# Analysis of vulnerability to espionage

## Espionage risks and national safety and security

# Contents

# Executive summary

The Dutch Minister of the Interior and Kingdom Relations (BZK) acknowledges that economic, strategic, technical and scientific espionage form a current threat to Dutch national safety and security. To gain a deeper understanding of this threat, and in order to make recommendations for its further reduction, the General Intelligence and Security Service of the Netherlands (AIVD) and the Directorate General for Safety and Security (DGV) at the Ministry of BZK have jointly analysed the risks from espionage in the areas of economic welfare & scientific potential, public administration and critical infrastructure. In the process of conducting its counterespionage analyses, the AIVD has observed that a number of foreign intelligence services are actively gathering information in sectors within these areas of attention.

Through various interviews and through use of available intelligence data from the AIVD, information and data were identified that would harm the Dutch national security if attained by foreign intelligence services/governments. Such data or collections of data are referred to in this report as core interests. The various ways in which *core interests* are vulnerable to espionage are referred to as *vulnerabilities*. These too have been analysed. As a result, the analysts concerned make a number of general recommendations based on the insights and conclusions described in this report. These recommendations point the way towards a follow-up policy trajectory under the umbrella of the Dutch national strategy of safety and security. In this follow-up policy trajectory the general recommendations will have to be made concrete and assigned to action owners.

## Core interests

The analysis reveals that core interests can be found in all sectors investigated. These core interests can roughly be divided into the following categories:

- Datasets and blueprints: this relates to databases, designs and drawings in organisations;
- Positions and strategy: for example, policy premises, long-term philosophy and negotiating strategies;
- Emerging core interests and infrastructure: for example, scientific innovations that may be able to make important contributions to the Dutch economy in the future.

## Vulnerabilities

The most important pretexts for espionage activities by foreign intelligence services can be categorised as 'people' and 'technology'. Intelligence services try to obtain information relevant to them via people who have direct or indirect access to this information or by deploying technical devices in order to hack, tap or monitor. The various ways of intercepting telecommunications form a significant vulnerability in this context. The analysis also reveals that the increasing interconnectivity and complexity of computer systems and the linking of data storage systems increase vulnerability of sensitive data. Outsourcing activities such as system and server management, data warehousing and data processing likewise carry the risk of espionage.

Targeted policy in both the private and public sector can serve to strengthen resistance to espionage and make the core interests of the Netherlands more secure. The quality of this policy will determine the extent to which core interests are vulnerable to intelligence activities. The analysis shows that certain policy decisions have inadvertently increased vulnerability to espionage activities in a few sectors. The promotion of knowledge migration from and to the Netherlands, for instance, has had the undesirable side-effect of enabling intelligence officers to conceal themselves relatively easily among the student population.

Counteracting intelligence activities requires those who are at risk of being spied on to be aware of the fact that they may be interesting to foreign services. It also requires them that they are aware of how intelligence activities are carried out. The analysis shows that awareness of espionage in the sectors concerned is often low. This limited awareness is visible on three levels:

- *Awareness of the value of information:* organisations and individual workers sometimes fail to realise, or insufficiently realise, the value of the information they possess or to which they can obtain access;
- *Awareness of security:* the security and safety of core interests do not always command sufficient attention in organisations; other considerations often take priority in their policy;
- *Weighing up interests:* short-term organisational interests and/or government interests are (often) given precedence over long-term interests. The defection of strategic knowledge or activity relevant for long-term Dutch national safety and security to other countries is given insufficient attention.

## Recommendations

Based on these conclusions, three main recommendations are made for further strengthening resistance to espionage:

- Actively strengthen awareness among managers and workers in government, industry and institutions of the value of the information they have and of the possible interest foreign governments may have in this information.
- Work on changing the culture around security. In this respect users, the organisation of data flows and databases and the techniques used for detecting incidents are important focus areas.

- When formulating policy, pay explicit attention to protecting core interests and the effects of policy on the Netherlands' interests in the longer term. These recommendations are illustrated in chapter 10 with a number of possible, more concrete prospects for action. It is not within the remit of the analysis to make such actions more concrete or assign them; this will have to be done by the policy departments concerned in a follow-up policy trajectory.

# Rationale

Our society is vulnerable. National safety and security can be threatened in various ways. If vital interests of the Dutch state and/or society are threatened to such an extent such that potential societal disruption could occur, national safety and security becomes an issue. Some dangers are patently obvious, such as the risk of natural disasters or a terrorist attack. Others are not as obvious because they manifest themselves stealthily or they happen, largely or entirely, hidden from view, even for practised observers. Espionage is an example of this.

The National Safety and Security Strategy will enable the government of the Netherlands to determine which threats could endanger national safety and security and how they should anticipate such threats, of whatever nature. The Dutch National Safety and Security Strategy is a comprehensive, government-wide approach, under the responsibility of the Minister of the Interior and Kingdom Relations in the Netherlands.

The Directorate-General for Safety and Security is responsible for coordinating the implementation of the strategy. In the context of protecting national safety and security, the AIVD has the task of identifying and countering intelligence activities from other countries. As part of this task, the AIVD, the Directorate-General for Safety and Security and the Ministry of the Interior and Kingdom Relations have jointly investigated which types of information (referred to as core interests in this report) are important for Dutch national safety and security and which are at risk of interest from foreign powers by means of espionage.

The full significance of espionage on national safety and security has never before been highlighted from this perspective. The aim of this broad, exploratory compilation is to identify the risks of espionage more fully and to make a few general recommendations so that the risks that are outlined can be reduced as far as possible.

Threat

Espionage

Intelligence activities

Breaches of security

National Safety and Security

Strategy

# 1. Introduction

The Minister of the Interior and Kingdom Relations in the Netherlands acknowledges that economic, strategic, technological and scientific espionage[1] by a number of countries forms a current threat to the Netherlands. The considerable importance of technological developments leads to concerns about the intentions of other countries to steal this knowledge through espionage and the consequences of this for the present and future Dutch knowledge economy.

Furthermore, the Netherlands' critical infrastructure, which includes the telecom and energy sector, could also be threatened by espionage. The consequences of this could range from protected customer data ending up in the wrong hands, to large-scale digital security breaches at a government level and/or at businesses. The AIVD has identified a number of cases of this form of espionage. One of these involves foreign intelligence services trying to obtain sensitive information about the infrastructure of the telecom sector to aid their intelligence activities.

Foreign intelligence services also try to get hold of classified and other confidential political, military and economic information, including government information, to use for their own national interests. Gathering this type of intelligence is even explicitly embedded in the statutory task of the intelligence services in a number of countries.

The AIVD has established that other countries have a fundamental interest in such areas of interest and it therefore remains essential to focus attention on the phenomenon of espionage and the risks it entails. Every form of intelligence activity by a foreign power in the Netherlands harms Dutch interests. All secret intelligence activities performed by foreign intelligence services on Dutch soil represent a breach of Dutch sovereignty.[2] Not only that, they can affect political, administrative and official integrity, the Dutch technological, scientific, economic and military potential, or the rights of Dutch residents. That is why intelligence activities, including espionage, form a threat to Dutch national safety and security.

## Espionage and national safety and security

When the damage done by foreign intelligence activities leads to the *vital interests of our society and/or state being so adversely affected that actual or potential societal disruption occurs, the Netherlands' national safety and security is jeopardised*. This definition of the term national safety and security has been formulated as part of the National Safety and Security Strategy set up by the Dutch Cabinet.[3] The government of the Netherlands intends that the strategy of national safety and security will ensure that internal and external threats to society and the population on Dutch territory are tackled comprehensively and cohesively. The procedure described in the strategy will enable the Dutch authorities to determine more quickly than before which threats could endanger national safety and security and how these threats could be prevented or its consequences mitigated. Given the fact that espionage forms a threat to national safety and security, it is also important to place this threat within the strategy. This report gives the initial impetus.

The National Safety and Security Strategy contains a definition of five 'vital interests' that the Netherlands ought to protect to ensure national safety and security. The Dutch national safety and security is at stake if one or more of these vital interests is infringed to a level that leads to societal disruption. These five vital interests are:

- *Territorial integrity:* the ability of the Netherlands to function as an independent state, and more specifically, the territorial integrity of the Netherlands. Territorial integrity is jeopardised in the event of, for example, the threat of occupation of State territory by another power, but also in the event of a terrorist attack;
- *Physical security:* the ability of people to function without hindrance in the Netherlands and surrounding areas. Physical security can be endangered if public health is threatened by the outbreak of an epidemic, but also by a dyke bursting on a massive scale or by an accident in a chemical plant.
- *Economic security:* the ability of the Netherlands to function without hindrance as an effective and efficient economy. Economic security could be adversely affected if, for instance, trade with an important foreign partner were to cease.
- *Ecological security:* the ability of the natural environment to recover sufficiently on its own after being adversely affected. Ecological security could be jeopardised by disruptions to the management of surface water or climate change.

[1] The AIVD generally uses the broader term 'intelligence activities'. Intelligence activities can be described as undesirable activities carried out by foreign powers (generally intelligence services) on Dutch territory. Espionage refers exclusively to those intelligence activities aimed at acquiring information secretly or under false pretences (and does not therefore include such activities as exerting undue influence, disruption or other secret, undesirable activities). This analysis focuses on espionage and so this, rather than the broader expression 'intelligence activities', will be the term used throughout this document. The term intelligence activities will only be used if a form of intelligence activities other than espionage is explicitly alluded to.

[2] The only exception to this is intelligence activities for which the government of the Netherlands has received prior notification and has given its permission.

[3] The Dutch House of Representatives, 2006–2007, 30821, no. 3

- *Social and political stability:* the ability of the social climate, in which people can live together in harmony within the framework of the democratic constitutional state and shared core values, to continue to exist undisturbed. Social and political stability could be jeopardised if changes occur in the demographic structure of society, to social cohesion or the degree to which the population participates in social processes.

### Espionage as a danger to national safety and security

Intelligence services could harm these 'vital interests' and thus the Dutch national safety and security. If the democratic process is secretly affected, this could harm social and political stability. To take an even more extreme case, a country might offer support to a terrorist network that carries out an attack in the Netherlands. In that case, intelligence activities would be endangering the physical security of people in the Netherlands and the territorial integrity of the Netherlands. And finally, the intelligence activities of other countries could harm Dutch economic security if, for example, valuable business secrets are stolen through espionage, resulting in the loss of the Netherlands' competitive position and large-scale loss of income for the Netherlands.

### Research

In recent years, the AIVD has detected espionage in areas such as economic welfare and technical and scientific potential, public administration and the Netherlands' critical infrastructure. This knowledge makes it desirable to look at all these areas of interest to gain an overview of the most important *information within these areas of interest, which, should such knowledge become known, could adversely affect national safety and security and which can be assumed to be of interest to foreign intelligence services/governments.*[4] Such data or collections of data are referred to in this report as core interests. The way in which core interests are vulnerable to espionage, referred to from now on as 'vulnerabilities', are defined in this report as *the principle factors that enable a core interest to be adversely affected by espionage.*

This need to find out about interests and vulnerabilities has led the AIVD and the DGV to jointly conduct research into these areas of interest. To this end, a large number of representatives of sectors within the areas of interest (economic welfare and technological and scientific potential, public administration and critical infrastructure) were interviewed. These interviews form the basis for this report. In addition, use was made of information from AIVD studies.

