Spionagerisico's bij reizen naar het buitenland

Spionage in het buitenland: nog altijd divers en onzichtbaar, maar wel aanwezig

Algemene Inlichtingen- *en* Veiligheidsdienst

Spionagerisico's bij reizen naar het buitenland

Spionage in het buitenland: nog altijd divers en onzichtbaar, maar wel aanwezig

U denkt misschien: de Koude Oorlog is voorbij, en daarmee is het risico van spionage ook een zaak van het verleden. Het tegenovergestelde is echter het geval.

Het aantal landen dat spionage- of inlichtingenactiviteiten ontplooit is gegroeid. Het risico van spionage komt niet langer alleen van de 'bekende vijand' van de Koude Oorlog, maar ook vanuit landen die niet aan het oude vijandbeeld beantwoorden. Daarnaast is het aantal beschikbare middelen, waarmee vaak ongemerkt informatie verzameld kan worden, met de ontwikkeling van de technologie sterk toegenomen. Kortom, het risico van spionage vanuit het buitenland is meer gegroeid dan afgenomen.

Waarom u?

Als u naar het buitenland reist, kunt u om verschillende redenen interessant zijn voor buitenlandse inlichtingendiensten. Bijvoorbeeld omdat u beschikt over bepaalde kennis of informatie of vanwege uw positie. Inlichtingendiensten in het buitenland verzamelen via spionage informatie over onderwerpen als kwetsbare militaire, technologische, politieke of economische gegevens. Ook proberen zij Nederlanders, bijvoorbeeld ambtenaren of politici, op heimelijke wijze te beïnvloeden in hun besluitvorming.
U kunt zelf het beste beoordelen of u vanuit uw functie of privé-leven beschikt over dergelijke kennis of dat u zich in een dergelijke positie bevindt, die interessant kan zijn voor buitenlandse inlichtingendiensten.

De interesse van een buitenlandse dienst voor uw persoon kan al gewekt zijn vóór het vertrek, bijvoorbeeld door gegevens van de visumaanvraag of

door andere reisgegevens, zoals de aankondiging op internet van uw naam op de deelnemerslijst van een congres. In dat geval kunt u direct vanaf uw binnenkomst in het buitenland onder enige vorm van controle staan.

Het kan ook zijn dat u interessant bent voor een buitenlandse inlichtingendienst, doordat u zich in een bepaalde omgeving bevindt waarvoor deze dienst belangstelling heeft, bijvoorbeeld op een wetenschappelijk congres of bij het brengen van een bezoek aan bepaalde bedrijven.

Een voorbeeld uit de praktijk: zomaar een praatje?
Twee Nederlandse overheidsfunctionarissen, die ook persoonlijk bevriend zijn, worden tijdens hun gezamenlijke vakantie benaderd door twee charmante jongedames. Er ontspint zich een aangenaam gesprek over allerlei zaken, waaronder het werk. Achteraf pas realiseren de Nederlanders zich dat de dames vóóraf al wisten wat hun functie was en dat in het gesprek doelbewust is aangestuurd op bepaalde onderwerpen.

Werkwijze van inlichtingendiensten bij het verzamelen van informatie

Buitenlandse inlichtingendiensten beschikken over een breed arsenaal aan middelen om aan informatie van u of over u te komen. Hieronder staan enkele voorbeelden:

- Kopiëren van bestanden op gegevensdragers (denk hierbij aan laptops, mobiele telefoons, pda's enzovoort).
- Afluisteren van telefoon- en dataverkeer, vast of mobiel.
- Gebruik van camera's en of microfoons, bijvoorbeeld in de hotelkamer.
- Menselijke contacten, bijvoorbeeld 'toevallige' ontmoetingen of gerichte vragen over uw persoon of functie. Houd er rekening mee dat sommige inlichtingendiensten uitgebreid (soms jaren!) de tijd nemen voor het opbouwen van contacten.

- Openbaar beschikbare informatie, bijvoorbeeld op de website van uw bedrijf, over bijvoorbeeld uw positie of achtergrond.

Een voorbeeld uit de praktijk: kopiëren van gegevens aan de grens
Sommige landen kunnen reizigers vragen om bij binnenkomst aan de grens gegevensdragers zoals laptops af te staan. Het is voorgekomen dat Nederlandse zakenlieden bij aankomst op het vliegveld hun laptop, waarop concurrentiegevoelige bedrijfsinformatie stond, moesten afgeven. Later ontstond het vermoeden dat verschillende bestanden waren gekopieerd.

Wat kunt u doen om de risico's bij uw buitenlandse reizen te beperken?

