Espionage and security risks

Invisible, but still existing

Algemene Inlichtingen- *en* Veiligheidsdienst

Defensie

Ministerie van **Binnenlandse Zaken** *en* **Koninkrijksrelaties**

Espionage and security risks

Invisible, but still existing

Contents

Foreword

This brochure provides information about undesirable intelligence activities in the Netherlands. Several foreign intelligence organisations are conducting activities in the Netherlands that may harm our national security. In addition to traditional espionage activities, such as gathering secret military, political, economic and scientific information and influencing political-administrative decision-making, these services also focus on influencing migrant communities in the Netherlands, monitoring and intimidating opponents resident in this country and on the illegal procurement of equipment, material and knowledge for the production of weapons of mass destruction.

It is the task of the General Intelligence and Security Service (AIVD) and the Defence Intelligence and Security Service (MIVD) to identify such activities, to help terminating them and to arm society against them. It is important that people working in the public service and the private sector are aware of the risks constituted by espionage. This brochure is meant to contribute to this awareness. It also provides a number of tips to identify and prevent espionage.

S.J. van Hulst
Director General of the General Intelligence and Security Service (AIVD)

General Major B. Dedden
Director of the Defence Intelligence and Security Service (MIVD)

1 Espionage: still relevant to our times

Since the end of the Cold War era, many people have been inclined to think that the threat from espionage was largely a thing of the past. In the Netherlands too, security awareness in this area has slackened among citizens and authorities. Although governments can largely satisfy their need for information by consulting open sources, they also use, for example, their intelligence services in order to obtain secret political, military and economic information. When such intelligence activities pose a threat to national security, we call it espionage.

Until 1989 the threat constituted by espionage mainly emanated from intelligence services from the former Eastern bloc countries and China. In recent years, however, the scope of the threat has considerably widened, not only in terms of the amount of foreign intelligence activity, but also in terms of the diversity of the focus areas for this activity. Various foreign intelligence services have proved to be interested in a wide range of subjects. Over the years, both the AIVD and the MIVD have established that the damage caused by activities of foreign services in the Netherlands is still substantial. More details about this will be given hereafter.

1.1 An invisible phenomenon

One of the main characteristics of effective espionage is its invisibility. Professional intelligence services go to great lengths to cover up their activities and achievements. Some cases of espionage have nevertheless been exposed, and these have provided insight into how foreign intelligence services operate and what they are interested in. Obviously, the resulting damage to Dutch interests usually does not get much publicity. And the fact that only a small number of cases make it to the media adds to the dwindling public interest in the phenomenon. But espionage is still relevant to our times, and sometimes it is even closer than you think.

In February 2003 eavesdropping equipment was discovered in the office of the European Council in Brussels. A major meeting hall, as well as rooms used by the delegations of the United Kingdom, Austria, France, Germany and Spain were tapped. Over the past few years, several important meetings of various European bodies were held in the meeting hall in question. The eavesdropping equipment had probably already been planted during the building of the office in 1995. So far it has been unclear which country is behind the eavesdropping operation. The scope of the system and the connections with extensive cables suggest a large-scale technical operation, possibly set up with help from inside.

1.2 Manifestations of foreign espionage

Foreign intelligence activities in the Netherlands mainly manifest themselves in the following focus areas.

1 *Violation of political and administrative integrity*

Espionage may lead to serious violation of political and administrative integrity. Sometimes the activities of foreign intelligence services are aimed at obtaining secret government information on political, military or economic subjects, or at improper influencing of politicians, public servants and decision-making processes. This may involve corrupting of Dutch government officials.

FBI agent Robert P. Hanssen was arrested in the United States in February 2001. It turned out that he had started spying for Russian intelligence services as early as in 1979, in exchange for 1.4 million dollars in money and diamonds. Hanssen's activities allegedly led to the execution of at least two American double agents within the Russian KGB in the days of the Soviet Union. Hanssen was sentenced to life imprisonment in May 2002.

Over the past few years the AIVD and the MIVD repeatedly established that officers of the Russian military intelligence service GRU approached officers of the Dutch Ministry of Defence, asking them straight out for information about military matters.

2 *Infringement on the economy and the scientific-technological capacity*

Several foreign intelligence services are trying to collect information on economic and scientific-technological subjects. The major part of that information comes from publicly available open sources or can otherwise be obtained in a non-clandestine way. In some cases, however the

information is indeed gathered in a clandestine way. Foreign intelligence services are particularly interested in large international tenders and research projects in the areas of biotechnology, ICT and military technology.

Espionage that leads to leaking of technology developed and financed in the Netherlands may undermine the international legal order and stability. It may also harm the international competitive position of the Netherlands. Companies and research institutions in the Netherlands and other western countries are espionage targets for countries seeking to reduce their economic and technological inferiority. But also technologically advanced states do not hesitate to improve the competitive position of their national trade and industry by means of espionage at the expense of foreign competitors.

