Spionage en veiligheidsrisico's

Actueel, onzichtbaar en divers

Defensie

Ministerie van
Binnenlandse Zaken *en*
Koninkrijksrelaties

Spionage en veiligheidsrisico's

Actueel, onzichtbaar en divers

Inhoud

Voorwoord

Voor u ligt een brochure over ongewenste inlichtingenactiviteiten in Nederland. Verscheidene buitenlandse inlichtingenorganisaties ontplooien activiteiten die schade kunnen toebrengen aan onze nationale veiligheid. Naast traditionele spionageactiviteiten, zoals het verwerven van geheime militaire, politieke, economische en wetenschappelijke informatie en het beïnvloeden van de politiek-ambtelijke besluitvorming, richten deze diensten zich op het beïnvloeden van in Nederland aanwezige migrantengemeenschappen, het controleren en intimideren van in ons land verblijvende opposanten, en de illegale verwerving van apparatuur, grondstoffen en kennis voor de productie van massavernietigingswapens.

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) hebben tot taak dergelijke activiteiten te onderkennen, te helpen beëindigen en de maatschappelijke weerstand ertegen te verhogen. Het is van belang dat medewerkers van overheidsinstellingen en het bedrijfsleven zich bewust zijn van de bestaande risico's van spionage. Deze brochure is bedoeld om een bijdrage te leveren aan die bewustwording. Ook vindt u in deze brochure een aantal tips ter onderkenning en voorkoming van spionage.

S.J. van Hulst
Hoofd Algemene Inlichtingen- en Veiligheidsdienst

Generaal-Majoor B. Dedden
Directeur Militaire Inlichtingen- en Veiligheidsdienst

1 Spionage: nog altijd actueel

Sinds het einde van de Koude Oorlog wordt nogal eens gedacht dat de dreiging van spionage grotendeels tot het verleden behoort. Ook in ons land is op dit terrein het veiligheidsbewustzijn bij burgers en bestuurders afgenomen. Hoewel in hun informatiebehoefte grotendeels wordt voorzien uit open bronnen, trachten overheden ook via bijvoorbeeld hun inlichtingendiensten geheime politieke, militaire en economische informatie te verwerven. Wanneer zulke inlichtingenactiviteiten de nationale veiligheid bedreigen, spreken we van spionage.

Tot 1989 was de spionagedreiging vooral afkomstig van inlichtingendiensten uit het voormalige Oostblok en China. De dreiging heeft zich de afgelopen jaren echter aanzienlijk verbreed, zowel naar aantal buitenlandse inlichtingenactiviteiten alsook naar variëteit van terreinen waarop die activiteiten betrekking hebben. Verscheidene buitenlandse diensten blijken belangstelling te hebben voor een breed scala aan onderwerpen. In de loop der jaren is door zowel de AIVD als de MIVD vastgesteld dat de schade die door de activiteiten van buitenlandse diensten in Nederland wordt aangericht, nog altijd aanzienlijk is. Verder in deze brochure zal hierop nader worden ingegaan.

1.1 Een onzichtbaar fenomeen

Eén van de belangrijkste kenmerken van effectieve spionage is de onzichtbaarheid ervan. Professionele inlichtingendiensten doen hun uiterste best hun activiteiten en successen te maskeren. Gevallen van spionage die desalniettemin blootgelegd worden, geven inzicht in de werkwijze en belangstelling van buitenlandse inlichtingendiensten. Het spreekt vanzelf dat doorgaans weinig ruchtbaarheid wordt gegeven aan de schade die op deze wijze wordt toegebracht aan Nederlandse belangen. Het geringe aantal zaken dat in de media komt, draagt vervolgens weer bij aan de beperkte aandacht in de publieke opinie voor dit fenomeen. Spionage is dan ook nog altijd actueel en soms dichterbij dan men denkt.