## 1.1 Aim

The AIVD and the DGV intend this report to broadly outline the most important core interests that have been identified and their associated vulnerabilities in the sectors surveyed. It is explicitly not their aim to provide an exhaustive view of all Dutch core interests and vulnerabilities. This would hardly be possible given the high speed at which specifically technological developments and innovations occur. Moreover, in order not to inadvertently provide pointers for the intelligence activities of foreign intelligence services, not all the findings appear in detail in this publicly available publication.

The results of the research, and the general recommendations made as a result, offer leads for further policy development as a means of better protecting the Dutch core interests identified. The results discussed here can be used for further policy development as part of the National Safety and Security Strategy. This report will also enable the responsible professionals in businesses and government to identify and better protect their own core interests and vulnerabilities.

## 1.2 Research method and delineation

The analysis of core interests and vulnerabilities in this report is based to a great extent on interviews with dozens of representatives of business and organisations in sectors prominently represented in the aforementioned areas of interest (economic welfare and technological and scientific potential, public administration and critical infrastructure). This report therefore focuses on core interests in these sectors. Further clarification and analysis of this information was obtained by making use of the information already available at the AIVD about intelligence activities detected, modi operandi and vulnerabilities.

The choice of the sectors mentioned arose in the first place because, partly as a result of increased globalisation, international interdependency and complexity, the AIVD suspects and has observed a need for intelligence about these very sectors.[5] The sectors and threats that are already well known, or for which responsibility has already been explicitly assigned, have not been included in the research. That is why no, or hardly any, attention is paid to the more traditional espionage targets of military and nuclear technology and knowledge. However, not including these two areas does not imply in any way that there are currently no espionage activities in these areas in the Netherlands.

[4] Core interests can also be damaged by non-state actors (terrorist organisations, foreign opposition groups operating in the Netherlands, etcetera). These are outside the scope of this analysis. And anyway, the core interests and vulnerabilities that are threatened by state actors will, in many cases, be the same as those threatened by non-state actors. There may, however, be differences in the aims and modi operandi of these actors.

[5] Greater interdependency makes it desirable for states to know about positions and strategy in these areas.

## 1.3 Layout of the report

After the introductory chapter, chapter 2 contains a description of the three categories of core interests singled out in this report. All three categories of core interests can be found in some sectors, while only one or two emerge in other sectors. The sectors surveyed are described one by one in the next five chapters. In these chapters, the core interests are arranged as described in chapter 2. Chapter 8 then describes the various vulnerabilities that have emerged from the research and which, to a greater or lesser degree, touch on all the core interests reviewed in the previous chapters. Finally, chapters 9 and 10 contain the conclusions and the general policy recommendations respectively.

Core interests

Strategy

Stereotypical targets

Datasets

# 2. Types of core interests

Interviews with representatives of parties in the field revealed that core interests in the sectors surveyed can roughly be divided into three categories:

- Datasets and blueprints
- Positions and strategy
- Emerging core interests and infrastructure

These three categories will be explained further in the next sections.

## 2.1 Datasets and blueprints

Core interests in the category datasets and blueprints form the most stereotypical targets for espionage. These relate to actual and compiled information (datasets) or detailed, usually technical, information. These could be blueprints of advanced technologies or descriptions of important production processes. But files of privacy-sensitive data also come under this category. Examples of this are the addresses and contact details of organisations, Municipal Personal Records Databases (GBA) and the calls and payment data of customers of a telephone services provider.

This category of data is often already protected by the organisation itself and is considered confidential by the organisation because, for example, the information could be interesting for competitors or criminals. But such information may also be targeted by intelligence services. This is then no longer classified as criminal or industrial espionage but as economic espionage: actively gathering commercial knowledge by *state actors* for the benefit of their own economy.

**Reverse Engineering**
On a visit to a Dutch company, a foreign delegation asked whether they could look at a prototype. The delegation was given the prototype but it was never returned. It is very likely that the prototype was dismantled in order to find out how it worked by means of reversed engineering. Probably they were then unable to reassemble the prototype correctly and so were unable to return it.

## 2.2 Positions and strategy

The Netherlands, as every other country, has numerous core interests in the category Positions and Strategy. These core interests can be found in government, in business, and where the two intersect. Examples of this type of knowledge are negotiating margins or positions to be taken on an international level. Government information could include the Dutch position with regard to the expansion of the European Union (EU) or to economic negotiations in the Group of Twenty (G-20). Business information could include prior knowledge of the content of tenders or premature knowledge of takeover plans.

Public administration and Dutch business could be substantially damaged by leaks of sensitive policy strategies, policy outlooks and positions. Once in possession of this knowledge, the other party could obviously make more well-considered decisions about the strategy it should pursue, to the detriment of the Government of the Netherlands or Dutch business.

**Greatest espionage scandal in the history of NATO**
In February 2009, the Estonian former Defence Chief, Herman Simm, was convicted of espionage and sentenced to twelve and a half years in prison. Simm had been passing on secret NATO information to the Russian civil intelligence service SVR for years. The amount of information Simm passed on is so vast that NATO calls it the greatest espionage scandal in the alliance's sixty-year history. Simm received enormous sums of money for his espionage work, but money was not his only motive. Another important reason for Simm to work for the SVR was that this service was able to effectively exploit his feelings of frustration and vanity. The Russians held out the prospect of his obtaining a senior military rank and high Russian honours. Simm's contact at the SVR was a Russian intelligence officer who had successfully posed for years as a South American businessman. His cover was assisted by a correct and complete set of identity papers, registration in government databases and a CV that could be verified.

Here, and more so than with any other category, communication about this type of core interest is done by e-mail or telephone. Draft documents, comments, moot points and other relevant information are exchanged intensively between the interested parties by (sometimes wireless) e-mail systems and telephone. This further increases vulnerability of the core interests. Due to the relatively short period in which such information is valuable, telecom interception[6] is one of the obvious methods. Furthermore, knowledge of strategy and positions can lead to more general information that remains valuable for the longer term and which parties can use to anticipate future positions.

[6] In the context of intelligence, interception means 'tapping' telecommunications.

## 2.3 Emerging core interests and infrastructure

The core interests in this category are ideas, scientific research or information and concepts that are currently still public but which have the potential in the longer term to lead to economically or strategically interesting applications. Crucial components of the Dutch infrastructure also belong in this category. Neither of these types of core interests are secret or protected, legally or otherwise, but at the same time they are of vital importance to the future economic functioning of Dutch society.

The third category of core interests differs on one crucial point from the first two categories. Core interests in this category have been made deliberately accessible to a greater or lesser extent or have been made public by their owners. They also differ from the core interests in the other categories due to their time dimension. The full consequences of this category being compromised only becomes visible in the long term. This is in contrast to '2.2 Positions and strategy' and '2.1 Datasets and blueprints', for which the length of time before the consequences of compromise appear is incomparably shorter.

Although core interests in this category need not be stolen by means of 'traditional' espionage activities, account should be taken of the possibly dishonest intentions of research partners or potential buyers. Each case should be carefully considered to see if it is an honest request for collaboration or whether there is a hidden agenda behind the proposed exchange. This makes this category, similar to the other two, important to national safety and security. Those involved can only make a substantiated cost-benefit consideration if they have sufficient understanding of the vulnerabilities in this category of core interests.

**Spying students**
Technological knowledge, even if it is not classified 'secret', can be very valuable to other countries. The Netherlands too can be considered an interesting country in which to gather scientific and technological knowledge. There is often an active international community in the scientific sector (universities and research institutes), which provides intelligence services with additional opportunities for espionage. A number of intelligence services are very active in collecting scientific intelligence and the AIVD is tracking them intensively. The AIVD has indications that students studying abroad are sometimes deployed as spies by the intelligence services of their native countries.

High-quality knowledge

Technology

Knowledge economy

Patent

# 3. Core interests in economic welfare and in technical and scientific potential

Organisations and businesses in the Netherlands are in possession of valuable, high-quality knowledge and expertise. To a substantial degree, the competitive position of the Netherlands is based on this highly developed knowledge and expertise, particularly in technology and applied sciences. The technological knowledge developed in the Netherlands often results in very successful applications in industry. Technical universities, companies' research & development departments (R&D) and public and private knowledge and research institutes form part of the infrastructure of research and development in the Netherlands. The knowledge and expertise built up here is highly thought-of internationally in various areas and makes an important contribution to Dutch economic prosperity.

In a world in which the production of goods is increasingly taking place in low-wage countries, it is important for the Netherlands to continue to play a leading role in research and development. This has led the Government to express its ambition for the Netherlands to acquire (once again) a top international position as an innovative knowledge economy. To do this, it is of the greatest possible importance that innovative knowledge and understanding is not only strengthened, but also retained for the benefit of the Dutch economy.

As indicated previously, economic security is one of the vital interests that ought to be protected as part of national safety and security. The Netherlands' ability to function undisturbed as an effective and efficient economy will guarantee the economic security of the country. Thus damage to the economic welfare of the Netherlands has an immediate impact on national safety and security. Core interests in this area of interest can be found in all categories (datasets and blueprints, positions and strategy and emerging core interests and infrastructure). This last category is prominently represented in this area of interest.

It would be interesting to know how much economic damage is done through espionage. However, up to now, the financial consequences of economic espionage have never been quantified for the Dutch economy. As an indication of the consequences of economic espionage, the Germans have estimated that Germany suffers around 20 billion euros worth of damage through economic espionage every year. Estimates in the US of the damage suffered as a consequence of economic espionage vary tremendously: sums of between 50 and 200 billion dollars a year are mentioned.[7]

[7] Dave Drab, 'White paper: Economic Espionage and Trade Secret Theft – Defending Against Pickpockets of the New Millennium', Xerox Global Services, August 2003.

## 3.1 Datasets and blueprints

The sector of economic welfare and technical and scientific potential has many datasets and blueprints that are of interest to foreign intelligence services. The most important examples are listed below:

### Patents pending

A patent is an exclusive right to an invention, which prohibits others from applying this invention commercially for a certain period. To obtain a patent, a procedure has to be initiated at the Dutch or European Patents Office. The technology and knowledge on which the new product or process is based has to be made transparent for the purposes of the application. This information appears in the patent document that describes the new invention. It is important to describe the technology of the new invention specifically and accurately in order to demonstrate how it differs from already existing patents and thus get a strong patent document.

A patent document of this nature is interesting to third parties, because it contains a detailed description of a new invention. Knowledge of patent applications also provides an insight into the direction in which research in other countries / companies is going. Although patent information eventually becomes publicly available, the application process takes 18 months. Should others acquire the information in that period, it would, for example, offer them the opportunity to adjust their own R&D a year and a half earlier. This makes espionage in this area profitable.

### Unpatented knowledge (possibly intentionally)

Despite the 'monopoly rights' a patent offers, in practice the knowledge can still be used by others. Upholding patent law depends on the willingness of individual countries to insist that their national industries observe these rules. This willingness is not the same everywhere, certainly not when it comes to strategic products or major financial interests. A company may therefore choose not to patent an invention or technology, but to keep it secret. These inventions need not necessarily be technical blueprints; production processes may also be intentionally kept secret. Such unpatented knowledge is interesting to get hold of; after all, it can even be used without openly infringing patents pending.

Core interests in the category of blueprints and datasets can not only be found in the region of patents pending and intentionally unpatented knowledge. The same is true for already developed and applied knowledge and technologies.

