunnen hier dan ook de revue passeren. Informatie op websites bijvoorbeeld kan voor een organisatie een groter gevaar opleveren dan informatie die via andere kanalen beschikbaar is. Om dat gevaar tegen te gaan bevelen experts een zogenaamde *zero based* benadering aan. Stel vast welke informatie, in combinatie met andere gegevens, van kritieke betekenis kan zijn voor een buitenstaander. Die actie veronderstelt overigens dat die buitenstaanders en hun belangen in kaart zijn gebracht. Bekijk verder welke informatie je als bedrijf op een website moet plaatsen om als bedrijf te kunnen functioneren. Maak vervolgens een afweging van risico's wanneer zaken op gespannen voet met elkaar blijken te staan en pas daarop de website aan. Om zo'n goede en delicate balans tot stand te brengen is een samenwerking vereist van verschillende disciplines: security (informatiebescherming), business intelligence, pr en marketing en webredactie. Diezelfde benadering geldt ook voor artikelen en interviews waarbij eigenaren of medewerkers van het bedrijf betrokken zijn. Wie zakelijke bezoeken in het buitenland aflegt, moet zeer goed nadenken hoe hij of zij bedrijfsinformatie beschermt. Daarbij maakt het niet uit of die informatie digitaal is of in iemands hoofd zit. Vooral bij dat laatste is het echter van groot belang dat iemand van tevoren beseft wat de informatiewaarde kan zijn van zelfs ogenschijnlijk triviale gegevens. Dat lukt alleen maar als een bedrijf dat systematisch in kaart heeft gebracht. En uiteindelijk de persoon in kwestie de invloed van vermoeidheid, drank en andere verleidingen weet te weerstaan...
Bewustwording, voorbereiding en training kunnen daarbij helpen. Maar misschien is het ook tijd om eens te denken aan een Nederlandse versie van de Economic Espionage Act. Al was het maar om iedereen op scherp te zetten. «

drs. Paul Koedijk is werkzaam bij Integis BV te Overveen, een onderzoeksbureau van forensisch accountants en andere onderzoeksspecialisten. Hij is tevens lid en oud-voorzitter van de Netherlands Intelligence Studies Association (NISA).

Samenvatting

- Nederlandse instellingen en bedrijven hebben reden om zich over **economische spionage** zorgen te maken of er op zijn minst alert op te zijn.
- Economische spionage raakt een **bedrijf** het hardst, maar de gevolgen treffen ook een **samenleving** in bredere zin.
- Het **grootste gevaar** is afkomstig van concurrerende bedrijven en van buitenlandse inlichtingendiensten. Maar ook georganiseerde criminaliteit en terroristische groeperingen vormen een groeiend risico.
- Om te verhinderen dat een derde partij kritische informatie over de onderneming verwerft en uitbuit, is inzet van **operationele beveiliging** (OPSEC) nodig naast de 'gewone' beveiliging.