Eind februari 2003 werd afluisterapparatuur ontdekt in het gebouw van de Europese Raad in Brussel. Een belangrijke vergaderzaal, alsmede delegatieruimten van het Verenigd Koninkrijk, Oostenrijk, Frankrijk, Duitsland en Spanje zijn het doelwit geweest van deze afluisterpraktijken. In de betrokken vergaderzaal hebben de afgelopen jaren belangrijke vergaderingen plaatsgevonden van verschillende Europese organen. Het lijkt erop dat de aangetroffen apparatuur reeds is aangebracht tijdens de bouw van het raadsgebouw in 1995. Men heeft tot op heden niet kunnen vaststellen welk land achter de afluisteroperatie zit. De omvang van het systeem en de verbindingen met de uitgebreide bekabeling wijzen op een grote technische operatie, waarbij mogelijk steun van binnenuit is verkregen.

1.2 Verschijningsvormen van buitenlandse spionage

Buitenlandse inlichtingenactiviteiten in ons land manifesteren zich vooral op de hieronder genoemde aandachtsgebieden.

1 *Aantasting van politieke en ambtelijke integriteit*

Spionage kan leiden tot ernstige aantastingen van politieke en ambtelijke integriteit. Soms zijn buitenlandse inlichtingendiensten gericht op het verwerven van geheime overheidsinformatie op politiek, militair of economisch terrein, of op onrechtmatige beïnvloeding van politieke en ambtelijke personen en besluitvormingsprocessen. Dit kan gepaard gaan met het corrumperen van Nederlandse overheidsfunctionarissen.

In februari 2001 werd in de Verenigde Staten de FBI-agent Robert P. Hanssen gearresteerd. Deze bleek reeds vanaf 1979 voor Russische inlichtingendiensten te hebben gespioneerd, in ruil voor 1,4 miljoen dollar aan geld en diamanten. Als gevolg van Hanssen's activiteiten zouden in elk geval twee Amerikaanse dubbelagenten binnen de Russische KGB in de Sovjet-tijd zijn geëxecuteerd. Hanssen werd in mei 2002 tot levenslange gevangenisstraf veroordeeld.

De AIVD en de MIVD hebben in de laatste jaren herhaaldelijk vastgesteld dat functionarissen van de Russische militaire inlichtingendienst GRU zich richtten tot medewerkers van het Nederlandse ministerie van Defensie en zonder veel omhaal vroegen om informatie over militaire aangelegenheden.

2 *Aantasting van de economie en het technisch-wetenschappelijk potentieel*

Verscheidene buitenlandse inlichtingendiensten trachten informatie op economisch en technisch-wetenschappelijk gebied te verkrijgen. Het grootste deel van de informatie die wordt ingewonnen, komt uit open bronnen of is anderszins op niet-heimelijke wijze te verkrijgen. In een ander deel van de gevallen wordt informatie echter wel heimelijk vergaard. Vooral grote internationale aanbestedingen en (onderzoeks)projecten op het terrein van biotechnologie, ICT en militaire technologieën genieten de aandacht van buitenlandse inlichtingendiensten.

Het weglekken van in Nederland ontwikkelde en gefinancierde technologieën als gevolg van spionage kan de internationale rechtsorde en stabiliteit ondermijnen. Ook kan het de internationale concurrentiepositie van ons land aantasten. Bedrijven en onderzoeksinstellingen in Nederland en andere westerse landen vormen een doelwit van spionageactiviteiten uit landen die op deze manier hun economische en technologische achterstand willen inhalen. Maar ook technologisch geavanceerde staten schromen niet, door middel van spionage de concurrentiepositie van het eigen nationale bedrijfsleven te bevorderen ten koste van buitenlandse concurrenten.

Een prominent voorbeeld van heimelijke vergaring van militair-economische spionage kwam in 2002 aan het licht. In Zweden werden drie medewerkers van het telecombedrijf Ericsson gearresteerd op verdenking van spionage voor Rusland. Twee Russische diplomaten, actief als inlichtingenfunctionarissen, werden uitgewezen. Ericsson is vooral bekend om zijn mobiele telefoons, maar ontwikkelt ook radar- en raketgeleidingssystemen voor de Zweedse luchtmacht.