In the Netherlands, a number of high-quality applications are relevant in this context, such as the production and application of optics, radar technology and aviation and space technology. The same applies to a certain extent to areas such as applied robotics, non-intrusive scan technologies and innovative applications that can be put to use under water. Techniques and applications that are still being developed are dealt with in section 3.3 'Emerging core interests and infrastructure'. Developments are also taking place in a military and dual-use[8] context; these will be mentioned briefly, but are outside the scope of this analysis.

The knowledge of optics applied in the Dutch scientific world and Dutch business is at a very high level. This technology also complements numerous Dutch operations. Optics are important in such application areas as chip manufacture (lithography) and advanced observation equipment. The latter area of development can be crucial at a strategic and military level. High-quality chip manufacture includes both economic interests and strategic and military interests, with economic interests probably being greater than direct strategic and military interests if we consider that over half of all integrated circuits (ICs, chips) are now made using Dutch photonics techniques. These economic, and strategic and military applications explain foreign intelligence services' interest in research into high-end optics and their application areas, but this has not gone unnoticed. The interest shown by foreign intelligence services is also the reason why Dutch businesses in this sector have a relatively high risk profile in terms of espionage.

High Tech Systems (HTS) is an innovation area that interfaces with many disciplines: mechanics, electronics, photonics and control technology. The central technology is mechatronics, an advanced integration of these disciplines. This technology forms the hub of the motion & control systems that are important in almost all high tech systems.

Mechatronic systems are used in all sorts of products, instruments, systems and sectors: manufacturing processes, consumer electronics, robotics, medical systems, the automobile sector, aviation and space travel, and in technologies developed for the defence sector.

Robotics is an emerging technology with the potential to make its mark on society in the medium to long term. The Netherlands occupies a leading position in certain sub areas of robotics. Dutch autonomous medical robotics and mechatronics are highly regarded throughout the world. The focal point of robotics in the Netherlands involves the application of custom-made robot technology. Robot systems are delivered to clients fully customised to meet their requirements.
The Netherlands in addition has a prominent position in the chip industry, a strong cluster of medical technology and is home to various top international HTS players. A relatively large number of mechatronics patents are applied for in the Netherlands. Their number is far higher than either the European or the US average.

Mechatronics represents an enormous value both economically, militarily and strategically. Such applied knowledge is very attractive to foreign intelligence services.

Radar technology developed in the Netherlands could be very valuable to foreign intelligence services. Radar technology can be used in both a civil context and in a military context. This means that from a national safety and security point of view, the leaking of such knowledge could threaten the Netherlands' economic welfare as well as its territorial integrity.

There is a great deal of knowledge about aviation and space technology and their application in the Netherlands. Such knowledge is interesting to some states. A country (or national industry) could consider it very financially and strategically important to possess such high-quality technologies. Important components of the expertise available in the Netherlands include knowledge of innovative materials and civil and military avionics (hardware and software) Knowledge of satellite technology also forms part of this group.

First and foremost, knowledge about aviation and space technology, and their application, has an economic importance for the Dutch branch of industry that contributes to the development and production of components for airplanes and satellites. If knowledge is lost to third parties, there is a risk that Dutch businesses will suffer economic damage. Participating in international programmes would be endangered because any potential Dutch input has already become known through other channels and consequently, concrete loss of orders for the industry could occur.

Leaking of knowledge could lead to the production of high-quality defence material in countries of concern. Added to that, parties could derive information about Dutch/European defence material and their potential weaknesses from such knowledge. This, too, affects national safety and security.

[8] The applicability of a certain type of knowledge or equipment for both civil and military purposes.

### Hydraulic engineering, hydraulic technology and the management of hydraulics

Water is an integral part of the Netherlands and it has been necessary for the country to build up a great deal of valuable hydraulic engineering knowledge. Dutch knowledge of dams is unique. The request for help in strengthening the dykes in New Orleans in the US after hurricane Katrina struck in 2005 came about for a good reason.

In addition, the Netherlands holds a unique position in the dredging industry. Dutch dredging firms are considered the best in the world and are well represented in the global dredging market. All in all, such knowledge represents enormous value in sizeable infrastructure and other projects, certainly for emerging economies who carry out many such projects (or would like to). The theft of such knowledge would cause substantial economic damage to Dutch business.

## 3.2 Strategy and positions

With regard to the Netherlands' economic welfare and technical and scientific potential, the core interests in the area of Strategy and positions mainly relate to international orders and planned mergers and takeovers of major companies that are heavily involved in the Dutch economy.

### International orders

Contracts put out to tender internationally can involve vast sums of money. Contracts can be so valuable and prestigious that it matters very much to a foreign power that such a contract be awarded to its national industry. If a foreign power knows whether a competitor is going to submit a tender and, if so, if its people can acquire knowledge of the details of that tender, they can take this into account when drawing up their own tender, and so increase their chances of being awarded the contract.

A well-known example of direct economic espionage took place in 1985 when an American aircraft manufacturer was seriously harmed by a French intelligence service. During the negotiations about the delivery of a fighter jet to the Indian government, French intelligence officers were able to discover the terms of the Americans' final offer and pass them on to a French competitor for the order. This competitor succeeded in securing the contract, worth over two billion dollars.

### Knowledge of planned mergers or takeovers

Foreign powers may have an economic interest in planned mergers and takeovers of or by multinationals. Once the players and sums of money are known, other actors could influence mergers and takeovers or even play an active role in them. Takeovers could be prevented in this way or the sums of money involved in a takeover could be lowered or even raised. Other strategic motives can also play a role, such as the desire to keep important companies owned by a national parent company. All this is particularly relevant when one of the parties involved is a Dutch enterprise important for the Dutch economy in terms of employment, taxation contributions or dividend payments. After all, if such an enterprise is damaged economically it indirectly damages the Dutch economy.

## 3.3 Emerging core interests and infrastructure

Technological and scientific knowledge, information and know-how in a relatively early stage of development makes an important contribution to the Dutch economy in the medium to long term. The Netherlands hosts a relatively large number of these core interests, in its technical universities for instance, but also in high-quality technical multinationals or initiatives such as a High Tech Campus.

The importance of such knowledge to the Dutch economy includes opportunities for continuing development and increases its economic value. What is more, being in possession of this type of 'early' knowledge often leads to the formation of a cluster of high-quality spin-off or new companies. It is economically very important to create such clusters on Dutch territory also for the future, once a domain has matured. If knowledge leaks to competitor countries, the chance that clusters will be formed in the Netherlands will decrease, regardless of whether initial investments were made here.

The AIVD has observed that foreign powers are using different means to acquire this knowledge and information and thereby stimulate their own economy. Not only through traditional espionage, but also by having their compatriots educated in the Netherlands (preferably at technical universities) and by acquiring high-quality technological companies. A few of the research areas relevant in this context are discussed below.

In many cases of innovative developments, the potential dual use goes unrecognised, so that developments are less well protected than if people were aware of their strategic or military application potential.

### Innovative materials

The Netherlands is at the forefront of the development of innovative materials. This knowledge area explicitly ties in with the previously described aviation and space technology, but extends far beyond this topic alone. This knowledge can count on arousing the interest of foreign intelligence services. Knowledge of, for example, lightweight composite, or self-healing materials not only has various regular uses, but is also very important for applications with a clear strategic and military nature.

The economic consequences of espionage can be enormous in this field. If Dutch businesses and research institutions are able to supply unique high-performance materials, this directly

contributes to the prosperity of the Netherlands. If such knowledge is leaked to third parties, Dutch companies may be faced with unfair competition. This becomes apparent, for example, in major international cooperation projects, where high-quality knowledge of materials ought to be a unique selling point for Dutch business, but all of a sudden another party secures the ultimate participation. Furthermore, there is a clear strategic interest here: innovative materials are extremely important for the production of knowledge of high-quality defence material. The loss of such knowledge could therefore have direct consequences for the territorial security and other defensive interests of the Netherlands and our allies.

### Biotechnology

Biotechnology is an economically relevant, emergent field of research. It is a broad discipline in which historically, the Netherlands and Japan have been in the vanguard, but where the Netherlands is currently loosing its leading position. The implications of advanced biotechnology applications are nonetheless still vast. Given the enormous economic potential and possible dual-use applications of biotechnology, the Dutch knowledge in this field has value for other governments.

### Bio-based economy

The bio-based economy is an emerging concept focusing on the use of agricultural/organic products as raw materials for all sorts of materials for non-food applications. These are new applications and, in particular, changes in scale. The bio-based economy will be of vital importance in the future to countries such as China and India, given the growing demand in these countries for energy and food. The global shift now anticipated in this direction and the enormous financial and other implications of 'greening the economy' mean that it is economically crucial for the Netherlands to protect its good knowledge position in this field.

### Life sciences

The Netherlands has a number of successful bio-science parks. The park in Leiden, for example, is among the top five in Europe. Substantial investments are being made in these locations and some of them, such as those in Amsterdam and Utrecht, are still being extended. Investments are also being made in specialist scientific research in these parks to develop innovative medical technologies, including biotechnology, and new medicines. Major investments in life sciences will eventually be recouped; new businesses will grow into new players in the pharmaceutical industry and established businesses will make new discoveries. This makes research into life sciences a valuable component of the Dutch knowledge economy. It is as true for life sciences as for many other core interests in this area of interest that, if the knowledge ebbs away just before it becomes economically profitable, investments will have been made without the ability to reap the benefits.

### Nanotechnology

Nanotechnology is a broad scientific domain whose future application potential will have both a social and an economic impact. Nanotechnology is a collective word for applications and techniques that take place on a very small physical scale (or nano scale). Nanotechnology has implications and applications for numerous other fields of applied science, such as cryptology, biology (bio-nanotechnology), physics (photonics, quantum computing), chemistry, biochemistry and medical technology/pharmaceutics. Nanotechnology opens up possibilities for a whole range of new or improved products and is possibly one of the most striking core interests.

Dutch researchers in this field, in both the private and the public sector, are internationally among the very best. The field currently involves economic interests in the form of investments in research and R&D. A leading position in the field of nanotechnology may result in the longer term in spin-off companies and patents that represent an even greater economic interest. If a cluster of first-rate nanotechnology companies were to form in the Netherlands, this would represent an enormous economic interest. In the international competition to become a 'Centre of Excellence' in nanotechnology, the loss of information to other parties could therefore have major consequences for the future position of the Netherlands. A second important notion is that the technology not only represents an economic value, but that numerous strategic (and military) applications are also imaginable, which countries will see as vital for their national safety and security.

**Scientific cooperation in first-rate technology**

The AIVD has established that foreign intelligence services are spying on nanotechnology in the Netherlands, and are prepared to operate boldly in order to obtain the information they are looking for. Recently, more than half of a foreign scientific delegation on a visit to the Netherlands turned out to be intelligence officers. The aim of the visit was to reach further scientific cooperation in the field of nanotechnology. The participants in the delegation were 'real' scientists who understood the subject matter. But they simultaneously were intelligence officers. Ostensibly looking for cooperation, intelligence officers are thus gaining access, under false pretences, to people and companies working on nanotechnology. This is a form of traditional espionage used as a means of acquiring relatively public information.

Data communications

Network layouts

Damage

Interception

# 4. Core interests in the telecom sector

Damage to interests in the telecom sector has an almost immediate adverse effect on national safety and security. Communication, including data communications, is vitally important to enable Dutch society to function unimpeded. Intelligence services can also use the sector as a means of accessing information. And indeed, the AIVD reports that the telecom sector is being targeted by foreign intelligence services. This makes telecom both a core interest and a vulnerability. The vulnerabilities in the telecommunication sector have direct repercussions on all other sectors. Damage to interests in the telecommunications sector has an immediate effect on the interests of the sector itself and/or its users.

