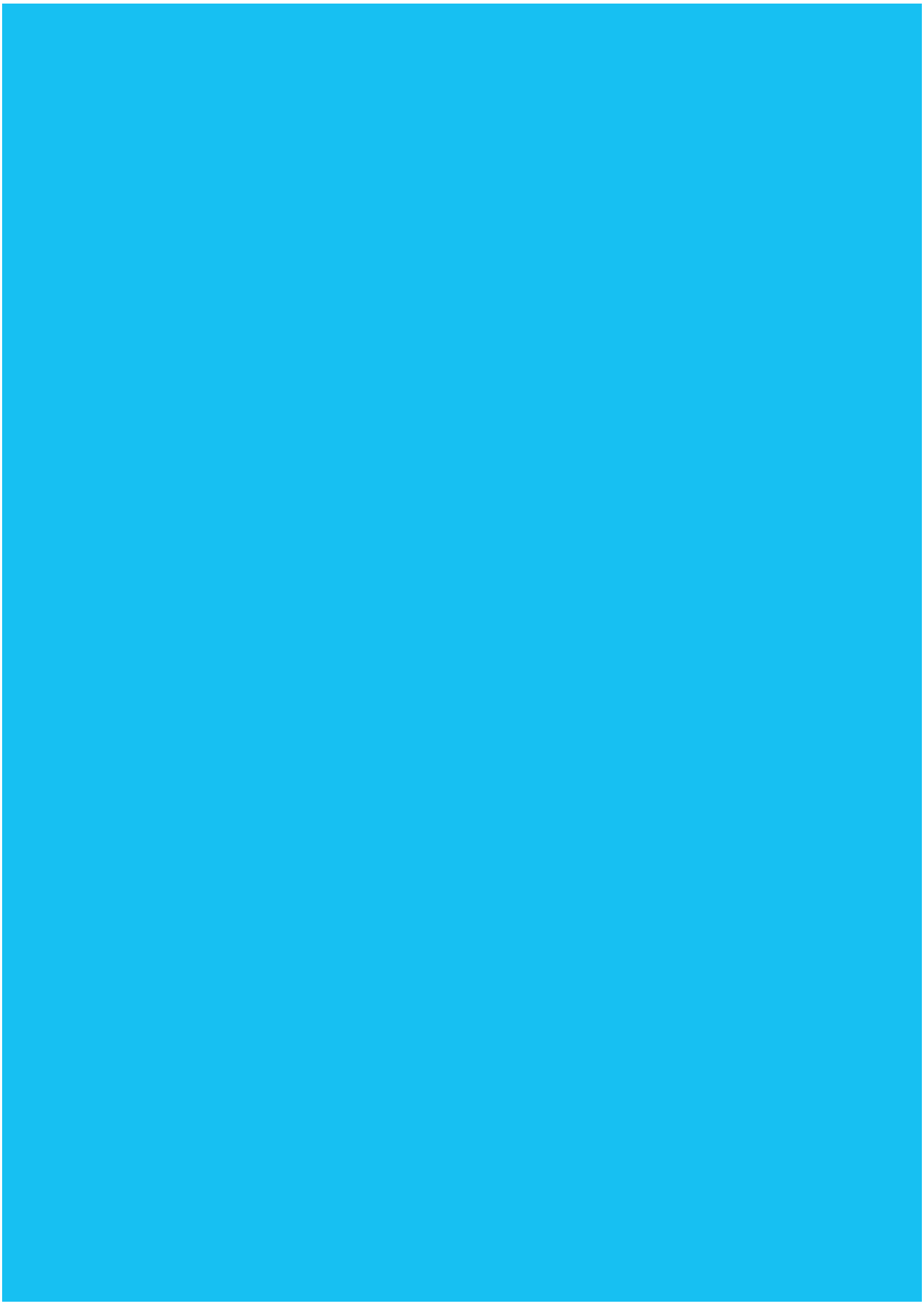
Spionage in Nederland

Wat is het risico?