A prominent example of clandestine gathering of military-economic information was exposed in 2002, when in Sweden three employees of the telecom company Ericsson were arrested on suspicion of espionage for Russia. Two Russian diplomats who had been active as intelligence officers were expelled. Ericsson is mainly known for its mobile phones, but the company also develops radar and missile guidance systems for the Swedish airforce.

In recent years it happened several times that Chinese students and scientists who were (temporarily) studying or working in the West proved to be involved in intelligence activities. These persons usually stay in the West as part of official Chinese government programmes for intensification of knowledge: public programmes aimed at raising the inferior Chinese knowledge economy to a higher level. In some cases participation in such programmes proved to serve as a cover. A couple of years ago, two Chinese students in the US succeeded in collecting American information on the production of a chemical substance that is used in sensors and weapons. They managed to pass the information to China before their activities were discovered.

3 *Proliferation of weapons of mass destruction and military technologies*

The presence of relatively high-grade technological knowledge and the Netherlands' position as a junction of logistic and transport infrastructure have made this country an attractive target for countries that try to obtain - in or via the Netherlands - material, means of production or expertise for the development of weapons of mass destruction and missile programmes. In addition to this, it has been established that representatives of foreign intelligence services in Western

countries, including the Netherlands, secretly try to obtain sophisticated military or defence-related technologies .

The espionage activities of the Pakistani nuclear expert Abdul Qadeer Khan at the Dutch uranium enrichment plant at Almelo in the 1970s have helped Pakistan to obtain the required nuclear technologies for the development of its own nuclear weapons programme.

In April 2003 a former employee of the defence company British Aerospace was sentenced to ten years imprisonment for an attempt to sell missile secrets to Russia. He was found out when he tried to sell stolen documents to an officer of the British security service whom he mistook for a Russian agent.

4 *Support to international terrorism*

A number of countries give support to internationally operating terrorist networks. This phenomenon is known as state-sponsored terrorism. This support may involve the provision of money and goods or the provision of services, such as surveillance operations or accommodation.

Four members of the Iranian-Kurdish opposition were killed in a bomb attack on the Berlin Mykonos restaurant in September 1992. The trial following the attack showed that it was the Iranian government who was behind the attack.

5 *Undesirable influencing of migrants*

A number of foreign intelligence services represented in the Netherlands, mainly from the Middle East, North Africa and China, are involved in manipulation, influencing an controlling of migrant groups in this country through so-called control and influencing networks. These networks try, for example, to obstruct the integration of former compatriots into the Dutch society. But these control networks are also used for pressuring migrants into (eventually) espionage activities for their country of origin.

A recent development that gives reason for concern is the tendency towards radicalisation within part of the Muslim communities in the Netherlands. There have been indications that behind the scenes a number of foreign governments are playing a role in ideological influencing which leads to radicalisation of certain groups and individuals. This radicalisation involves the risk that people isolate

themselves from the Dutch society and resort to violent and other unwelcome activities to express their anti-western sentiments.

In 1999 the then National Security Service (BVD) discovered that a high-ranking employee of the World Islamic Call Society, who acted as imam at a Moroccan mosque in Utrecht, was in fact a representative of the Libyan intelligence service. The man used his position as imam as a cover for his pro-Libyan activities. His efforts were aimed at limiting the integration of the Muslim community into the Dutch society as much as possible. He was declared an undesirable alien and subsequently expelled on the basis of an official BVD report.

6 *Infringement on vulnerable/vital government and ICT networks*

In recent years we have been confronted with spectacular attempts by hackers to paralyse sensitive international communication networks of government organisations, vital companies and military research laboratories. However, foreign intelligence activities in these areas are usually aimed at obtaining information unnoticed. Many foreign intelligence services are capable of breaking into information and communication networks. To that end they use various methods, including hacking, the deployment of human sources with access to vulnerable networks and manipulating software and hardware systems that are offered on the international market. Society in the Netherlands has become increasingly reliant on such vulnerable processes and ICT structures.

1.3 What can you do yourself?

The AIVD and MIVD give security advice to organisations that are of vital importance for the continued existence of the social order, as was laid down in the Intelligence and Security Services Act (Dutch abbreviation Wiv 2002). It is of great importance, however, that government organisations, companies and research

institutions are able to assess themselves whether they may be a potential target of foreign intelligence activities. Obviously, such an assessment is closely connected with the nature of the organisation in question and its knowledge infrastructure.