Authorities in the safety and security chain (including the police, the AIVD and the Dutch Military Intelligence and Security Service (MIVD)) make use of telephone communication data and other user information for reasons of national security. It is essential to ensure that only these authorised parties can make use of this statutory interception. After all, if foreign intelligence services or organisations were to tap Dutch telecommunications, this would be an infringement of the rights of all Dutch citizens. Furthermore, it would seriously undermine confidence in the Government.

The enormous interest shown by foreign intelligence services can be explained by the fact that telecommunication is a bottleneck through which a large proportion of all 'technical' espionage activities have to pass. Apart from offering interception opportunities, this sector also offers numerous opportunities for carrying out active attacks on any computer systems linked to it. Practically all core interests could be reached in this way.

Telecommunication is a sector that has undergone tumultuous development in recent years as a result of continuous innovation. The sector's core interests and vulnerabilities are therefore subject to change, probably more so than in other sectors. Something that is well protected today, might be vulnerable tomorrow. It is therefore crucial to continually monitor all technological and digital developments.

## 4.1 Datasets and blueprints

Digital data communication involves data that could potentially offer access to information about other core interests in other sectors, such as strategic decision-making at government level or corporate secrets.

### Information in the telecom network

The AIVD has substantial indications that foreign intelligence services are interested in information on the Dutch telecom network. This includes telephone communication data and customer data (who is calling whom, subscriber data linked to telephone numbers, MAC addresses (unique numbers that identify computer equipment), e-mail addresses, home addresses and IP addresses). Such information is relevant for foreign intelligences services' data mining and data analysis activities.

Telecom information has been one of the most important sources of information for intelligence services from its very inception. Undesirable activities carried out by foreign powers aimed at acquiring telecommunication data could adversely affect Dutch interests, even if these activities are not directly aimed at the Netherlands. Another imaginable scenario is attempts to get hold of information with economic relevance. In some countries, getting hold of foreign economic information is actually part of the intelligence services' explicitly formulated orders. In addition, attention may be focused on telecom services (or their content) offered by way of the sector to other sectors, such as the clearing and settlement of funds transfers in the financial sector or administrative transactions in the energy sector.

Such activities do not always remain restricted to companies based in the Netherlands. They can also occur at a Dutch company or institution based abroad.

The networks carry huge quantities of data that come from other sectors, such as the energy sector, banking data and government communication including:

- invoicing data from telecom providers;
- data communication for regulating and controlling the critical infrastructure;
- data communication related to digital financial and economic transactions;
- IT infrastructure and communication systems belonging to the Government of the Netherlands, the EU and NATO in the Netherlands;
- confidential corporate information sent over a network.

Improper viewing, copying or stealing of information from the telecom sector can have a number of repercussions. Economic damage could occur if corporate secrets end up in the wrong hands. If strategic information originating from the Government of the Netherlands were to get into foreign hands, the Netherlands' position internationally could be undermined.

And finally, legal interception (by the Government of the Netherlands) could be interfered with if foreign parties are able to obtain access to these legal means of interception.

### Information about the telecom network

If a foreign intelligence service has information about the infrastructure and organisation of the networks themselves, it can get an idea of the vulnerabilities in the network. An economic advantage might also be attainable as a result of acquiring such information surreptitiously. For example, if a foreign intelligence service is able to get hold of technical information about how the network is organised, it could obtain access to a telecom provider's infrastructure and then find out about the communication on the network or make use of the provider's services. It would also be able to get an idea of the parties involved in managing and maintaining the networks. This might provide information about ways of gaining access to the networks.

Intersections of telecommunication service and data flows, such as AMSIX (the biggest switchboard in Europe, which is located in the Netherlands) are very valuable. These intersections could act as access points or tapping points for intelligence services, providing them with the information mentioned above.

## 4.2 Positions and strategy

Although interception of telecommunication is a good way of acquiring strategic knowledge about core interests, strategic knowledge about this sector itself is probably not the primary target of espionage. Such knowledge will mainly be sought by intelligence services in order to establish a position within the Dutch telecom infrastructure. Knowledge of the market could help foreign telecom companies and suppliers (of data warehouse services[9], billing services, or of hardware and software, for instance) to enter the Dutch market. The AIVD reports that some of the companies that operate in the Netherlands as suppliers originate from high-risk countries and that some have past or present links with foreign intelligence services. This provides an increased risk of espionage.

## 4.3 Emerging core interests and infrastructure

Owing to the information sent over this network, and the importance of Dutch society being able to function unhindered, the physical infrastructure of the Dutch communication network is a core interest in itself. Should unauthorised actors obtain access to telecom networks, or should parties that already have access abuse their authorisations, damage could be done to both national safety and security, to the privacy of citizens and to the integrity of the telecom sector. The interests of users of the telecom infrastructure (authorities and companies) could also be adversely affected. Viewed in this light, all, or part, of the telecom networks being in the possession of foreign parties is a potential threat. Ownership obviously also increases access to information about the network itself, as well as the data sent over it. Both types of information could be acquired from such companies if they are put under pressure by a foreign intelligence service.

[9] A database in which data from a number of systems is copied in order to be able to generate reports and analyses from this information.

Economic Security

Leaks

Crucial

Opposition groups

# 5. Core interests in the financial sector

Economic security is defined in the National Safety and Security Strategy as one of the five vital interests that have to be protected in the context of national safety and security. The strategy refers to 'the Netherlands' ability to function undisturbed as an effective and efficient economy' as a guarantee for the economic security of our country.

The welfare of the Netherlands is highly dependent on the open economy functioning well, with an efficiently working financial and economic infrastructure for customers and suppliers, consumers and producers. This facilitating infrastructure must be reliable and must meet the quality standards customers require. A second important factor when monitoring Dutch economic security relates to safeguarding information that is interesting in an economic sense, such as investment intentions or the granting of important orders. Information leaks in this regard could result in considerable economic damage.

The technical ability to transfer funds is also crucial for society to function well. Major disruptions in this area would constitute a direct threat to national safety and security and could lead to social disruption. However, disruption to transferring funds is outside the scope of this analysis and will not be dealt with further.

The core interests in the sector are dealt with point by point in the next sections. Our research revealed that these core interests are only to be found in the category of datasets and blueprints. The other categories, at least for the purposes of this analysis, are therefore not represented.

## 5.1 Datasets and blueprints

### Understanding funds transfer

Foreign intelligence services are primarily interested in the transfer of funds in order to get an idea of the activities of those individuals and groups they are investigating. These might be a migrant community, opposition groups or jihadi terrorists, or individual members of such groups. By examining the transfer of funds, intelligence services may also discover the payment patterns of the main actors in the Dutch economy. This could have adverse effects on the competitive position of Dutch business. Knowledge and an understanding of monetary transfers from and to state banks may reveal where the Government of the Netherlands is making investments.

The focus of foreign intelligence services on Dutch funds' transfers or the Dutch side of the international transfer of funds is certainly undesirable from the point of view of economic espionage, but in the context of combating terrorism, sharing this type of information is desirable. Indeed, by combining information about financial transactions with files on people under investigation, suspect transactions, such as those related to financing terrorism, may come to light. These conflicting interests make protecting the transfer of funds even more complex.

### Personal details held by banks

Apart from information on financial transactions that take place, banks also have extensive datasets about their customers. This information helps intelligence services to find out about individuals and groups they are investigating. Information about a person's financial situation and spending patterns, in combination with the name of his or her employer, are sensitive. It enables intelligence services to target people who have an interesting employer and at the same time may be susceptible to bribery or blackmail.

Certainty of energy provision

Oil and gas

Competitiveness

Sources of energy

# 6. Core interests in the energy sector

Energy and the energy sector form an important pillar of the Dutch economy. The Netherlands operates the largest natural gas field in Europe, the Rotterdam port is the number one oil hub for Western Europe and large oil producing and trading companies have branches on Dutch territory. In addition to technical knowledge of oil and gas extraction, storage, processing and transport, gathered over many years, the Netherlands also boasts knowledge of and skills in energy trading, especially as regards gas. Both the hard, technological side of the sector, knowledge about energy, and its softer side, the skills in marketing energy on the trading floor, determine the Netherlands' international competitiveness. This makes both sides interesting to foreign intelligence services.

Energy will continue to be very important for the Netherlands in a number of fields in the future. The Dutch government explicitly supports the ambition to turn the Netherlands into Europe's 'gas roundabout', thus further reinforcing the role of the Netherlands as a European energy hub. This implies that the Netherlands will increase its importance as a logistic, gas storage and transport hub for northwest Europe. This will enable the Netherlands to secure its future energy supply. Besides this, acting as a hub can greatly stimulate Dutch industry. Knowledge about a possible strategy to achieve this hub function is a potential target for intelligence activities and the same applies to the knowledge that makes it possible to get control of strategic parts of the 'gas roundabout'.

The Netherlands' ambitions in the field of energy go beyond being the 'gas roundabout'. High-level research into green energy, energy savings and $CO_2$ reduction is also conducted in the Netherlands. Such knowledge should provide the Netherlands with the means to continue to play an important role in the European energy market in the long run. Due to decreasing fossil fuel reserves and increasingly widespread concerns about the environment and the climate, knowledge about green energy generation, transport and storage processes is of great economic interest. Innovations in the energy sector related to sustainable energy sources and carriers (also known as energy efficiency) are important on the long run. The Netherlands now has major economic interests in energy, but to safeguard these interests in the future as well, the country will have to continue paying attention to the development, operation, application and marketing of existing and new sources of energy and innovative means of energy transmission and transport.

In addition to the purely economic interest of energy and energy supply, the sector also represents a politico-strategic interest. Energy supply influences international political relations. There is a great area of tension between different countries with regards to favourable pricing of the energy and raw materials to be bought and the certainty of delivery of these raw materials. Countries with considerable energy sources occupy an important position in this area of tension. The potential influence of energy-supplying countries involves risks for buying countries, including the Netherlands, as these countries could be put under pressure by threatening to supply less energy to them. Countries that have safeguarded their energy supply and that are not dependent on one supplier or just a few suppliers have more freedom to operate independently in the international arena.

## 6.1 Datasets and blueprints

Core interests within the category of datasets and blueprints often touch upon innovative technologies for oil and gas extraction and for the transport, storage and processing of fossil fuel. Technologies for utilising alternative sources of energy also belong to this category.

### Oil and gas extraction technologies

The Netherlands is in a strong position as regards knowledge of oil and gas extraction. This technical knowledge distinguishes Dutch companies from foreign competitors, enabling the Netherlands to win major oil field operation contracts. An example of this is offshore technology, a field in which the Netherlands has extensive knowledge. Due to the scope and the duration of such projects the economic impact of participating in them is significant. As knowledge of these technologies is both financially and strategically attractive to other countries, technical knowledge about oil and gas extraction is a target for the activities of intelligence services. Intelligence services of countries that are under a ban are even more interested in such technologies. If they cannot import knowledge and knowhow from the energy sector through commercial channels, for instance because they are under a trade ban, they will only be able to obtain such knowledge through espionage or other secretive ways.