Spionage in Nederland

Wat is het risico?

Spionage is van alle tijden en komt zelfs vanuit landen waarvan u het misschien niet verwacht.

Buitenlandse overheden putten uit openlijk toegankelijke informatiebronnen, maar verwerven ook geheime politieke, militaire en economische informatie via hun inlichtingendiensten.

De Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) stellen vast dat de schade die buitenlandse inlichtingendiensten aanrichten, aanzienlijk is. Daarom is het van belang dat u zich bewust bent van de risico's van spionage. In deze brochure informeren de AIVD en de MIVD u hierover en leest u hoe u de risico's op spionage kunt beperken.

Loopt u risico?

Effectieve spionage is onzichtbaar. Professionele inlichtingendiensten doen hun uiterste best hun activiteiten en successen te verbergen. Toch is spionage nog altijd actueel en soms dichterbij dan u denkt.

Beoordeel zelf of u vanuit uw functie of privéleven risico loopt op spionage. Bedenk of u beschikt over interessante kennis of dat u zich in een positie bevindt, die interessant is voor buitenlandse inlichtingendiensten. Vaak weet u meer dan u in eerste instantie denkt.

Europese Raad afgeluisterd
Eind februari 2003 werd er afluisterapparatuur ontdekt in het gebouw van de Europese Raad in Brussel. De doelwitten: een belangrijke vergaderzaal en delegatieruimten van het Verenigd Koninkrijk, Oostenrijk, Frankrijk, Duitsland en Spanje. De omvang van het afluistersysteem en de verbindingen met uitgebreide bekabeling wijzen op een grote technische operatie. Het lijkt er op dat de apparatuur al aangebracht is tijdens de bouw van het gebouw in 1995. Het is nog steeds onbekend welk land achter de afluisteroperatie zat.

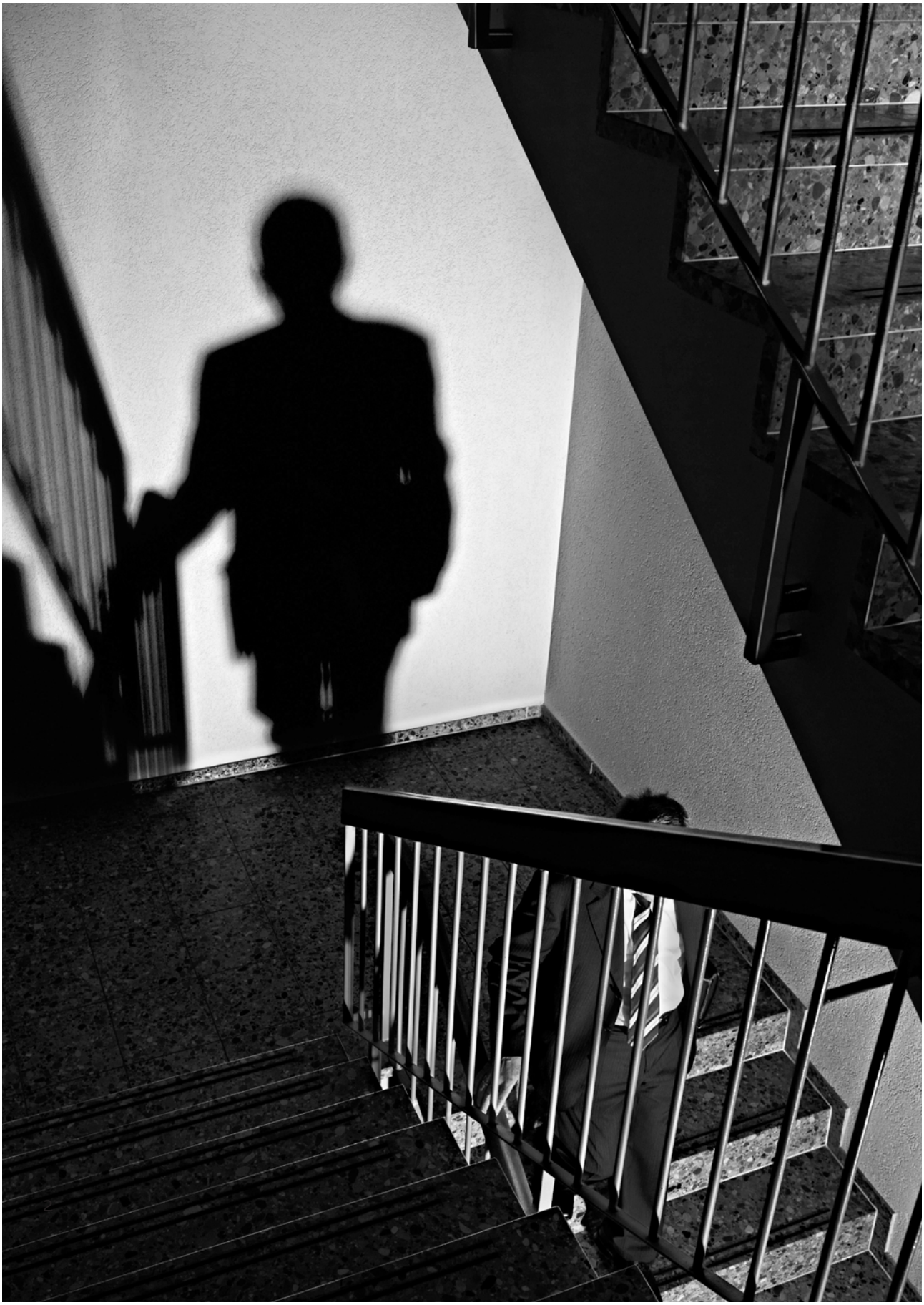
Hoe werken inlichtingendiensten?