Vooraf

- Voordat u vertrekt is het belangrijk om na te gaan welke factoren u interessant zouden kunnen maken voor een buitenlandse inlichtingendienst. Beschikt u over bijzondere kennis op een terrein waar het land in het bijzonder in is geïnteresseerd? Bent u in een positie van besluitvorming over zaken die het land aangaan, of beschikt u over informatie over dergelijke besluitvorming?
- Neem niet meer mee dan nodig. Bedenk vooraf wat er op de gegevensdragers staat die u gaat meenemen. Bevat uw laptop bijvoorbeeld bestanden die u niet nodig heeft op uw reis, maar wel concurrentiegevoelige informatie bevatten? Verplaats deze dan naar een andere computer voor u vertrekt.
- Het is aan te bevelen om de belgeschiedenis van telefoons te wissen voor vertrek.
- Gebruik altijd passwords voor mobiele telefoons en laptops en schakel deze toestellen tijdens het reizen altijd uit. Schakel deze toestellen pas weer in nadat de douane is gepasseerd.

Onderweg

- Zorg ervoor dat de blue tooth functie van telefoons en laptops altijd uitgeschakeld staat.
- Vervoer vertrouwelijke informatie en gegevensdragers zoals USB-sticks, cd-rom's, floppy's, telefoons en laptops altijd in de handbagage en niet in de koffer. Op deze manier is het altijd duidelijk voor de eigenaar wanneer een ander in aanraking is geweest met de informatie of gegevensdragers.
- Wees voorzichtig met vertrouwelijke gesprekken aan boord van vliegtuig, trein of andere vervoersmiddelen, bijvoorbeeld het busje waarin u wordt opgehaald. Mensen hebben vaak de neiging om tijdens de reis de onderhandelingen voor te bereiden en sommige inlichtingendiensten maken hier handig gebruik van. Sommige (vliegtuig)maatschappijen hebben nauwe banden met inlichtingen- en veiligheidsdiensten.
- Neem geen bagage mee voor anderen.

Op de plek van bestemming

- Bescherm vertrouwelijke informatie. Laat geen vertrouwelijke gegevens achter op een plaats waar anderen ze zouden kunnen inzien. Dit geldt ook voor de hotelkamer of een hotelkluis. Bescherm uw gegevens op een manier waarop u kunt controleren of ernaar is gekeken.
- Wees selectief met het verstrekken van informatie. Ga in contacten uit van het 'need to know' principe en vertel uw gesprekspartner niet meer dan noodzakelijk is.
- Wees alert op signalen van buitengewone interesse: is uw gesprekspartner bijvoorbeeld extra in u geïnteresseerd nadat u verteld heeft waar u werkt? Wordt u gevraagd om voortzetting van het contact na terugkomst in Nederland?
- Neem als u onterecht wordt aangehouden of bij een ernstige inbreuk op uw privacy altijd contact op met de Nederlandse ambassade ter plaatse.

Bij thuiskomst

- Heeft u aanleiding om te vermoeden dat u onder de aandacht heeft gestaan of bent benaderd door een buitenlandse inlichtingendienst, neem dan bij thuiskomst contact op met de afdeling Beveiliging van uw bedrijf of met de AIVD/MIVD. Uiteraard zal uw melding met de uiterste vertrouwelijkheid behandeld worden.

Een voorbeeld uit de praktijk: 'persoonlijke' interesse

Een Nederlandse overheidsmedewerker bezoekt een conferentie in het buitenland. Tijdens het sociaal programma wordt hij aangesproken door een knappe jongedame, die eveneens aan de conferentie deelneemt. Ook na afloop van de conferentie blijft zij contact opnemen met de Nederlander en probeert steeds meer persoonlijke informatie van hem los te krijgen. De Nederlander vindt dit gedrag opvallend en meldt de kwestie bij de inlichtingendienst. Onderzoek bewijst dat de dame in kwestie niet alleen verbonden is aan de strijdkrachten, maar zelfs aan de inlichtingendienst van het betreffende land.

Colofon

Uitgave

Algemene Inlichtingen- en Veiligheidsdienst
Postbus 20010
2500 EA Den Haag
Telefoon: 079 - 320 50 50
Fax: 070- 320 07 03
www.aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst
Postbus 20701
2500 ES Den Haag
Telefoon: 070- 441 90 27
Fax: 070 - 441 90 10
www.mivd.nl

Grafische verzorging

Zijlstra Drukwerk, B.V., Rijswijk

1e druk, september 2008


Defensie
Ministerie van
Binnenlandse Zaken en
Koninkrijksrelaties