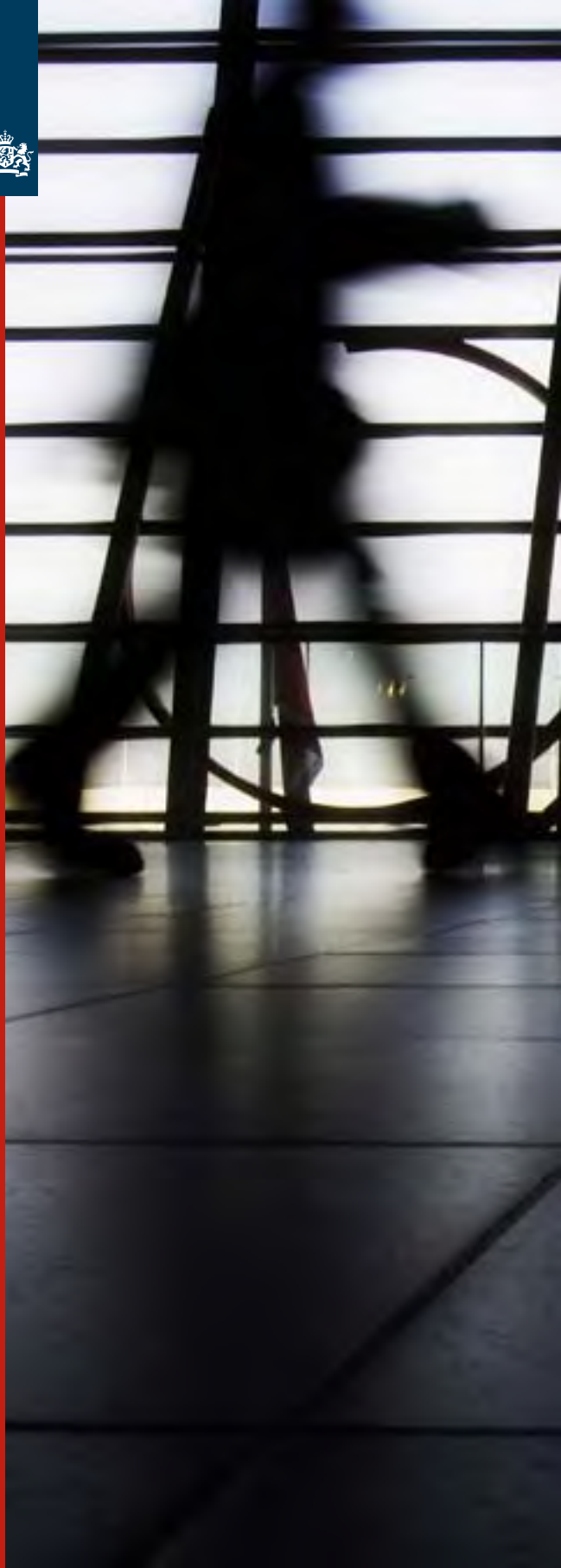
# Espionage when travelling abroad

What are the risks?



# Espionage when travelling abroad

## What are the risks?

Espionage is as much a danger now as it ever has been. And it can even be practised by countries you would not expect to want to spy on the Netherlands or Dutch organisations. Moreover, technological progress has given intelligence services more ways to gather information surreptitiously.

In this brochure, the General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) and the Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) of the Netherlands explain how you could fall victim to espionage when travelling abroad. You will also find tips to minimise that risk before, during and after your journey.

### Are you at risk?

Foreign governments may target you for espionage if:

- you possess information or know-how of interest to them;
- your position gives you access to that kind of information or to a network of interest to intelligence services;
- you are in a situation conductive to information gathering, such as a scientific congress or company visit.

Intelligence services and other government agencies sometimes use espionage techniques in an effort to acquire sensitive political, military, economic or technological data. They may also use clandestine means to try to influence businesspersons, civil servants, politicians and others with decision-making powers. Potential targets range from diplomats to the staff of government ministries and even local government officers.

When considering whether you are at risk, ask yourself if your work or private life makes you a person of interest to foreign intelligence services. Consider whether you have access to valuable information or are in a position that could be of interest to foreign intelligence services. It is quite likely that you know more than you may think at first.

**'Your laptop, please...!'**
An executive is travelling abroad on business. Upon arrival, a customs officer immediately makes him hand over his laptop. It is not returned for three hours. When he checks it later, he suspects that various files containing competition sensitive information have been copied.

### How do intelligence services operate?

Foreign intelligence services possess a host of means to obtain information from or about you. They include:

- copying data from devices like laptops, mobile telephones and PDAs;
- tapping telephone calls and data traffic, both mobile and on landlines;
- planting cameras or microphones in hotel rooms and other locations;
- personal contact, perhaps in the form of 'chance' meetings leading or probing questions about you or your work;
- the use of publicly available information, such as details of your job and background on your organisation's website or personal data from social networking sites like Hyves and Facebook.

Even before you leave home, an intelligence service may take an interest in you. For example, it can obtain information from your visa application, by searching the internet or because your name is on a list of conference participants. In such cases, you could well be under surveillance from the moment you enter the country. And intelligence services are often prepared to take plenty of time – years even – to develop valuable contacts.


CUSTOMS
DOUANE

# What can you do?

Here are some tips to help you minimise the risk of falling victim to espionage before, during and after your journey.