Buitenlandse inlichtingenfunctionarissen presenteren zich in allerlei hoedanigheden: als diplomaat, student, wetenschapper, journalist of zakenman. Zo krijgen zij op onverdachte wijze toegang tot interessante politieke, zakelijke en wetenschappelijke kringen. Vaak worden echte wetenschappers, zakenlieden en studenten door de overheid van hun land ingeschakeld om in het buitenland informatie te verzamelen op militair en technisch-wetenschappelijk gebied. Inlichtingenfunctionarissen zijn zowel mannen als vrouwen. Het traditionele beeld dat inlichtingenwerk uitsluitend mannenwerk is, is verre van reëel.

Hoe komen inlichtingenfunctionarissen ons land binnen?

In welke rol kunt u hen verwachten?

- als leden van een overheidsdelegatie of diplomatieke vertegenwoordiging;
- als werknemer of eigenaar van privé-bedrijven, buitenlandse media of wetenschappelijke instellingen;
- als lid van een migrantengemeenschap.



Welke verschijningsvormen van spionage zijn er?

De verschillende verschijningsvormen van spionage zijn:

Verwerven van politieke en ambtelijke informatie en beïnvloeden van besluitvorming

Buitenlandse inlichtingendiensten richten zich vaak op verwerving van geheime overheidsinformatie op politiek, militair of economisch gebied. Zij kunnen ook politieke en ambtelijke functionarissen en besluitvormingsprocessen heimelijk beïnvloeden. Soms slagen zij er zelfs in om overheidsfunctionarissen corrupt te maken. Ook in Nederland worden overheidsfunctionarissen benaderd door buitenlandse inlichtingendiensten.

Verliefd op een Taiwanese
In 2007 werd een hoge Amerikaanse ambtenaar van het State Department veroordeeld voor het verstrekken van geheimen aan de Taiwanese inlichtingendienst. Hij was een buitenechtelijke relatie aangegaan met een Taiwanese vrouw, die 27 jaar jonger was dan hij. Hij vertelde haar staatsgeheimen, niet wetend dat zij een medewerkster was van de Taiwanese inlichtingendienst.

