Espionage in the Netherlands

What are the risks?

Espionage in the Netherlands

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.

Foreign governments draw on public sources of information that are openly accessible but they also gather classified political, military and economic information via their intelligence services.

The General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) and Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) of the Netherlands find that the damage caused by foreign intelligence services is considerable. That is why it is important to be aware of the risks of espionage. In this brochure the AIVD and MIVD provide information and show you how you can limit the risks of espionage.

Are you at risk?

Truly effective espionage is invisible. Professional intelligence services go to great lengths to conceal their activities and achievements. All the same, espionage remains topical and is sometimes closer to home than you think.

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.

Eavesdropping devices found at the European Council

In February 2003 eavesdropping equipment was discovered in the office of the European Council in Brussels. The targets were a major meeting hall and rooms used by the delegations of the United Kingdom, Austria, France, Germany and Spain. The scale of the system and the connections with extensive cables suggest a large-scale technical operation. The equipment appears to have been planted during the office's construction in 1995. Which country was behind the eavesdropping operation remains unknown.

How do intelligence services operate?

Foreign intelligence service officers present themselves in all manner of capacities: as diplomats, students, scientists, journalists or businesspersons. This allows them to gain access to interesting political, business and scientific circles without arousing suspicion. In many cases, real-life scientists, students and businesspersons are recruited by their government to gather information of a military, technological and scientific nature abroad. Both men and women are employed as agents by intelligence services. The traditional image of intelligence work as the exclusive preserve of men is far from being a reality.

How do intelligence agents enter the country?

In what kinds of capacity can you expect them to enter the country?

- as members of a government or diplomatic delegation;
- as employees or owners of private companies, foreign media or scientific institutes;
- as a member of an immigrant community.

What are the different forms of espionage?

Different forms of espionage are:

Gathering political and official information and influencing decision-making

The objective of foreign intelligence services often is to gather confidential government information of a political, military or economic nature. Another aim can be to influence politicians, civil servants and decision-making processes surreptitiously. In some cases they even manage to corrupt government officials. As elsewhere, foreign intelligence services approach government officials in the Netherlands too.

In love with a Taiwanese woman

In 2007 a senior US civil servant in the State Department was judged guilty of supplying confidential information to the Taiwanese intelligence services. He had started an extra-marital affair with a Taiwanese woman, his junior by 27 years, and told her state secrets, unaware of the fact that she was employed by the Taiwanese intelligence service.

The Simm Case

The case of Hermann Simm is known as the largest espionage scandal in the NATO's sixty year history. Simm was a former senior defence official in Estonia. He passed on confidential NATO information to the Russian civil intelligence service SVR for years on end. Simm received large sums of money in exchange but he was also motivated by frustration and vanity. This allowed the Russians to manipulate him effectively, by promising him a high military rank and honours, for instance. In February 2009 Simm was sentenced to twelve and a half years in prison.


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

Gathering economic, technological and scientific information

Gathering information of an economic, technological or scientific nature is a core task of many foreign intelligence services. In some countries this task is even set down in law. Countries do this in order to make up for their own economic or technological disadvantage or to boost their competitive position. The Netherlands' international competitiveness is damaged when there are leaks of knowledge and technology that has been developed and financed here. Intelligence services gather much of their information from open sources, but they also gather information secretly. They are particularly interested in large-scale international recruitment programmes, tender procedures, and projects relating to pioneering technologies.

Looking in on Ericsson

In 2002 three employees of the telecommunications company Ericsson in Sweden were arrested on suspicion of spying for Russia. Two Russian diplomats, working as intelligence agents, were deported. Ericsson is best known for its mobile phones, but the company also develops radar and missile homing systems for the Swedish air force.

Conspicuous curiosity

Many Chinese students and scientists come to Western countries for temporary work or study. In many cases they are participants in China's official government programme aimed at knowledge intensification. In some cases, however, this is merely used as a cover for gathering and passing on information.

In 2005 a Chinese student was arrested in France. She was doing a work placement in the automotive industry. She attracted her colleagues' attention because she often consulted certain computers for longer than necessary. Checks revealed that her laptop contained information, the downloading of which was not permitted according to company regulations. A subsequent search of her home uncovered three computers and two hard disks containing confidential data relating to vehicle designs.