Oil and gas transport, storage and processing technologies
In addition to knowledge about the technical aspects of extracting oil and gas, the Netherlands also houses plenty of knowledge about affiliated processes, such as technologies to process, transport and store oil and gas products. Another valuable asset is knowledge of natural gas liquification, and of treating and transporting Liquid Natural Gas (LNG). Such technologies may be major trump cards in the Netherlands' ambition to be an international hub for the transhipment of energy and energy products. If such knowledge falls into the

hands of foreign intelligence services, this will weaken the Netherlands' position in international competition for achieving such a major economic target.

Alternative energy generation and CO2 storage technologies
Besides knowledge about extracting conventional sources of energy, knowledge of alternative energy generation is also abundantly present in the Netherlands. The Netherlands holds a prominent position in the research into and the production of solar cell technology. Various sophisticated innovative findings, such as flexible foil with solar cells and efficient wind energy generation, originated in the Netherlands.

### Nuclear energy

Nuclear energy-related knowledge is a subject of regular analysis conducted by the Dutch intelligence and security services, specifically in the context of non-proliferation, and has not been studied in depth as part of this analysis. However, its core interest is briefly noted in this report given the high level of knowledge the Netherlands has in this area and the major economic and other interests involved. For example, a considerable part of all enriched uranium used worldwide is produced in the Netherlands, using centrifuge technologies that were developed there too. In addition, more than half of all medical isotopes used in Europe come from the Netherlands.

## 6.2 Positions and strategy

The Netherlands intends to continue to play an important role in the international energy market in the future. This is partly due to economic considerations and partly to strategic considerations that touch on safeguarding the supply of energy. To fulfil these ambitions, the Netherlands is working on long-term energy strategies, visions and policies, some of these are developed in collaboration with other countries. Important elements of these strategies, visions and policies are core interests in the category 'Positions and strategy'.

### Energy policy of the Netherlands and the EU

The knowledge that is present in the Netherlands about our country's long-term energy policy and that of European bodies such as the EU is a core interest. The vision papers, strategic documents and other information that touch on the Dutch ambition to interconnect European gas flows form a part of this. However, the Netherlands is not the only country with this ambition; other European countries have ambitions to function as European gas hubs or are at least trying to keep as much of a grip on this as possible. As a result, all knowledge about the Dutch strategy to become the 'gas roundabout' and other comparable strategic policies should be considered valuable to intelligence services.

### Strategic business information

Strategic business information belonging to major corporations in the oil and gas industry is interesting to foreign intelligence services. This includes knowledge about stock volumes, calculation and analytical models and replies to invitations to tender. The companies' financial situation and their investment and business strategies, such as information regarding the development of new oil and gas fields, are also matters that intelligence services are interested in. This is also because quite a few internationally active companies in this sector are state-owned companies or have very close ties with a national government. If this type of knowledge leaks out, it will result in a deterioration of the economic positions of the companies that are affected. This would also harm the economic position of the Netherlands, in terms of loss of employment, fewer tax revenues and lower dividends, to name a few. In addition, the certainty of energy supply for the Netherlands could be indirectly affected.

### Trading skills (market culture and structure)

Traditional actors in the Dutch energy landscape possess a combination of commercials skills and knowledge of the cultural and structural organisation of the Dutch energy market. The manner in which the Dutch market is organised and how it works is the result of a long process. Foreign actors could benefit from openly or secretly learning about the culture and structure of the Dutch market in order to be able to access it in the right manner. The skills concerned are largely cultural and commercial.

Foreign actors could - either openly or secretively – try to become acquainted with the culture and structure of the Dutch gas trade, for example by proposing forms of collaboration, entering into joint ventures or making investments in the Netherlands. This would enable foreign energy companies to take their first steps onto the Dutch energy market and some of these parties might see this as a first step in their ambition to make an important and decisive mark on the Western European energy market in due course.

## 6.3 Emerging core interests and infrastructure

The introduction of the Dutch Unbundling Act *(Wet Onafhankelijk Netbeheer)* brought about a rapid succession of events in the energy sector. As a consequence of the Unbundling Act, the production and delivery of energy were split up and independent grid management came into existence. As a result, many actors that are important for safeguarding the supply of energy in the Netherlands are now mainly influenced by developments in the free market and the Dutch government has minor influence on them. This may diminish the Dutch government's control and protection of core interests in this sector and may lead to unwanted consequences.

### Energy infrastructure, delivery and storage

Knowledge and information that guarantee the certainty of energy supply in the Netherlands form a core interest. It is important to make sure that the Netherlands continues to maintain access to energy stocks reserved by Dutch actors in the event of energy scarcity. However, it is not certain which possibilities the Netherlands has if a Dutch or foreign commercial company is no longer able to comply with its contractual commitments to all parties and decides not to honour the Dutch part of its energy supplies but instead to safeguard its energy supplies to a larger customer or to the country where it has its registered seat. By keeping not only the energy infrastructure in Dutch hands, but also elements that are crucial to controlling energy production and delivery, the Netherlands will make itself less dependent on others as regards safeguarding its energy supply. Knowledge which might enable foreign energy companies to get control of crucial components of the Dutch energy sector form a core interest since concentrating crucial elements of the 'gas roundabout' in the Netherlands brings opportunities for our country. On the other hand, it will also bring risks in the event that the ownership and, as a result, control of crucial elements of the Dutch energy sector fall into the hands of private or state-owned foreign energy companies.

However, owning and controlling an infrastructural network is only part of safeguarding energy supply; owning a network has little to do with the question of which party wants to supply energy via that network and at what price. The assumption that energy is available and that energy that has been procured will also be actually delivered only holds in a market that is functioning under normal conditions. But if energy is scarce or if there are tensions or conflicts, obtaining energy may no longer be considered self-evident. The distinct separation that exists in the Netherlands between government and market is less clear in other EU countries and outside the EU it is often even more diffuse. In a tense market, there may be increasing pressure on commercial agreements if state interests manifest themselves in the foreign energy party. For political or commercial reasons energy may not be delivered to the Netherlands as agreed, for instance because a buyer who offered a higher price has been found, or because the country that offers energy is 'squeezing' volumes as means of applying political or economic pressure. Fluctuations in the energy price will affect consumers and the industry. Higher gas or electricity prices for the Netherlands will immediately have a negative effect on our economic position as our industrial production will become more expensive.

### Knowledge regarding alternative sources of energy

The Netherlands has high-quality technological knowledge about renewable energy, alternative sources of energy and systems to lower energy consumption and to make it more efficient. The Netherlands is making huge investments in these fields. Foreign governments are also interested in this knowledge. Currently, little attention is paid in the Netherlands to preserving this potentially highly valuable knowledge. This may result in knowledge secretly leaking out to countries which, just like the Netherlands, will have to switch over to other sources of energy in due course. And the consequence of this will be that all underlying research work of a more fundamental nature and Dutch investments in its development will disappear abroad.

Government policy

Manipulation

Constitutional state

Integrity

Infiltration

# 7. Core interests in public administration

The national government plays a role in protecting the five 'vital interests' identified in the National Safety and Security Strategy. In addition, the national government forms a symbol of the Netherlands' independence as a state. As such, the national government fulfils an important role of trust in respect of Dutch citizens. Pressure is put on the integrity and reliability of the Dutch government if foreign intelligence services are able to secretly gather intelligence from the government or if they actively and secretively try to influence government policy. Dutch citizens trust that the government will protect the safety, security and rights of its citizens, without any undesired external interference. This makes the 'public administration' sector, being a part of the national government, of great importance for national security.

There are several reasons why the Dutch government is an evident target of foreign powers' espionage activities. Firstly, it possesses an enormous amount of information that may be interesting to other countries. This information varies from the government's strategic and tactical policy plans to citizens' personal data, and economic information on companies and industries. Secondly, government officials take important decisions that set the course for the role played by the Netherlands in international bodies. Members of the government and senior civil servants have access to sensitive information (positions, room to negotiate and strategy) prior to international negotiations and meetings. And finally the government is the interface to companies and institutions, funds are awarded to Dutch industries at government level (in the form of subsidies) and the government acts as a facilitator and intermediary in the field between companies and citizens. The government thus plays an influential financial/economic role, which may make it interesting for a foreign power to try and secretively steer this role in a certain direction.

As the Dutch police and the judiciary represent the Dutch constitutional state in its most concrete form, espionage and foreign involvement in this element of public administration directly touch on the integrity and independence of the constitutional state. A foreign power may have an interest in obtaining information about their former or current fellow-countrymen from the police and the judiciary. An economic motive for infiltration or manipulation is maintaining ties with the migrants' community in the Netherlands, with the underlying objective of ensuring that money continues to flow from the Netherlands to the country of origin.

Finally, the government holds a monopoly on violence and in this capacity the police and the judiciary have authorities that other organisations lack (making arrests, special means of investigation). Knowledge about investigative techniques employed by the police and the judiciary may be interesting to foreign powers as they may reduce the risk of secretive activities being discovered. If such information leaks out, it may increase the vulnerabilities of core interests in other sectors as well.

The following paragraphs deal with the individual core interests of public administration.

## 7.1 Datasets and blueprints

### Databases

The Dutch government has an enormous amount of information about Dutch citizens, companies and organisations at its disposal in centralised and decentralised databases. Several of these databases have attracted the interest of foreign intelligence services.

Some examples of interesting data files managed by the Dutch government are:

- the income and other details of private individuals, companies and organisations kept by the tax authorities;
- information from the data files of the Municipal Personal Records Databases *(GBA)*;
- details on government personnel, specifically from such departments as the Dutch Ministries of Foreign Affairs, General Affairs or Defence;
- information from police information systems such as the *Herkenningsdienst system (HKS)* and Xpol;
- information from various other information systems such as the systems of the *Sociale Verzekeringsbank (SVB* - the organization that implements national insurance schemes in the Netherlands), *Dienst Uitvoering Onderwijs (DUO* - a governmental organization, responsible for – amongst other things – the payment of study grants to students), the Immigration and Naturalisation Service *(IND)*, and Customs.

The increasing interconnection between data files of different governmental organisations has improved user-friendliness for the government and for citizens, but on the other hand it has made these files more vulnerable to their being accessed by unauthorised parties as there are now more ways into these systems. The system with the weakest protection can be used to access data that is much harder to access directly: the chain is only as strong as its weakest link.

These interconnected or individual files enable a lot of specific information to be obtained on private individuals and organisations. Although not every database listed above is actually a core interest in its own right, various files can offer valuable insights through the use of such techniques as data-mining.

Data from these databases can provide intelligence services with information on people and/or organisations they are interested in. In addition, the data in the databases provides access to other core interests as it enables people in interesting positions, and their potential vulnerabilities (such as their financial situation, family situation, criminal records), to be identified very effectively.

Furthermore, the data on citizens and organisations or companies that is filed in the various systems, is privacy-sensitive and vulnerable. This is data that cannot be indiscriminately shared publicly in the Netherlands. Citizens' trust in the national and local governments would be severely affected and national security would be threatened if such information were to be leaked to foreign powers.

### Knowledge of security systems

Research into measures to improve the resistance of ICT systems and into security systems such as cryptography and biometrics is done at several places within the government. Both this knowledge itself and knowledge of its application as part of Dutch security measures may be valuable to intelligence services as it offers opportunities for other countries to improve their own security or to circumvent the security measures that have been implemented to safeguard other Dutch core interests. This knowledge also enables intelligence services to make a better assessment of the 'risk of failure' that may be involved in carrying out intelligence operations.