De 'Simm'-zaak
Het grootste spionageschandaal in het zestigjarig bestaan van de NAVO. Zo wordt de spionage genoemd van Herman Simm. Simm was oud-defensietopman in Estland. Hij gaf jarenlang geheime NAVO-informatie door aan de Russische civiele inlichtingendienst SVR. Simm ontving hiervoor grote geldbedragen, maar hij deed het ook uit frustratie en ijdelheid. En de Russen wisten hem hierdoor effectief te bespelen. Zo werd hem een hoge militaire rang en een hoge onderscheiding voorgehouden. In februari 2009 werd Simm veroordeeld tot een gevangenisstraf van twaalf en een half jaar.


32
31
30
0; k < 12;
= w[j - 32]
int k = 0;

Verwerven van economische en technisch-wetenschappelijke informatie

Informatie verwerven op economisch en technisch-wetenschappelijk gebied is een kerntaak van veel buitenlandse inlichtingendiensten. In sommige landen is deze taak zelfs wettelijk verankerd. Dit doen landen om hun eigen economische en technologische achterstand in te halen of om hun concurrentiepositie te bevorderen. De internationale concurrentiepositie van Nederland wordt aangetast als kennis en technologieën weglekken die in ons land ontwikkeld en gefinancierd zijn. Veel informatie halen inlichtingendiensten uit open bronnen, maar daarnaast vergaren ze informatie in het geheim. Ze zijn vooral geïnteresseerd in grote internationale verwervingstrajecten en aanbestedingsprocedures en projecten over baanbrekende technologieën.

Binnenkijken bij Ericsson

In 2002 werden in Zweden 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.

Nieuwsgierig

Veel Chinese studenten of wetenschappers studeren of werken tijdelijk in westerse landen. Veel van hen doen mee aan het officiële Chinese overheidsprogramma voor kennisintensivering. Maar dat is soms slechts een dekmantel om informatie te achterhalen en door te sturen.

In 2005 werd in Frankrijk een Chinese studente opgepakt. Zij liep stage in de auto-industrie. Het viel haar collega's op dat ze vaak langer achter computers zat dan nodig was. Bij controle bleek dat haar laptop informatie bevatte die volgens de bedrijfsvoorschriften niet gedownload had mogen worden. Bij haar thuis werden vervolgens drie computers en twee harde schijven met geheime gegevens over auto-ontwerpen gevonden.

Verwerven van kennis over massavernietigingswapens en militaire technologieën
Nederland heeft hoogwaardige technologische kennis over massavernietigingswapens en raketprogramma's en beschikt over geavanceerde militaire technologieën. Bovendien is Nederland een knooppunt van logistiek en transport. Inlichtingendiensten proberen daarom veel in of via Nederland grondstoffen, productiemiddelen of kennis te verkrijgen.

Raketgeheimen te koop
Een medewerker van het defensiebedrijf British Aerospace probeerde in 2003 raketgeheimen te verkopen aan een Russische agent. Dat dacht hij althans. De Russische agent bleek een agent van de Britse veiligheidsdienst. De medewerker werd veroordeeld tot tien jaar celstraf.

Pakistaan steelt uit Almelo
De spionageactiviteiten van de Pakistaanse atoomgeleerde Abdul Qadeer Khan in de jaren zeventig bij een uraniumverrijkingsfabriek in Almelo hebben eraan bijgedragen dat Pakistan de beschikking kreeg over nucleaire technologieën voor de ontwikkeling van een eigen Pakistaans kernwapenprogramma. Hoewel dit al meer dan dertig jaar geleden gebeurde, zijn de ernstige gevolgen van de activiteiten van Khan nog altijd actueel.