Gathering knowledge about weapons of mass destruction and military technologies

The Netherlands has high-quality technological information about weapons of mass destruction and missile programmes and has advanced military technologies at its disposal. Furthermore, the Netherlands is a gateway for logistics and transport. That is why intelligence services frequently try to acquire base materials, means of production and knowledge in or via the Netherlands.

Missile secrets for sale

In 2003 an employee of the defence contractor British Aerospace tried to sell confidential information about missiles to a Russian agent. Or so he thought. The Russian agent turned out to be an agent of the British security service. The employee was convicted and received a ten-year prison sentence.

Pakistan steals from Almelo

The espionage activities carried out by the Pakistani nuclear scientist Abdul Qadeer Khan at a uranium enrichment factory in Almelo in the 1970s helped Pakistan to acquire nuclear technologies for the development of Pakistan's own nuclear weapons programme. Even though they took place more than thirty years ago, the serious consequences of Khan's activities are still relevant today.

Manipulation of migrants

A number of foreign intelligence services are involved in manipulating, influencing and monitoring migrant groups in our country. They command networks aimed at influence and control. The aim of these networks is to prevent former countrymen and women from integrating in Dutch society. Such networks are also used to try and exert pressure on migrants to eventually carry out espionage activities for their country of origin.

Moroccan interest in the Dutch police

In 2008 it came to light that the Moroccan intelligence service was accessing closed Police files in the Netherlands. The Moroccan intelligence service was able to do this by deploying a number of police officials with a Moroccan background. As a result of this case, a number of Moroccan diplomats stationed in the Netherlands were recalled to Morocco.

Manipulation following disturbances in Tibet

It is a known fact that the Netherlands is also one of the countries where the Chinese government uses intelligence methods to structurally monitor and oppose dissident parties in exile. Chinese migrant organisations are also manipulated covertly to get them not only to voice international support for China's political and economic line but also to expel any independent or critical voices. An example of undesirable manipulation of migrants came to light following the disturbances in Tibet at the beginning of 2008. Soon after, IT security agencies in Europe reported an increase in digital attacks on pro-Tibet groups. For a variety of reasons, the involvement of the Chinese government in these activities is judged to be highly probable.

Attacking IT networks

A large number of foreign intelligence services have ways of breaking into vulnerable information and communication networks covertly. This often concerns networks belonging to the government, companies in vital sectors and scientific institutions. They break in by:

- hacking websites;
- deploying people who have access to vulnerable networks;
- manipulating software and hardware systems available on the international market.

A dangerous subscription

Many civil servants have a subscription to one of the European Union's news services. An attacker can send them an email with an infected attachment. As the email appears to have been sent from the news service of the European Union, the civil servants do not hesitate to open the attachment.

A coordinated digital attack

In 2009 it came to light that the espionage network GhostNet was hacking into hundreds of embassies, ministries and international organisations. GhostNet operated by way of infected Word and PDF documents. As soon as a computer had become infected, GhostNet would start to copy the documents and tap any conversations conducted via webcams and microphones. Nearly all the computers used to run GhostNet were traced to China.


1307/23/13
130 7/23/07

What can you do?

What can you do to limit the risk of espionage? Here are the AIVD and MIVD's recommendations:

Lay down security procedures and chart information streams

Lay down security procedures in detail and chart the situation regarding IT and other information streams clearly. This will enable quick intervention and damage limitation in the event of information misuse.

Only pass on confidential information to those people who need it

If you are dealing with information that is only relevant to a limited part of your organisation, clearly demarcate the group who should be privy to it. Limit access to confidential information to the people who really need it. Act on a 'need to know' basis instead of a 'nice to know' basis.

Only give access to workstations containing confidential information to those people who need to be there

Access to workstations containing confidential information should be restricted to those members of staff that actually need to carry out activities at that workstation. Act on a 'need to be there' basis instead of a 'nice to be there' basis. Also make sure that the workstation is monitored and supervised.