### Before you leave

Ask yourself the following questions.

1. Do I know things that another country might be interested in?
2. Do I have the power to make decisions that could affect the interests of other countries?
3. Do I possess information about decisions affecting other countries?

If the answer to any of these questions is 'yes', we advise you to take the following precautions.

- Make sure that you take along only the information you really need. Be especially cautious about taking confidential or sensitive material.
- In particular, review the data held on devices like laptops, mobile telephones and PDAs.
- If any of these items contain sensitive information you do not need whilst abroad, transfer it to another device and make sure that the original files have been permanently deleted.
- Delete the call history in your mobile telephone.
- Use passwords to prevent unauthorised access to your mobile telephone, PDA and laptop.
- As far as possible, keep all electronic devices switched off when you are not using them. Whenever they are on, they are vulnerable to espionage attempts.

### While travelling always

- Switch off the Bluetooth function on your electronic devices.
- Carry all sensitive information in whatever form – on USB sticks, CD-ROMs, diskettes, a telephone, a PDA or a laptop – in your hand luggage. Never check it in. Only if you can see it at all times can you be sure that it has not been tampered with.
- Exercise extreme caution when conducting confidential conversations in any public place. That includes on aircraft, trains or other means of transport, even 'private' cars or buses. Many business travellers, for example, use the journey to prepare their negotiating position. But some intelligence services are quick to exploit this practice. And certain airlines and other transport operators have close ties with those services.
- Never carry luggage for or on behalf of other people.

### At your destination

- Protect sensitive information. Never leave it in where other people could gain access to it. That includes hotel rooms and even hotel safes. And always make sure that you have a means to check whether anybody has tried to look at it.
- Disclose information only very selectively. Whoever you are talking to, whether about professional or private matters, strictly apply the 'need to know' principle. Never reveal any more than is absolutely necessary.

**A nice chat...?**
Two Dutch civil servants, friends as well as colleagues, take a holiday together. On a café terrace they are approached by two charming ladies. The encounter leads to a long and pleasant conversation on all sorts of subjects. Including their work...
As the two friends are walking back to their hotel later that evening, one of them suddenly has his doubts. "Did they ask us about our jobs, or did we just tell them?" At that moment the penny drops. The women must have known in advance what work the pair do, because they were deliberately steering the conversation around to particular subjects.

**'What a coincidence!'**
A Dutch government employee attends a conference abroad. At one of the social events she gets chatting to a man. He, too, is a delegate. After the conference he calls her a couple of times, but she rebuffs him. Then, apparently by coincidence, they run into one another at a restaurant. The man immediately engages her in conversation, asking a lot of questions in the process. The woman finds that odd, and so reports it to us. Our investigations reveal that the man has links to the intelligence service of the country hosting the conference.

- Be alert to signs of unusual attention. In conversation, for example, does the person you are talking to take a particular interest after you tell them where you work? Are you asked to stay in touch after you return home?

- Always contact the nearest Dutch embassy if you are arrested or otherwise detained without good cause, or if your privacy is seriously violated.

## After you return home

Do you suspect that you have been under surveillance? Have you been approached by a foreign intelligence service? If so, inform your organisation's security officer as soon as you return home. Or contact the AIVD or MIVD directly. You can find the addresses and telephone numbers at the back of this brochure.
Naturally, all reports are treated in the strictest confidence.

# What do we do?

The counterespionage task of the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) is officially defined as follows.

*To identify intelligence activities, to bring them to an end – or help to do so – and to enhance national public resilience to them.*

Be alert to the risks posed by espionage. And raise awareness of that risk throughout your organisation. Please report any suspicious activity or incidents to us, even if you are not sure about their significance. We are always pleased to hear from you.

# Are you interested in finding out more?

You can find more information on the following sites:
- www.aivd.nl
- www.mivd.nl

At www.aivd.nl and www.mivd.nl you can find:
- The brochure 'Espionage in the Netherlands. What are the risks?'
- The brochure 'Digital espionage. What are the risks?'
- The annual reports of the AIVD and MIVD

If you have any questions or wish to pass on information,
please do not hesitate to contact us at one of the following addresses.

**General Intelligence and Security Service (AIVD)**

Postal address: PO Box 20010
2500 EA The Hague
the Netherlands
Telephone: +31 (0)79 320 5050
Fax: +31 (0)70 320 0703
Website: www.aivd.nl

**Military Intelligence and Security Service (MIVD)**

Postal address: PO Box 20701
2500 ES The Hague
the Netherlands
Telephone: +31 (0)70 441 9027
Fax: +31 (0)70 441 9010
Website: www.mivd.nl

**Colophon**
This brochure is a publication of:

**Ministry of the Interior and Kingdom Relations of the Netherlands**
General Intelligence and Security Service
www.aivd.nl

PO Box 20010 | 2500 EA The Hague, the Netherlands

**Ministry of Defence of the Netherlands**
Military Intelligence and Security Service
www.defensie.nl/mivd

PO Box 20701 | 2500 ES The Hague, the Netherlands

**Graphic Design**
Zijlstra Drukwerk BV, Rijswijk, the Netherlands

1st print, September 2008
2nd print, November 2008
3rd translated revised print, March 2010

**Photographs**
Hollandse Hoogte