Beïnvloeden van migranten

Een aantal in Nederland aanwezige buitenlandse inlichtingendiensten is betrokken bij het manipuleren, beïnvloeden en controleren van groepen migranten in ons land. Zij beschikken over zogeheten beheers- en beïnvloedingsnetwerken. Zulke netwerken willen voorkomen dat voormalige landgenoten integreren in de Nederlandse samenleving. Ook wordt via zulke beheersnetwerken geprobeerd druk uit te oefenen op migranten om (uiteindelijk) spionageactiviteiten voor het land van herkomst te verrichten.

Marokkaanse interesse voor Nederlandse politie

In 2008 bleek dat de Marokkaanse inlichtingendienst zich in Nederland toegang verschafte tot besloten gegevensbestanden van de politie. Hiertoe heeft de Marokkaanse inlichtingendienst enkele Nederlandse politiefunctionarissen met een Marokkaanse achtergrond ingezet. Naar aanleiding van deze kwestie is een aantal in Nederland gestationeerde Marokkaanse diplomaten teruggeroepen naar Marokko.

Beïnvloeding na onlusten in Tibet

Het is bekend dat de Chinese overheid ook in Nederland met inlichtingenmethoden de naar het buitenland uitgeweken oppositie structureel in de gaten houdt en tegenwerkt. Eveneens wordt op verborgen manieren invloed uitgeoefend op Chinese migrantenorganisaties om niet alleen internationaal steun te betuigen aan de politieke en economische koers van China, maar ook om onafhankelijke of kritische geluiden uit te bannen. Een voorbeeld van ongewenste beïnvloeding van migranten werd zichtbaar na de onlusten in Tibet begin 2008. Vrij snel hierna berichtten ICT-veiligheidsinstellingen binnen Europa over het stijgende aantal digitale aanvallen op pro-Tibet-groeperingen. Betrokkenheid van de Chinese overheid hierbij wordt om verschillende redenen ingeschat als zeer waarschijnlijk.

Aantasten van ICT-netwerken

Veel buitenlandse inlichtingendiensten beschikken over mogelijkheden om ongezien in te breken in kwetsbare informatie- en communicatienetwerken. Het gaat dan vaak om netwerken van de overheid, bedrijven in vitale sectoren of wetenschappelijke instellingen. Ze breken in door:

- het hacken van websites;
- het inzetten van personen, die toegang hebben tot kwetsbare netwerken;
- het manipuleren van software- en hardware-systemen op de internationale markt.

Een gevaarlijk abonnement

Veel rijksambtenaren zijn geabonneerd op een nieuwsservice van de Europese Unie. Een aanvaller stuurt hun een e-mail met een geïnfecteerde bijlage. De e-mail lijkt afkomstig van de nieuws-service van de Europese Unie. Dus openen de rijksambtenaren zonder te aarzelen deze bijlage.

Doelwitten digitaal belaagd

In 2009 bleek dat het spionagenetwerk GhostNet honderden ambassades, ministeries en internatio-nale instellingen hackte. GhostNet hackte via gerichte e-mails met geïnfecteerde Word- en pdf-bestanden. Zodra een computer geïnfecteerd was, kopieerde GhostNet de documenten en luisterde gesprekken af via webcams en micro-foons. GhostNet werd aangestuurd met computers die bijna allemaal leidden naar China.


1307/23/23
1307/23/13
NBG
1307/23/07
1307/22/37
1307/22/33

Wat kunt u doen?

Wat kunt u doen om de risico's op spionage te beperken? De AIVD en de MIVD adviseren:

Stel uw beveiligingsprocedures vast en breng informatiestromen in kaart

Leg beveiligingsprocedures nauwkeurig vast en breng de situatie op ICT-gebied en andere informatiestromen helder in kaart. Zo kunt u bij eventueel misbruik van informatie snel ingrijpen en schade beperken.

Geef vertrouwelijke informatie alleen aan mensen die het nodig hebben

Is informatie voor een beperkt deel van uw organisatie relevant? Bepaal die 'kring van ingewijden' dan nauwkeurig. Beperk toegang tot vertrouwelijke informatie tot die mensen die het ook echt nodig hebben. Ga uit van het need-to-know-principe in plaats van het nice-to-know-principe.