## 7.2 Positions and strategy

The Netherlands' positions in international policy matters, Dutch strategies when negotiating with international partners and the long-term view of how critical sectors are organised form a set of core interests that foreign intelligence services have always been highly interested in. The presence of a large number of international organisations in the Netherlands - specifically in The Hague – also attracts foreign intelligence activities.

### Positions of the Government of the Netherlands in international matters

Knowledge of the Netherlands' positions and the strategy it wants to employ in international deliberations may be used by other countries to shape their own positions and strategy. An example of this is the position of the Government of the Netherlands as regards EU policy and strategy. Besides the negative effects of the leaking of information about these positions on the Netherlands' scope for negotiating in international bodies, the information could also be used to secretively mobilise other parties. Examples of this are the Netherlands' positions as regards the EU, safeguarding energy supply and trade interests.

### Information about the EU and NATO

The European Union (EU) with its 27 member states and nearly half a billion inhabitants is an influential partnership, both economically and otherwise, and as such it is a target of espionage by non-EU member states. The same goes for the North Atlantic Treaty Organization (NATO). Intelligence services are extremely interested in information about the internal relations within international organisations. The positions taken in individual differences of opinion between EU or NATO member states are particularly interesting to foreign actors, for example the expansion of the EU or NATO. Information on possible individual differences of opinion may be used to drive a wedge between different actors and thus weaken the organisation's international performance. This gives other actors in the international arena more room to manoeuvre. If the EU or the NATO were weakened, this would harm the international position of the Netherlands and would negatively affect Dutch interests, both economically and otherwise.

In addition, intelligence services are interested in classified information of international organisations, such as the planned strategy for a certain case. All participating countries that have access to such information have the responsibility to adequately protect it. To find ways in, intelligence services will look for weak spots among the different participating actors. Apart from the interest that is inherent in this information, the Netherlands would be politically harmed internationally if a weak spot were found to be located in the Netherlands.

The Netherlands is host to many international organisations. Being a host to these organisations also implies a responsibility to guarantee that they can operate unimpeded. As a result, counteracting such organisations being spied on is a responsibility of the Government of the Netherlands. The international position of the Netherlands would be harmed if such an organisation were to fall victim to espionage incidents.

Technical route

Weakest link

Monitoring conversations

Intelligence service

Social engineering

# 8. How does information leak out? Risks of and vulnerabilities to espionage

The core interests of several sectors that are interesting to foreign intelligence services have been identified in the previous chapters. Roughly speaking, there are two ways in which these services may try to obtain these core interests. The first is to use people to gather information. The other method uses technical means to intercept information. All factors that enable core interests to be affected by espionage are related to these two routes – people and technology.

Foreign intelligence services employ various methods to obtain access to interesting information or data via people. Every intelligence service has its own modus operandi for this, but there are some common denominators. They will be discussed in section 8.2.

The technical route is also employed by virtually all services. However, here there are major differences in the capacities of the different services. Section 8.1 examines these technical vulnerabilities. Actually, intelligence operations often employ a wide range of combined methods and means that complement, verify and reinforce each other, i.e. there are countless mixed forms of 'operating'.

Since intelligence services will continue to make use of the two access routes of 'people' and 'technology', this is where attention should be primarily focused in order to protect core interests. However, it is worth noting that developments in the intelligence world sometimes take place at high speed; a continuous race to develop new attack techniques and countermeasures is going on in both fields, making it necessary to continually evaluate vulnerabilities. Protective measures that were sufficient only yesterday may no longer provide enough protection today.

The analysis has revealed three important developments that are currently affecting the vulnerability of Dutch core interests. They are policy, outsourcing and interconnection. These developments will be discussed in more detail later in this chapter.

The way in which an intelligence service will preferably try to obtain information depends on a number of factors, such as the 'speciality' of the intelligence service in question and its willingness to take risks. However, the most important consideration will always be finding the weakest link in the security system, i.e. the greatest vulnerability of a core interest. And that weakest link - technology or people, interconnection with other systems or outsourcing - is closely associated with the core interest that a foreign power intends to steal.

## 8.1 Access route 1: technical access

The first method of gaining access to core interests is by technical means. Information is stored in documents, is available in the form of prototypes or can be retrieved from the design of a factory. The information is stored in digital format on computer systems and is the subject of communication by post, e-mail and telephone. Technological means of obtaining the information sought can be applied to all these forms of information storage and transmission.

### Interception of fixed and wireless telecommunication

The main forms of telecommunication are fixed and mobile telephony, VOIP telephony (making telephone calls 'via internet') and e-mail.

Regardless of the form of telecommunication used, the integrity of the information can no longer be guaranteed as soon as a foreign party's telecom network is used for telephone calls to or from a foreign country. This is always true for all forms of internet and e-mail usage (either wireless or corded) as it is not clear which route the information will take to travel over the internet. Information that travels through foreign 'nodes' can be intercepted by intelligence services. E-mails, documents or web conferences that are not or insufficiently encrypted can be intercepted and read. It is quite likely that several actors are structurally and automatically intercepting data traffic from the internet and analysing, storing and using it for intelligence purposes. Encrypting confidential information to adequately protect it before sending it via internet is very important, as is considering whether using such a – relatively unsafe – medium is opportune.

And finally, there are also mobile systems that make use of their own separate storage servers abroad, for instance to temporarily store e-mails on them. Such central storage systems make this type of equipment inherently vulnerable to intelligence activities by foreign services. This latter form of communication is all the more worrying because it is exactly this type of system that is used by senior management in both companies and government organisations: i.e. the people in key positions who take decisions about positions and strategy and who have knowledge of and access to information.
It cannot be ruled out that foreign intelligence services are able to intercept communication that is sent through Dutch networks since these intelligence services are perfectly able to manipulate hardware or software in such a way that they are

enabled to remotely access systems. And as they can also try to intercept wireless and corded communication locally, communication via landlines, PDAs, smartphones and DECT phones is by definition no longer safe.

**Smartphone**
The American president, Barack Obama, likes to use his smartphone, but he was initially forbidden to use it for security reasons. After months of discussion it was announced that Obama could continue to use his PDA, but that he would also be given a safe smartphone, developed by the secret service, to be used for matters of state.

Potentially interesting data flows in the Netherlands include communication to and from embassies, various ministries such as the Ministries of Defence, the Interior and Kingdom Relations, Justice, Economic Affairs and General Affairs and the data flows of the interdepartmental 'Hague Ring' communication system. Wireless and corded telecommunication from and to NATO and EU delegations in the Netherlands also require attention in this context.

### Digital attacks

In addition to intercepting information, the internet also offers countless opportunities of actively attacking computer systems. Intelligence service can obtain all kinds of information through direct attacks or by trying to reach the relevant staff via internet. An organisation can become the target of internet attacks by means of hacking, phishing,[10] or Trojan horses (Trojans). For example, Trojans are programs that are attached to messages that seem to be bona fide and that install themselves on the addressee's system when the message is opened. Once activated, they can gather information from the addressee's PC and send it unnoticed. Trojans often accompany personal e-mail to which a document that the addressee in question is personally interested in is attached. Other digital data carriers may also be infected by similar harmful files which self-activate as soon as the data carrier is inserted into a computer. Examples of such data carriers are USB sticks and CD-ROMs whose origins are not clear.

**GhostNet**
In early 2009 a NATO base in the Netherlands was found to have become the target of a substantial internet espionage network, driven by computers which could virtually all be traced back to Chinese territory. The espionage network, called GhostNet, spied on computers in more than one hundred countries. Hackers infected computers at embassies, ministries and international institutions through targeted e-mails that contained infected Word and PDF files. Information was taken from the infected computers by copying documents and by monitoring conversations via webcams and microphones.

[10] Phishing is asking for sensitive information via digital means, apparently originating from a reliable party.

### Observation, monitoring conversations and physical theft

Tapping telephone calls via the telephone switchboard is not the only method of monitoring conversations. Monitoring equipment or directional-type microphones can also be used to monitor conversations. The microphones may be concealed in walls or in furniture. And of course, information stored in the form of documents or on computer hardware can physically be stolen by breaking into an office and copying the information or taking the information carriers from the office.

**Monitoring conversations**
In 2004, monitoring equipment was found in the UN offices in Geneva in the room where videoconferences with the UN headquarters in New York are held. The equipment had probably been there for four years. Quite a lot of sophisticated monitoring equipment had already been found in the building of the European Council in Brussels the year before.

## 8.2 Access route 2: human access

People who have direct or indirect access to core interests or to information about core interests form a means of getting at the core interest. People may have sensitive knowledge in their heads, know the password that provides access to digital files or have the key to a safe. Sometimes people are the only way to gain access to information, for instance if information systems are not connected to the internet (stand-alone computers or networks).

Intelligence services employ all kinds of different methods in their attempts to obtain information via people. Some will work slowly, making sure that their activities go unnoticed, whereas other services are less reticent and go for a confrontational approach. It also depends on how urgent it is that certain information be obtained and on the position of the future source.

Before people with relevant knowledge can be approached by a foreign intelligence service, this service has to know that they exist. This knowledge can be obtained in various ways, such as trying to spot the right people at tradeshows, symposiums, conferences and certain -mainly migrant- associations. Internet is also becoming increasingly important in this respect. Network sites like LinkedIn and Facebook are important sources of information for foreign intelligence services that are looking for potential agents and informants in Dutch companies or government organisations.

An important factor is whether the person in question is aware of the fact that they have interesting information at their disposal. Someone who is not aware of this will be less likely to realise that foreign services might be interested in them. People who are aware of the fact that they are carrying secrets will probably be more cautious.

## Awareness of value

This analysis has shown that often employees and management in relevant organisations do not realise that they have core interests at their disposal and that their company, job or knowledge is attracting attention from foreign intelligence services. People may disclose important information unaware that the information they have is interesting to a foreign intelligence service. Members of staff who are responsible for an organisation's security often have an acute awareness of the various risks and the potential vulnerabilities. However, until all members of the organisation have obtained a certain degree of awareness, many of these potential vulnerabilities will continue to exist.

There are significant differences in the awareness of information value of managers and their staff and this can vary within one and the same sector and between sectors. Staff members that are most aware are not necessarily those that have the most direct access to core interests. Whether staff are aware of the value of the information they work with largely depends on a company's culture. It is self-explanatory that a member of staff who does not know that the information he or she works with is espionage-sensitive information will not automatically treat it as confidential information. On the other hand, lower ranking staff may have a stronger awareness of the value of the information than management, specifically because they have more understanding of the information. In these situations, these staff members will want to handle the information with more care than prescribed or enforced by the organisation's policy.

It is not until awareness of the value of information is embedded in the entire organisation - both top-down and bottom-up - that a company culture can emerge in which knowledge that must be protected is actually treated as such by all layers of an organisation.

## Unfamiliar with espionage

As has been identified above, many people are insufficiently aware of the value of the information they have at their disposal. Another point is that people overestimate the safety of technical applications (e.g. PDAs) they use in their daily work, increasing the vulnerability of core interest. Examples of such behaviour is exchanging sensitive information by phone or e-mail. People will let ease of use prevail over securityconcerns, and will for example immediately insert a USB stick that was presented to them at a conference into the office computer.

Many people are unaware of the ways in which intelligence services use people to obtain sensitive information. People do not seem to see why it should be necessary to exercise any restraint when discussing the details of research results with a fellow researcher who has been attending the same symposiums for many years. Only a few people will wonder whether a friendly foreign colleague who is always interested might be an intelligence officer. But people may also be lured into giving away information unawares via phishing or during a conversation in a bar, after a meeting.