De afgelopen jaren zijn in verschillende landen Chinese studenten en wetenschappers die (tijdelijk) in het Westen studeren of werken, betrapt op inlichtingenactiviteiten. Betrokkenen verblijven veelal in het Westen in het kader van officiële Chinese overheidsprogramma's voor kennisintensivering: openbare programma's die beogen een 'inhaalslag' voor de Chinese kenniseconomie te realiseren. Deelname aan zulke programma's blijkt soms als 'cover' te dienen. Zo slaagden bijvoorbeeld enkele jaren geleden twee Chinese studenten in de VS erin, tijdens hun studieverblijf informatie te verzamelen voor de productie van een chemische substantie die wordt gebruikt in sensoren en wapens. Het lukte hen de verworven informatie door te spelen naar China voordat hun activiteiten ontdekt werden.

Westerse ondernemingen stuiten regelmatig op illegale nabootsing van hun producten die voortvloeit uit het ontduiken door China van intellectuele eigendomsrechten. In mei 2005 arresteerde de Franse politie een briljante Chinese wis- en natuurkundestudente die stage liep bij een groot toeleveringsbedrijf in de auto-industrie. De studente had al enige tijd de aandacht van collega's getrokken door zich binnen het bedrijf erg vaak met haar laptop te vertonen en zich dikwijls bij de computers op te houden, langer dan strikt nodig was voor haar opdrachten. Bij controle bleek zij een hoeveelheid informatie op haar laptop te hebben vergaard die volgens de bedrijfsvoorschriften nooit van de officiële werkstations hadden mogen worden gedownload. Bij huiszoeking werden vervolgens drie computers en twee harde schijven aangetroffen met geheime gegevens over auto-ontwerpen die vermoedelijk voor doorzending naar China waren bestemd.

3 *Proliferatie van massavernietigingswapens en van militaire technologieën*

Vanwege de aanwezigheid van relatief hoogwaardige technologische kennis en de positie van Nederland als knooppunt van logistiek en transport, vormt ons land een aantrekkelijk doelwit voor landen die trachten in of via Nederland grondstoffen, productiemiddelen of kennis te verkrijgen voor de ontwikkeling van eigen massavernietigingswapens en raketprogramma's. Daarnaast pogen vertegenwoordigers van buitenlandse inlichtingendiensten in westerse landen, waaronder uiteraard ook Nederland, heimelijk geavanceerde militaire of defensie-gerelateerde technologieën te verwerven.

De spionageactiviteiten van de Pakistaanse atoomgeleerde Abdul Qadeer Khan in de jaren zeventig bij een uranium-opwerkingsfabriek in Almelo hebben eraan bijgedragen dat Pakistan de beschikking kreeg over nucleaire technologieën voor de ontwikkeling van een eigen Pakistaans kernwapenprogramma.

Een Russische inlichtingenofficier, die onder een diplomatiek cover geplaatst was in Duitsland, heeft in 2004 op verzoek van de Duitse autoriteiten het land verlaten. De Russische inlichtingenofficier was tegen de lamp gelopen toen hij gerubriceerd materieel aannam van een agent van de Duitse veiligheidsdienst. De Rus probeerde, tegen betaling, gerubriceerde informatie over wapensystemen, telecommunicatie technologie en de structuur van de Duitse krijgsmacht in handen te krijgen.

4 *Ondersteuning van internationaal terrorisme*

Een aantal landen maakt zich schuldig aan het ondersteunen van internationaal opererende terroristische netwerken. Dit fenomeen staat bekend als *state-sponsored terrorism*. De ondersteuning kan bestaan uit het ter beschikking stellen van geld en goederen of het verlenen van diensten, zoals het verrichten van observatie-acties of het verschaffen van onderdak.