Geef toegang tot een werkplek met vertrouwelijke informatie alleen aan mensen die daar moeten zijn

Alleen personeel dat werkzaamheden moet verrichten binnen een werkplek waar vertrouwelijke informatie is, krijgt toegang tot die werkplek. Ga uit van het need-to-be-principe in plaats van het nice-to-be-principe. Zorg ook voor toezicht en controle op die werkplek.

Wees alert op verdacht gedrag

Schenk aandacht aan de volgende gedragingen, die op spionage kunnen wijzen:

- Een bekende van u probeert gaandeweg een steeds nauwere band met u op te bouwen. Dit kan jaren duren. Op die manier wil hij u voor hem laten werken. Indicaties zijn:
  - deze bekende besteedt intensief en langdurig aandacht aan de relatie met u;
  - deze bekende vraagt kleine diensten en vraagt daarbij steeds meer om vertrouwelijke of geheime informatie;
  - u ontmoet deze bekende steeds vaker buiten het werk, in de sociale sfeer;
  - deze bekende doet vaak een beroep op ideologische, etnische of religieuze motieven;
  - deze bekende biedt u rechtstreeks geld;
  - deze bekende chanteert u om uw medewerking te krijgen.

- Een onbekende vraagt vertrouwelijke informatie aan een medewerker binnen de organisatie die niet verantwoordelijk is voor deze informatie. Indicatoren zijn:
  - degene die de vraag stelt, heeft de medewerker nog nooit ontmoet;
  - degene die de vraag stelt, heeft een internetadres dat geregistreerd is in het buitenland;
  - degene die de vraag stelt, zegt dat hij/zij student of adviseur is;
  - degene die de vraag stelt, zegt dat hij/zij nergens anders terecht kan voor deze informatie.

- Een aantrekkelijke man of vrouw heeft een opvallende interesse in u. Ook in uw privéleven. Er zijn inlichtingendiensten die (seksuele) verleidingstactieken gebruiken om iemand in diskrediet te brengen of geheime informatie te verkrijgen.

Gegevens van Britse premier in gevaar

Een Britse regeringsmedewerker liet zich verleiden tijdens een officieel bezoek in het buitenland. De volgende ochtend was hij zijn Blackberry kwijt. Hoewel het apparaat waarschijnlijk geen geheime gegevens bevatte, bestond het risico dat met het toestel werd ingebroken op de server van de ambtswoning van de premier.

- Opvallend gedrag tijdens een bezoek.
  Indicatoren zijn:
  - er komt een medewerker van de ambassade mee;
  - het onderwerp van gesprek is anders dan afgesproken;
  - er worden op het laatste moment personen aan de delegatie toegevoegd;
  - de bezoeker zwerft 'per ongeluk' alleen door het gebouw.

- Verdachte sollicitaties, studenten en stageverzoeken.
  Indicatoren zijn:
  - de sollicitant komt van een organisatie die aan de staat gelieerd is;
  - de sollicitant komt van een bedrijf of land met een autoritair regime;
  - het werk heeft een min of meer vertrouwelijk karakter;
  - het werk geldt slechts voor een paar jaar en de salariswensen zijn beperkt.

- Opvallende uitnodigingen voor congressen en seminars.
  Indicatoren zijn:
  - uw onkosten als deelnemer worden betaald;
  - tijdens het congres spreken mensen met incomplete, onduidelijke naambordjes u aan;
  - tijdens het congres hebben mensen nadrukkelijk persoonlijke belangstelling voor u.

- Uitnodigingen van een ambassade.
  Om het land van herkomst van de ambassade te bezoeken of om een decoratie in ontvangst te nemen.

Rapporteer incidenten

Meld incidenten. Uit inbreuken op beveiligingsregels en procedures kunt u ongewenste belangstelling herleiden.