**Espionage via e-mail**

Some government officials subscribe to news services of the European Union. When they receive an e-mail with an attachment that seems to come from the news service, they will open it without any hesitation. However, there was a recent case in which just such an e-mail was found to have come from a third party and to contain a Trojan horse. Apparently the sender knew the subscribers' e-mail addresses and used them when sending the Trojan horse.

## Methods used by intelligence service

*Grooming (social engineering)*

Obtaining information from people usually starts by slowly gaining their trust, often in the form of an individual friendship, where the intelligence officer pays compliments and gives presents and, as a matter of course, something will eventually have to be done in return. The intelligence officer's actions consist of a number of logical steps in a carefully phased plan of interaction.

*Blackmail*

Blackmail is one of the most brutal and least frequently-used ways of obtaining information. An example of a traditional method is where a person who holds an interesting post is put into a position that makes them susceptible to blackmail, for example by luring them into amorous escapades. Once the person in question has committed acts that enable them to be blackmailed, they are asked to collaborate with the foreign intelligence service.

Actually both men and women have to be cautious of the charms of foreign intelligence officers and their agents. Anyone can become the target of such attempts at amorous social engineering.

**Dating spies**

During an official visit abroad, a British senior official spent the night with a local lady only to discover afterwards that his BlackBerry was missing. Although the device itself probably did not contain any secret information, it could be used to break into the server of the Prime Minister's official residence.

Just like social engineering, blackmail sometimes starts in a seemingly innocent way, with very little information or minor, seemingly insignificant details being asked initially. Once a relation of trust has been built after a period of 'nurturing', information will be asked for that is not really secret, but is just beyond the bounds of being innocent. And when this threshold

has been crossed, the person in question may think that there is no way back: he or she has slowly and deliberately been lured into a position where they can be blackmailed. Since (internal) rules have been broken, the person will be hestitant to report what has happened to the company's security department. By carefully building a situation in which things become increasingly more difficult for the target, intelligence officers eventually manage to get their victims into a position where they can be bluntly asked to reveal secret information.

*Deliberate leaks*
Of course, staff members may also deliberately disclose information. Various motives can play a role, such as money, personal benefit, recognition/ego, personal conviction, feelings of dissatisfaction or revenge. Intelligence officers will deliberately take advantage of such sentiments especially if background information is available on a certain person.

**Human access to files**
In 2008, the AIVD found that the Moroccan intelligence service was using police officers to gain access to closed data files. When the AIVD reported this, some Moroccan diplomats who were stationed in the Netherlands were recalled to Morocco in response. The police officers involved were also relieved of their duties and criminal investigations were started. This case sparked off initiatives to increase awareness of the risks of espionage within the Dutch police sector.

## 8.3 People as the focal point

The sections above describe how the factors 'technology' and 'people' influence the accessibility and vulnerability of core interests, regardless of the sector in which they are found. Since many technical devices like laptops, home workstations and PDAs are often insufficiently protected against the activities of intelligence services, the behaviour of human users is also crucial for safeguarding core interests. Employees must realise that they should not exchange any sensitive information using unsafe systems. However, human behaviour is not only determined by our awareness of the value of the information at our disposal. User-friendliness, speed and convenience also influence the extent to which people comply with agreements made with the intention safeguarding a core interest.

Implementing certain safety measures and actually complying with these measures are decisive factors for the success of any safety policy. This analysis has brought several developments to the fore that may increase the vulnerability of a core interest if organisations are not aware of the risks associated with these developments.

## 8.4 Development 1: policy

The first important factor is safety-related policy as well as its topicality and completeness. Policy may focus on protecting government information or be a company's clean desk policy. Choices in lots of policy areas that are not directly related to security many also influence the opportunities that are open to intelligence services, such as the outsourcing of maintenance on ICT systems.

The consequences may be economic loss, but the physical or even the territorial integrity of the Dutch state may also be affected. Such activities utilise the vulnerabilities in Dutch policy. Although Dutch interests could be harmed, attention is currently not always being paid to possible safety implications when formulating policy. Many current policies are not set up in a way that prevents national security being jeopardised and some policies even encourage the endangering of national security. Relevant examples include policy in respect of the education of foreign students and the liberalisation and privatisation of companies in some critical infrastructures.

### Prioritising security

Given the powers of intelligence services to find and exploit weak spots in security systems, an organisation-wide security policy that is maintained on a structural basis and that is generally supported is the only way to adequately protect core interests. In order to achieve these necessary measures, internal security must be on the agenda at a sufficiently senior managerial or administrative level. The priority given to security, including data security, greatly differs from one organisation to the next. An example of this is the position of the department responsible for security in an organisation. All too often security appears to be a residual item in the budget which has only a limited possibility of addressing points of attention at a sufficiently senior managerial level. The wider consequence of this may be that there are not only insufficient means for security in the organisation, but that there is insufficient support as well.

Deliberate attention from the more senior managerial layers is important, both from the point of view of the company-wide measures to be taken and as regards to the image of security in the organisation. A department with responsibility for security in an organisation must have sufficient impact and the right authorisations. Another option is to formulate policy where certain processes or workflows must always be approved by this department. Only if the importance of security awareness is explicitly demonstrated by senior management will this awareness penetrate throughout the organisation and increase.

### Education and research

The scientific world is vulnerable in a special way. On the one hand, the free exchange of research results and information forms the basis of science, but on the other hand scientific research often precedes knowledge of economic and/or

strategic value. It is not always easy to determine the point at which knowledge changes from being open scientific information to becoming valuable or even secret information. The dividing line between normal information and knowledge exchange for the sake of science on the one hand, and secretive information gathering for the economic or strategic benefits of another country on the other cannot always be decided unequivocally and/or easily.

It is the inherent openness of science that makes scientific espionage relatively simple. The open culture of universities and the presence of numerous foreign students and researchers makes it relatively easy for intelligence services to gather relevant information. Sensitive information has been found to be poorly protected and faculties are easily accessible. There is a culture of leaving office doors and cabinets open, and computer networks are relatively easily accessible.

In addition, the universities form a way in to further activities. It is relatively easy for foreign students to get traineeships at companies via the universities and these are often with companies that have core interests at their disposal, such as traineeships in R&D departments for students at technical universities.

Another important contribution that knowledge institutions make is that they not only produce knowledge, but knowledge workers as well. For example, about one million Chinese engineers graduate every year from Chinese institutions, but also from top universities in the Netherlands and in other countries. Science has a tradition of free exchange of knowledge and people, and a country like China is happy to make use of this, given the fact that China is trying to improve its international competitive position within the shortest time possible. In this respect, the Netherlands is an interesting place for students from China and other countries. The majority of these students return to their country of origin after graduation and take the knowledge and insights that they have gathered here with them.

The current Dutch education policy explicitly stimulates knowledge migration and attracting foreign students. This is understandable, since foreign students in the Netherlands make a contribution to the Dutch knowledge potential and eventually even to the economic development of the Netherlands. And it is a fact that not all migration of scientific knowledge is undesirable: for example migration of knowledge that does not harm the economic welfare is stimulated in the context of development cooperation. However, a disadvantage is that Master and PhD students may have ulterior motives and may, for the sake of their countries of origin, try to learn more about research techniques, applications and scientific insights that are developed at Dutch universities and are largely financed by the Dutch government. Innovative knowledge that should benefit the economic welfare of the Netherlands can thus be transferred to competitors.

Privatisation and liberalisation of the strategic infrastructure
It is of great importance that economic borders are opened up in Europe and that market actors are given honest competition opportunities in the European market. Part of that honest competition, in Europe and elsewhere, involves diminishing the role of the state in the market. However, where certain important elements of the critical infrastructure are concerned it is questionable whether privatisation and liberalisation of the industry are desirable, as this may have harmful consequences for Dutch national security. Private companies may be taken over by non-Dutch or non-European companies. The infrastructure will then be controlled by an actor that has no connection with the Netherlands, whereas choices about how to maintain or use the infrastructure may be of significant influence for the functioning of Dutch society. And at the same time, particularly if the infrastructure becomes the property of a non-European party, the influence that the Dutch government has on such choices will decrease.

An example of this is bandwidths, radio masts or other parts of the telecommunications network falling into foreign hands. This would give these parties more access to information about the network itself, and about the data sent via the network. Other examples can be found in the energy and transport sectors (airports, sea ports). The Netherlands has one of the most liberalised energy sectors in Europe. Other countries think more strategically in this respect and take their own national security into account more.

By tradition, the Netherlands is an open trading nation that tries to minimize protectionism as much as possible. This has brought great prosperity. However the disadvantage of this is that, compared to other countries, the Netherlands formulates little policy to protect strategic industries and strategic knowledge now and in the future.[11] Other countries do have this awareness to a varying extent. For example, some countries have a system where foreign investors are first assessed before they can take a participating share in a company. The Netherlands has also partly or completely privatised strategic knowledge organisations. Other countries still have such public research institutions.

### Dual use

An additional point of attention is the fact that lots of technologies are developed here in the Netherlands aimed at the user, i.e. the consumer, whereas the same technology can be 'misused' for strategic and military objectives (e.g. self healing materials, coatings or medical developments like

[11] A foreign research report ('Laws and Policies Regulating Foreign Investment in 10 Countries', GAO, February 2008) mentions the Netherlands as one of the few countries that has no policy framework to assure that strategic economic knowledge and companies are preserved for the Netherlands.

scans). These applications of technologies with consumer objectives are protected less well than technologies for strategic and military objectives. The Netherlands is not usually very aware of this possible 'misuse' of the technology. In some other countries, these 'dual-use' technologies are screened off from the outside world for reasons of national security due to their possible military applications.

## 8.5 Development 2: outsourcing and offshoring

The second development that deserves attention is the growth of mainly large-scale purchasing of technical equipment from abroad, outsourcing to third parties and offshoring (outsourcing to foreign countries) of activities in various fields (ICT maintenance as well as data storage and data entry, staff records or invoicing). If an external party can get such close access to an organisation's information, especially if the external party is located in a foreign country where other forms of assurance (legislation and regulations) apply, it is hard to keep the protection of the information sufficiently under control.

### Hardware & software

Companies and institutions make use of extensive hardware and software that has been developed abroad and/or that is maintained from abroad. Computers and other equipment are often bought from a foreign country, because a foreign company has been awarded the tender. In addition, keeping complex hardware and software running is frequently left to the specialists of the company that has designed it or to a specialised third party. Due to the specialist knowledge that is required to produce and maintain these products, it is difficult for organisation to keep a close eye on what is exactly happening in and on its own systems, and on who has access to specific information. Foreign maintenance companies may have close ties with their governments and intelligence services. Agreements may have been made about supplying information. Core interests could fall into the hands of another country in this way.

When buying foreign hardware and software, security risks have to be taken into account. It is easy to imagine that intelligence services will have companies from their own country build backdoors into their products enabling the intelligence services get access without being noticed.