Be on the look-out for suspicious behaviour

Pay attention to the following behaviours, which could point to espionage:

- An acquaintance is gradually trying to build up an increasingly close bond with you, a process that could go on for years. He does this in order to get you to work for him. Indications are:
  - this acquaintance devotes intense and lasting attention to his relationship with you;
  - this acquaintance asks you for small favours, increasingly asking you for confidential or classified information;
  - increasingly, you find yourself meeting this acquaintance in a social context outside of work;
  - this acquaintance frequently makes appeals to ideological, ethnic or religious motivations;
  - this acquaintance offers you money directly;
  - this acquaintance is blackmailing you to get you to cooperate.

- A stranger asks for confidential information from a member of staff who is not responsible for this information within the organisation.
  Indications are:
  - the person asking the question has never met the staff member before;
  - the person asking the question has an email address that is registered abroad;
  - the person asking the question says that he or she is a student or advisor;
  - the person asking the question says that he or she cannot get hold of this information anywhere else.

- An attractive man or woman is showing a conspicuous interest in you, which extends to your private life. There are intelligence services that use sexual seduction as a tactic to discredit someone or to get hold of confidential information.

The British Prime Minister's data at risk
A British government member of staff allowed himself to be seduced during an official visit abroad. The next morning his Blackberry was missing. Even though the device almost certainly did not contain confidential information, there was a risk of the appliance being used to break into the server of the prime minister's official residence.

- Conspicuous behaviour during visits.
  Indications:
  - you are, or your visitor is accompanied by an embassy staff member;
  - the subject of conversation is different to what was arranged beforehand;
  - members are added to the delegation at the last moment;
  - a visitor has 'lost their way' and is roaming the building on their own.

- Suspicious job applicants, students and requests for internships.
  Indications:
  - the applicant comes from an organisation with ties to the government;
  - the applicant comes from a company or a country with an authoritarian regime;
  - the work is of a more or less confidential nature;
  - the job is for a few years only and the applicant's salary demands are modest.

- Suspicious invitations to conferences and seminars.
  Possible signs:
  - your expenses are all taken care of;
  - during the conference you are approached by people wearing incomplete and unclear name badges;
  - during the conference people show an explicit personal interest in you.

- Invitations from embassies. To visit the embassy's home country or to receive a decoration.

Report incidents

Make note of any incidents. You can deduce undesirable attention from infringements of security regulations and procedures.

Take the risk of espionage into account in the general management of your organisation

In order to protect the information and knowledge held within your organisation you could consider the following aspects:

- *Identify the core interests of your organisation*.
  This means listing the interests you want to protect alongside the relevant risk or risk scenarios that are conceivable for your sector and your protection measures.
  Pay attention to:
  - awareness among staff of the actual possibility that espionage could take place in your organisation too;
  - digital attacks and the integrity of your digital information systems;
  - physical protection against intruders.

  This risk analysis should establish who needs to be protected against what. This also has a bearing on business considerations: what do you value more, your organisation's patented knowledge or commercial strategy?
- *Compulsory risk assessments*. Some companies are obliged to perform a risk assessment. If they receive assignments of a classified nature from the Ministry of Defence, for instance, companies need to comply with the conditions laid down in the General Security Requirements relating to Defence Orders (*Algemene Beveiligingseisen Defensie Opdrachten*, see www.mivd.nl). Contracts can also contain so-called project security instructions.
- *Look upon security measures as an added value* instead of a restriction on your freedom of action: all members of your organisation should regard safety measures as a 'business added value'.
- *Register and analyse reports of possible espionage or potentially related unaccountable incidents*: this will show up trends that do not come to light in a more decentralized mode of observation.
- *Foster a culture of openness, in which it is possible to talk about risks*: employees need to be able to discuss the risks they themselves and others may be running, relating to their actions, for instance, or to confidential material.

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 'Digital Espionage. What are the risks?'
- the brochure 'Espionage during travel abroad. 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 44 190 27
Fax: +31 (0)70 44 190 10
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, March 2004
2nd print, July 2005
3rd print, July 2008
4th translated revised print, March 2010

Photographs
Hollandse Hoogte