Besteed in uw bedrijfsvoering aandacht aan de risico's van spionage

Bij de beveiliging van uw informatie en kennis binnen de organisatie kunt u aan de volgende elementen denken:

- *Identificeer de (kern)belangen van uw organisatie*.
  Daarbij zet u de belangen die u wilt beschermen op een rij met daarnaast alle relevante en voor uw sector voorstelbare dreigingen of dreigingsscenario's en uw beschermingsmaatregelen.
  Denk daarbij aan:
  - het bewustzijn van medewerkers dat spionage ook in uw organisatie mogelijk is;
  - digitale aanvallen en integriteit van uw digitale informatiehuishouding;
  - fysieke weerstand tegen indringers.

  Uit deze risicoanalyse moet blijken wie waarvoor beveiligd moet worden. Dit heeft ook te maken met bedrijfskeuzes; is de inhoudelijke patentkennis of uw commerciële strategie belangrijker?
- *Verplichte risicoanalyses*. Sommige bedrijven zijn verplicht om een risicoanalyse te maken. Bijvoorbeeld als zij opdrachten met een gerubriceerd karakter krijgen van Defensie. Zij moeten zich houden aan de voorwaarden Algemene Beveiligingseisen voor Defensie Opdrachten (ABDO, www.mivd.nl). Ook 'project security instructions' maken soms deel uit van een contract.
- *Beschouw veiligheidsmaatregelen als een extra waarde*, niet als een beperking van de bewegingsvrijheid: iedereen in de organisatie moet veiligheidsmaatregelen beschouwen als een 'business added value'.
- *Registreer en analyseer meldingen van mogelijke spionage of mogelijk gerelateerde onverklaarbare voorvallen*: zo worden trends zichtbaar, die bij decentrale waarneming onzichtbaar blijven.
- *Zorg voor een open cultuur, waar risico's bespreekbaar zijn*: medewerkers moeten eigen en andermans risico's durven te bespreken. Bijvoorbeeld risico's van hun gedrag of hun omgang met vertrouwelijk materiaal.

Wat doen wij?

De taak van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) is:

inlichtingenactiviteiten te onderkennen, te (helpen) beëindigen en de maatschappelijke weerstand ertegen te verhogen.

Wees u bewust van het risico van spionage. Creëer ook bewustzijn binnen uw organisatie. Wilt u een melding over spionageactiviteiten of incidenten doen?
Dan horen we graag van u – ook wanneer u twijfelt.

Wilt u meer weten?

Meer informatie leest u op de volgende sites:
- www.aivd.nl
- www.mivd.nl

Op deze sites vindt u:
- de brochure ‘Spionage bij reizen naar het buitenland. Wat is het risico?’
- de brochure ‘Digitale spionage. Wat is het risico?’
- de jaarverslagen van de AIVD en de MIVD