In september 1992 kwamen vier leden van de Iraans-Koerdische oppositie om bij een bomaanslag in het Berlijnse restaurant Mykonos. Uit het proces dat hierop volgde, bleek dat de Iraanse overheid achter de aanslag zat.

5 *Ongewenste beïnvloeding van migranten*

Een aantal in Nederland aanwezige buitenlandse inlichtingendiensten, vooral uit het Midden-Oosten, (Noord-)Afrika en China, is betrokken bij het manipuleren, beïnvloeden en controleren van migrantengroepen in ons land. Zij beschikken over zogeheten beheers- en beïnvloedingsnetwerken. Zulke netwerken richten zich onder andere op het tegengaan van de integratie van voormalige landgenoten in de Nederlandse samenleving. Maar ook wordt via zulke beheersnetwerken geprobeerd druk uit te oefenen op migranten om (uiteindelijk) te participeren in spionageactiviteiten voor hun land van herkomst.

Een zorgelijke ontwikkeling is de tendens tot radicalisering binnen delen van de moslimgemeenschappen in ons land. Er zijn aanwijzingen dat achter de schermen een aantal buitenlandse overheden een rol speelt bij ideologische beïnvloeding die leidt tot radicalisering van bepaalde groepen en personen. Door die radicalisering bestaat het gevaar dat mensen zich isoleren van de Nederlandse samenleving en hun toevlucht nemen tot gewelddadige en andersoortige activiteiten om hun anti-westerse gevoelens uit te dragen.

De toenmalige BVD ontdekte in 1999 dat een hooggeplaatste medewerker van de World Islamic Call Society, die in Utrecht als imam opereerde in een Marokkaanse moskee, een vertegenwoordiger was van de Libische inlichtingendienst. De man gebruikte zijn functie van imam als dekmantel voor zijn pro-Libische activiteiten. Zijn optreden was erop gericht de integratie van de moslimgemeenschap in de Nederlandse samenleving zoveel mogelijk te beperken. Hij werd op basis van een ambtsbericht van de toenmalige BVD tot ongewenst vreemdeling verklaard en vervolgens uitgewezen.

Het is de AIVD bekend dat het regime in Beijing ook in Nederland met inlichtingenmethoden de naar het buitenland uitgeweken oppositie structureel in de gaten houdt en tegenwerkt. Eveneens op verborgen manieren wordt op Chinese migrantenorganisaties invloed uitgeoefend om internationaal steun te betuigen aan de politieke en economische koers van China en onafhankelijke of kritische geluiden uit te bannen.

6 *Aantasting van kwetsbare/vitale overheids- en ICT-netwerken*

De afgelopen jaren zijn er opzienbarende pogingen van hackers geweest om kwetsbare internationale communicatienetwerken van overheid, vitale bedrijven en militaire onderzoekslaboratoria lam te leggen. Buitenlandse inlichtingenactiviteiten op dit terrein zijn er echter meestal op gericht ongezien informatie te

bemachtigen. Veel buitenlandse inlichtingendiensten beschikken over de mogelijkheid in te breken op informatie- en communicatienetwerken. Dit gebeurt met verschillende methodieken, zoals 'hacking', het inzetten van interne menselijke bronnen die toegang hebben tot kwetsbare netwerken en het manipuleren van software- en hardwaresystemen die op de internationale markt worden aangeboden. De Nederlandse samenleving is steeds meer afhankelijk van dergelijke kwetsbare processen en ICT-structuren.

1.3 Wat u zelf kunt doen

De AIVD en MIVD verstrekken beveiligingsadviezen aan organisaties die van vitaal belang zijn voor de instandhouding van het maatschappelijk leven, zoals bepaald in de Wet op de inlichtingen- en veiligheidsdiensten (Wiv 2002). Het is echter van groot belang dat overheidsorganisaties, bedrijven en onderzoeksinstellingen zelf een goede inschatting kunnen maken of zij een potentieel doelwit zijn van buitenlandse inlichtingenactiviteiten. Uiteraard houdt een dergelijke afweging nauw verband met de aard van de organisatie en de aanwezige kennisinfrastructuur.