It is essential to define the interests and objectives of the organisation in order to gain insight into potential threats, the defence against them and, after balancing these elements against one another (a risk analysis), the risk run by the organisation. Making such a risk analysis is standard procedure for companies who get defence-related orders with a classified character. Such companies have to meet the conditions stipulated in the General Security Requirements for Defence Orders (Dutch acronym ABDO). It also happens that 'project security instructions' are included in contracts for certain orders. But even if such is not the case, it is recommendable that an organisation makes its own risk assessment.

1 *Espionage: by whom?*

It frequently happens that foreign intelligence officers operate in the capacity of diplomat, student or businessman, which gives them easy access to relevant political, business and scientific circles. They may be members of official delegations and diplomatic representations, but they may also operate under the cover of private companies, foreign media and scientific institutions. Intelligence officers also enter the country via international migration flows. Several foreign governments encourage their scientists, businessmen and students to collect specialist information on military and scientific-technological subjects abroad.

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

The various security procedures within a company should be laid down in detail. And it is important to monitor information flows. Both the ICT situation and other types of information flows should be mapped out in detail. Insight into these information flows makes it possible to intervene at an early stage and to limit possible damage in case of possible abuse of information. If certain information is only relevant to a limited part of the organisation, this 'group of insiders' should be

clearly defined, based upon the need-to-know principle, instead of the nice-to-know idea. In other words: access to confidential information should be restricted to those who really need that information in the performance of their duties.

Analogous to the need-to-know principle, there is also the need-to-be principle. Only employees who actually have to work at a place where confidential information is, should have access to that place. Other important conditions are supervision and checks, while incidents should always be reported. A breach of security rules and procedures may be a sign of undesirable interest.

1.4 Indications for possible espionage

Espionage can be prevented by paying attention to behaviour that might indicate espionage. A few examples:

- Attempts made by an acquaintance or friend to make a person do certain things for him on the basis of a personal relationship that has gradually evolved between himself and this person, sometimes over a couple of years. The acquaintance or friend has put much and intensive effort in cultivating this relationship over a long period of time. Initially he just asks small 'services', but very gradually he will ask for more confidential or secret information. He will meet the person in question more and more often privately, outside the office, and he often appeals to ideological, ethnical or religious motives. In some cases money is offered directly, or people are pressured by means of blackmail. Potential targets of foreign intelligence activities are, for example, dissatisfied or disappointed employees, but also owners of private property or other assets in the relevant country of origin.
- Requests for information with a confidential character made by unknown persons to other employees than those who are responsible for that information within the organisation. Indications may be: the employee who receives the request has never met the requestor, the requestor's Internet address has been registered in another country, the requestor claims to be a student or adviser or the requestor claims that he cannot obtain the requested confidential information elsewhere.
- Conspicuous behaviour during a visit. Indications may be: visitors are accompanied by a member of the embassy staff, the subject for discussion turns out to be different than the planned subject, persons are added to a delegation at the last moment or a visitor is 'accidentally' roaming the building.

- Suspicious applications, students and requests for trainee posts. Indications may be: the applicant comes from state-affiliated organisations or companies in countries with an authoritarian regime, the job concerned has a rather confidential character, the application concerns a period of a couple of years and the applicant is satisfied with a limited salary.
- Unusual invitations for congresses and seminars. Indications may be: all expenses are paid for, during the congress the invitee is approached by persons with incomplete, vague name badges or persons exhibiting obtrusive interest in personal matters.
- Invitations from the embassy of the invitee's country of origin, for example in order to visit the country or to receive a decoration.

For the sake of good order: the term intelligence officer in the above text refers to both men and women. The traditional idea that 'intelligence work is a men's work' is far from realistic.

1.5 In conclusion

Be aware of the risk of espionage and raise awareness of this risk within your organisation. The AIVD and MIVD are interested in reports about espionage activities or incidents, and if you have doubts, you can ask these organisations to help assess whether it may really be espionage.

If you have any questions about the matter described in this brochure, you can ask the AIVD or MIVD for more details, either directly or through a contact person of your organisation.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) or General Intelligence and Security Service

P.O. Box 20010
2500 EA The Hague
Telephone (070) 317 86 10
Fax: (070) 320 07 33
Internet: www.aivd.nl

Militaire Inlichtingen- en Veiligheidsdienst (MIVD) or Defence Intelligence and Security Service

Van der Burchlaan 31
2597 PC The Hague
Telephone: (070) 441 90 27
Fax: (070) 441 90 10
Internet: www.mindef.nl

1.6 Recommended information

Annual reports of the AIVD (formerly BVD);
Annual reports of the MIVD (formerly MID);
Regulation Information Security Government Service – special information 2004, published by the Ministry of the Interior and Kingdom Relations;
ISO 17799 – Code for information security.

Web sites with information about intelligence and security services:
www.aivd.nl; www.mindef.nl; www.fas.org; www.intelligenceonline.com; www.nisa-intelligence.nl; www.globalsecurity.org; www.oss.net; www.intellnet.org.

Maart 2004