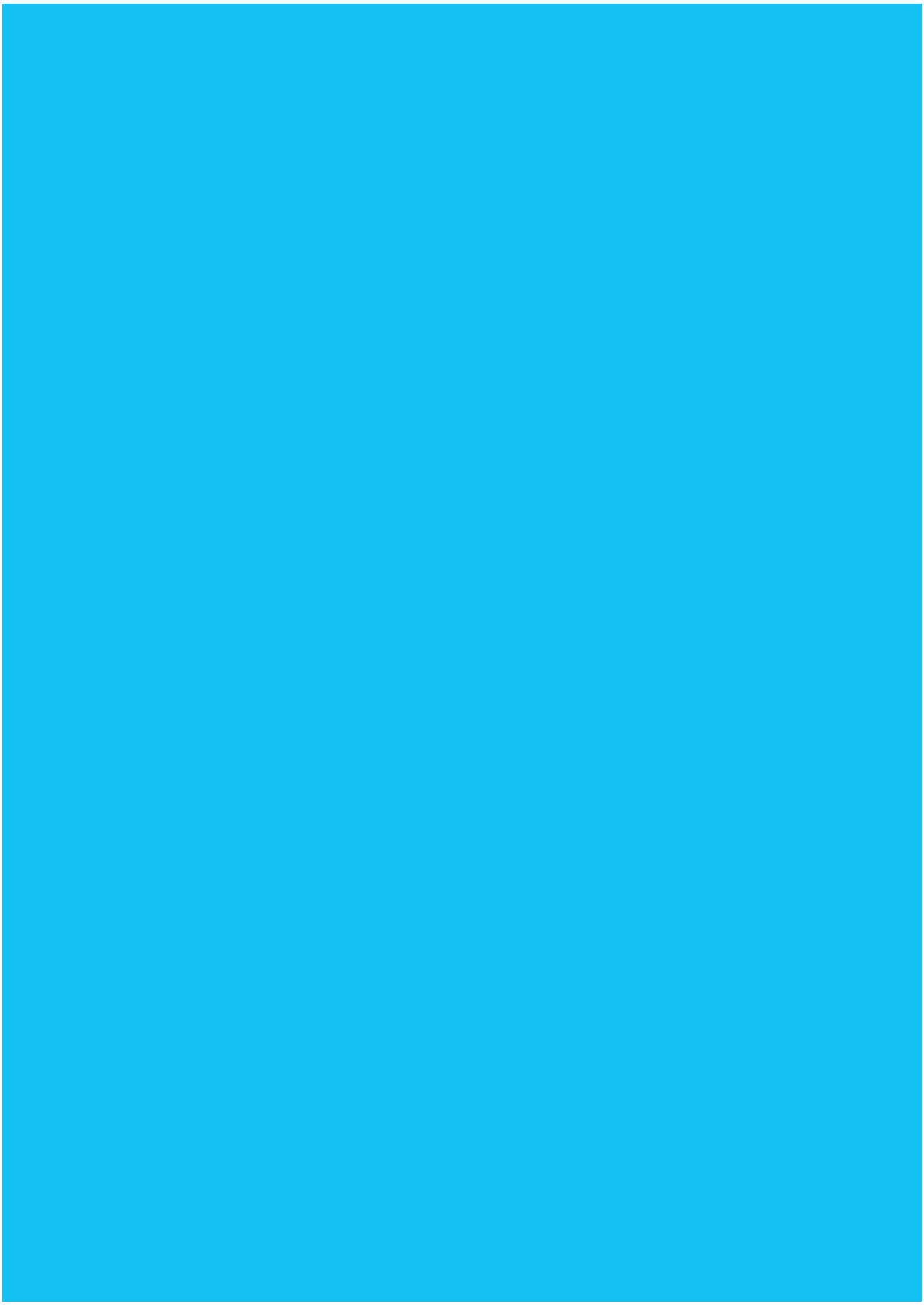
Heeft u vragen? Of wilt u een melding maken?
Neemt u dan contact met ons op. Onze adresgegevens zijn:

Algemene Inlichtingen- en Veiligheidsdienst

Adres:	Postbus 20010
	2500 EA Den Haag
Telefoon:	079 - 320 50 50
Fax:	070 - 320 07 03
Website:	www.aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst

Adres:	Postbus 20701
	2500 ES Den Haag
Telefoon:	070 - 441 90 27
Fax:	070 - 441 90 10
Website:	www.mivd.nl



Colofon
Deze brochure is een uitgave van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Algemene Inlichtingen- en Veiligheidsdienst
www.aivd.nl

Postbus 20010 | 2500 EA Den Haag

Ministerie van Defensie
Militaire Inlichtingen- en Veiligheidsdienst
www.defensie.nl/mivd

Postbus 20701 | 2500 ES Den Haag

Grafische verzorging
Zijlstra Drukwerk B.V., Rijswijk

1e druk, maart 2004
2e druk, juli 2005
3e druk, juli 2008
4e en herziene druk, 2010

Foto's
Hollandse Hoogte

Januari 2010