Met name een beschrijving van de belangen en doelstellingen van de organisatie is essentieel om inzicht te krijgen in mogelijke dreigingen, de weerstand daartegen en, na afweging van die elementen (een risico-analyse), van het risico dat een organisatie loopt. Voor bijvoorbeeld bedrijven die vanuit de defensie-organisatie opdrachten met een gerubriceerd karakter krijgen, wordt een dergelijke risicoanalyse standaard gemaakt. Zulke bedrijven moeten voldoen aan de voorwaarden zoals vermeld in de Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO). Bij andere opdrachten maken 'project security instructions' soms deel uit van contracten. Ook als hiervan geen sprake is, is het voor een organisatie aan te bevelen zelf een risico-analyse uit te voeren.

1 *Spionage: door wie?*

Buitenlandse inlichtingenfunctionarissen treden nogal eens op in de hoedanigheid van diplomaat, student of zakenman, waardoor zij eenvoudig toegang hebben tot voor hen interessante

politieke, zakelijke en wetenschappelijke kringen. Ze kunnen deel uitmaken van overheidsdelegaties en diplomatieke vertegenwoordigingen, of gebruik maken van dekmantels van privé-bedrijven, buitenlandse media en wetenschappelijke instellingen. Daarnaast komen ook via internationale migratiestromen inlichtingenfunctionarissen ons land binnen. Verscheidene buitenlandse overheden doen een beroep op eigen wetenschappers, zakenlieden en studenten om in het buitenland specialistische informatie en materiaal te verzamelen op militair en technisch-wetenschappelijk gebied.

2 *Need-to-know en need-to-be*

De verschillende beveiligingsprocedures dienen binnen een bedrijf nauwkeurig te worden vastgelegd. Ook doelgerichte monitoring van informatiestromen is van belang. Zowel de situatie op ICT-gebied, als de informatiestromen die op een andere wijze verlopen moeten helder in kaart worden gebracht. Zicht op deze informatiestromen biedt de mogelijkheid bij eventueel misbruik van informatie tijdig in te grijpen en mogelijke schade te beperken. Indien er sprake is van informatie die voor een beperkt deel van de organisatie relevant is, moet het mogelijk zijn deze 'kring van ingewijden' nauwkeurig te bepalen. Ga hierbij uit van het principe *need-to-know* in plaats van *nice-to-know*. Met andere woorden: beperk toegang tot vertrouwelijke informatie tot degenen die deze informatie voor de uitvoering van hun werkzaamheden echt nodig hebben.

In het kader van *need-to-know* dient ook de term *need-to-be* onder de aandacht gebracht te worden. Alleen personeel dat daadwerkelijk werkzaamheden moet verrichten binnen een werkplek waar vertrouwelijke informatie aanwezig is, krijgt toegang tot die werkplek. Zorg verder voor toezicht en controle en doe aan incidentenrapportage. Inbreuken op beveiligingsregels en procedures kunnen wijzen op ongewenste belangstelling.

1.4 Indicaties voor mogelijke spionage

Spionage kan worden voorkomen door aandacht te schenken aan gedragingen die mogelijk op spionage wijzen. Enkele voorbeelden.

- Pogingen van een bekende met wie gaandeweg, soms gedurende een aantal jaren, een nauwere band is opgebouwd, om via de persoonlijke relatie mensen voor zich te laten werken. Aan het onderhouden van deze relatie besteedt de kennis/vriend

intensief en heel langdurig aandacht. Aanvankelijk worden er kleine 'diensten' gevraagd en heel geleidelijk wordt dan verzocht om meer vertrouwelijke of geheime informatie. De ontmoetingen gaan meer en meer plaatsvinden buiten de werkplek, in de sociale sfeer. Er wordt daarbij vaak een beroep gedaan op ideologische, etnische of religieuze motieven. Soms wordt rechtstreeks geld geboden of worden mensen via chantage onder druk gezet om hun medewerking te verlenen. Onder andere ontevreden en teleurgestelde werknemers, alsmede personen met privé-bezittingen of andersoortige belangen in het land van herkomst vormen een potentiële prooi voor buitenlandse inlichtingenactiviteiten.

- Verzoeken van onbekenden om informatie met een vertrouwelijk karakter aan anderen dan degenen die binnen de organisatie voor de afhandeling hiervan verantwoordelijk zijn. Indicatoren kunnen zijn: de ontvanger heeft de vraagsteller niet eerder ontmoet, het internetadres van de vraagsteller is geregistreerd in een ander land, de vraagsteller stelt zich voor als student of adviseur, de vraagsteller geeft aan voor de gevraagde (vertrouwelijke) informatie niet elders terecht te kunnen.
- Opvallende gedragingen tijdens een bezoek. Indicatoren kunnen zijn: bezoekers worden bijgestaan door een medewerker van de ambassade, het onderwerp van gesprek blijkt een ander te zijn dan waarvoor de afspraak was gemaakt, er worden op het laatste moment personen aan de delegatie toegevoegd of de bezoeker zwerft 'per ongeluk' door het gebouw.
- Verdachte sollicitaties, studenten en stageverzoeken. Indicatoren kunnen zijn: de sollicitant is afkomstig uit aan de staat gelieerde organisaties of bedrijven in landen met een autoritair regime, het gaat om werkzaamheden met een min of meer vertrouwelijk karakter, het gaat om een periode van enkele jaren en de salariswensen zijn beperkt.
- Opvallende uitnodigingen voor congressen en seminars. Indicatoren kunnen zijn: betaling van alle onkosten van de deelnemer, aanspraak tijdens het congres door personen met incomplete, onduidelijke naambordjes of nadrukkelijke persoonlijke belangstelling.
- Uitnodigingen verzonden aan een medewerker door de ambassade van het land van zijn herkomst, bijvoorbeeld om het land te bezoeken of een decoratie in ontvangst te nemen.

Voor de goede orde: waar in de tekst sprake is van inlichtingenfunctionarissen, betreft het zowel mannen als vrouwen. Het traditionele beeld van 'inlichtingenwerk is mannenwerk' is verre van reëel.

1.5 Tot slot

Wees u bewust van het risico van spionage en creëer bewustzijn binnen uw organisatie voor dit risico. De AIVD en de MIVD zijn geïnteresseerd in meldingen over spionage-activiteiten of incidenten, en bij twijfel kunt u deze organisaties raadplegen voor een inschatting of er inderdaad sprake is van spionage.

Indien u naar aanleiding van deze brochure nog vragen heeft, kunt u zich rechtstreeks of via de contactpersoon binnen uw organisatie wenden tot de AIVD of de MIVD.

Algemene Inlichtingen- en Veiligheidsdienst

Postbus 20010
2500 EA Den Haag
Telefoon: (070) 317 86 10
Fax: (070) 320 07 33
Internet: www.aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst

Van der Burchlaan 31
2597 PC Den Haag
Telefoon: (070) 441 90 27
Fax: (070) 441 90 10
Internet: www.mivd.nl

1.6 Aanbevolen informatie

Jaarverslagen AIVD (voorheen BVD);
Jaarverslagen MIVD (voorheen MID);
Voorschrift Informatiebeveiliging Rijksdienst-bijzondere informatie 2004, uitgave ministerie van Binnenlandse Zaken en Koninkrijksrelaties;
ISO 17799 - Code voor informatiebeveiliging.

Websites met informatie over inlichtingen- en veiligheidsdiensten:
www.aivd.nl; www.mivd.nl; www.fas.org; www.intelligenceonline.com; www.nisa-intelligence.nl; www.globalsecurity.org; www.oss.net; www.intellnet.org.

Eerste druk maart 2004.
Tweede druk juli 2005.

Algemene Inlichtingen-
en Veiligheidsdienst