### Servers

The same considerations that apply to software which is managed from a foreign country also apply to back-up and other servers located abroad. If actors in the Netherlands are aware that their own confidential data is stored abroad, they often are unable to see who has access to the data on such servers.
It is difficult to determine whether data is being compromised where espionage via servers is concerned. Stealing information from a server does not require 'disguised' data traffic from the network to be sent abroad, as is often the case with software installed secretively. Intelligence services will probably be able to copy the entire contents of a computer server in their national territory unnoticed, especially if it is located in a local data centre. This will be more complicated for computer servers located at the regional head office of a multinational corporation.
The increasing number of internet services with only memory capacity is a development that may have additional consequences, as online memory capacity is eventually also physically located on servers that are in a country's territory. This applies to automatic back-up/synchronisation programs for PCs, laptops, telephones and PDAs, as well as online e-mail programs (that may be free) and applications that enable several people to simultaneously work on documents online. Developments like cloud computing (the mass processing of data via internet, instead of physically on one's own computer) make paying attention to the potential vulnerability of this kind of application all the more important.

### Support services

Such tasks as invoicing customers, keeping personnel records, translating texts, converting documents into digital (searchable) texts or data entry in databases are all forms of activities that can be and are outsourced by organisations to a great extent. These organisations are often unaware of the fact that this gives the service providers access to the information of the organisation. And furthermore it is relatively easy to commit espionage via such service providers, where security is often less strict than at the supplying company. Again, if the company in question is located abroad, the owner of the information has limited possibilities to control access to the information.

Another aspect that requires attention is the chain effect that may occur. Not only is the party to whom that work is outsourced important, but also the fact that this company may outsource the work or part of it to subcontractors (including external actors). This creates a chain of companies that all obtain some form of access to the information. Clear agreements must be made in order to be able to protect

information effectively, and all companies in the chain must be known and must have been found to be reliable. This requires not only knowledge of the direct party to which work is outsourced, but also of its support organisations.

### The role of intelligence services

In all the above examples of outsourcing, the difference between the activities of intelligence services and the threats of industrial espionage should be considered. Although the objective in both cases is to obtain sensitive information, an intelligence service is the spying party in the event of economic espionage. This means that it is likely that a wide range of means of obtaining intelligence will be employed. Even renowned companies, which have a good reputation as regards their protection against industrial espionage, cannot always or do not always want to offer protection against the activities of an intelligence service, for example because the company in question has been established by an intelligence service with the very objective of obtaining information in this way. Furthermore, a state may put pressure on a company located within its borders to cooperate with its intelligence service. Threats to refuse permits, charges for breaching national security or withholding lucrative government orders are instruments that companies can be extremely sensitive to. And finally, the government in question may be the owner of or at least have unrestricted access to all infrastructures around a company premises located on its national territory. Mail, digital data flows and telephony can then be intercepted without the company in question knowing. This is also a relatively easy way to compromise information. The bottom line is that there is a good chance that it is difficult for companies physically located abroad, no matter how reliable they tend to be, to refuse an 'invitation' to cooperate with their national intelligence service.

## 8.6 Development 3: interconnection of networks

Another factor that greatly influences vulnerability is the fact that, due to internet and ICT developments, more and more networks, systems and files are connected to each other and to the internet. This offers major practical benefits for daily operations, but it also creates an ever larger network of possible 'access points' for foreign intelligence services. A related vulnerability is the continued development of data mining.[12] The possibility of gathering various data files and combining them into one sensitive total file places additional requirements on information protection.

### Interconnection of networks

The current digital era has brought forth an additional complication as regards protecting information. Since more and more systems and files are connected, the weakest link principle applies ever more explicitly. An interconnected series of networks or systems makes it possible to hack into the systems from the inside, from system to system. The most poorly secured link in the chain of interconnected systems is then a logical way in to the total set of networks. As the number of offshoots grows, it becomes less and less transparent which files are directly or indirectly interconnected, and the risk of a weak point in the chain grows.

### Data mining

The increasing connection of ever more information to the internet makes the Netherlands more vulnerable to data mining, particularly given the increasing technical possibilities of fully computerized data mining. And information is becoming available via more and more commercial parties (marketing agencies, insurance companies, credit rating agencies). Data mining can be used to obtain strategic information from various databases that are filled with relatively useless fragments of information. The assumption that the whole of information is larger that the sum of its parts explicitly applies to data mining. This makes limited or anonymous files with information more likely targets of espionage.

[12] Data mining is extracting structured information from a larger whole of non-connected information.

Resistance

Protected to a limited degree

Security awareness

Vulnerable

# 9. Conclusions

Espionage by foreign intelligence services harms the Netherlands. The exact extent of the damage cannot be established on the basis of this analysis. However, this analysis is an attempt to provide a better understanding of the core interests and vulnerabilities within the areas of interest of economic welfare and technological and scientific potential, public administration and critical infrastructure. The notion of a 'core interest' has been defined as information, which, should such knowledge become known, could adversely affect national safety and security and which can be assumed to be of interest to foreign intelligence services and governments.

The previous sections report on the core interests that have been identified within the sectors and sketch the vulnerabilities surrounding these core interests. A number of conclusions can be drawn from this. This chapter summarizes the main conclusions and deals with some resulting policy recommendations.

## 9.1 Awareness as the overarching issue

The main conclusion that can be drawn from this analysis is that there is often little awareness as regards to espionage in the sectors concerned. This limited awareness is visible on three levels. An organisation's resistance to espionage is determined by the organisation being aware that it has one or more core interest(s) at its disposal and that other parties might be interested in those core interests. This awareness is visible on three levels.

- *Awareness of the value of information:* organisations and individual employees sometimes fail to realise or insufficiently realise the value of the information they possess or to which they can obtain access;
- *Awareness of security:* the security and safety of core interests do not always command sufficient attention within organisations, and other considerations often take priority;
- *Weighing up interests:* short-term organisational interests and/or government interests are often given precedence over long-term interests. The defection of strategic knowledge or activity relevant for long-term Dutch national safety and security to other countries is given insufficient attention.

## 9.2 Core interests and vulnerabilities

Core interests exist in all sectors. The analysis reveals that core interests can be found in all sectors investigated. They can broadly be classified into the following categories:

- Datasets & blueprints: databases, designs and drawings in organisations;
- Positions & strategy: for example, policy premises, long-term philosophy and negotiating strategies;
- Emerging core interests & infrastructure: e.g. scientific innovations that may become profitable in concrete applications in the future.

### The main factors that determine a core interest's vulnerability to espionage are the factors ‘technology’ and ‘people’.

Intelligence services try to obtain information by using technical means such as hacking, wire tapping or monitoring conversations or via people who have direct or indirect access to the information in question. Not all vulnerabilities in these two areas are recognised by the organisations that cooperated in this analysis. If a core interest is not recognised as such, no attention will be paid to its vulnerability to espionage. The analysis enables a number of specific conclusions to be drawn as regards to the vulnerabilities that have been observed. To illustrate this some of these conclusions are presented below, but it should be noted that this is not an exhaustive summary.

*Vulnerability: lack of familiarity with the value of information*

The analysis shows that institutions and companies are not always aware that they have information or knowledge at their disposal that may be valuable to intelligence services. This is mainly because their focus is on achieving high-quality results and not on protecting information against unsuspected threats. There is little knowledge about espionage. Espionage is seen as a relic of the Cold War. If any thought is paid to the risk of espionage, the general feeling is that espionage only threatens national security if it leads to serious disruption of parts of the critical infrastructure (e.g. energy supply or the transfer of funds) or if it is aimed at military applications. Most respondents know little about the extent of espionage in the Netherlands, how it works in practice and which information is interesting to foreign intelligence services. People are not always aware of the potential consequences of espionage for their own organisation and the national security of the Netherlands. The absence of a realistic image of what espionage entails, how it reveals itself and what it means to the Netherlands, makes the Netherlands as a whole vulnerable.

*Vulnerability: core interests are only protected to a limited degree*

The vulnerability of a core interest is partly determined by the degree of protection of a core interest: how well protected is the core interest? Some core interests mentioned in this report are not or insufficiently protected. Core interests that are insufficiently recognised as a core interest by the sector itself are particularly vulnerable. Core interests that are also directly

susceptible to industrial espionage or that are otherwise attractive to criminals are usually protected better than other core interests. However, this does not mean that they are protected sufficiently well to prevent espionage by intelligence services.

*Vulnerability: employees' ignorance*

Ignorance on the part of individual employees about the targets and methods of intelligence services makes organisations as a whole vulnerable to espionage. Individual employees may unknowingly disclose valuable information, but staff may also be blackmailed or manipulated, causing such information to fall in the wrong hands. Staff who are not aware of the risks that exist are more vulnerable to such practices than those who are aware.

*Vulnerability: interception of telecommunications*

One of the main technical vulnerabilities is the possibility of data being intercepted. This applies to wireless and corded telephony and internet. Large-scale use is made of highly unsafe communication systems even though several countries have been found to be carrying out intelligence activities in the field of telecommunications. That is why this analysis not only looked at telecommunications as a vital sector, but also as a vulnerability, due to its inherent value to espionage. By gaining access to the telecommunications sector, intelligence services can obtain access to virtually all other core interests. Vulnerability of the telecommunications sector increases the vulnerability of all core interests, at least to the extent that information is stored on systems connected to telecommunications networks or is transmitted via telecommunications networks.

*Vulnerability: interconnection of computer systems*

The interconnectivity of computer systems and the linking of data storage systems make data in these systems vulnerable; connections to systems that are protected less or not at all create access possibilities via the most poorly protected link in the system. This specifically applies to connected systems involving several actors; the weakest link can be the way in to all connected systems, networks and databases. If this weakest link is located out of sight of the owner of a core interest, the core interest's vulnerability is greater than the owner would suspect on the basis of the security in force for their own system.

The wide availability of fragments of information also increases the vulnerability of a core interest. This often also concerns non-confidential information that can be obtained via commercial actors, governments or sites, including network sites, on the internet. Enriched datasets are created by connecting these individual datasets and analysing them by means of computers. The information that can be derived from these enriched datasets is much more than the sum of their parts and may substantially increase the vulnerability of a core interest.

*Vulnerability: outsourcing*

Outsourcing and offshoring activities such as system and server management, data warehousing and data processing carry the risk of espionage. Outsourcing obscures the view of which external actors have access to the systems and data. The same applies to the hiring of external personnel if the safety requirements placed on these people differ from those placed on the company's own staff. In addition, attention must be paid to the chain effect that may occur when activities are outsourced. Not only is the organisation to which the work is directly outsourced important, but its suppliers or supporting parties as well. If, for example, the primary party which an organisation entrusts with its personnel files is reliable but the party that does their ICT maintenance is not, data can still be compromised.

*Vulnerability: policy*

Targeted policy in both the private and public sector can serve to strengthen resistance to espionage and make Dutch core interests more secure. The quality of policy and policy implementation significantly influences the vulnerability of core interests to intelligence activities. Government policy drawn up with non-safety-related interests in mind may also influence the vulnerability of core interests. Privatisation, liberalisation and anti-protectionist policies promote a free and open market economy providing a stimulus to prosperity in the Netherlands. However, free market economy forces can also lead to strategic parts of the Dutch economy being taken over by foreign private or state-owned companies. If companies that work with sophisticated technological applications, that were the result of fundamental research funded by Dutch public means, are bought by foreign parties, the applied knowledge and its corresponding economic value will flow to the foreign country. If this involves parts of the critical infrastructure, national security may be compromised. The possibility of espionage activities must therefore be taken into consideration during such processes, both from the perspective outlined above and against the background of the economic impact. Vulnerability to espionage is greater after a foreign takeover, since the parts of the Dutch economy that have been taken over are then out of sight for the Dutch government and beyond its control.

Weighing up interests

Awareness of value

Education

Changing the culture

# 10. Recommendations

The research results lead to three general recommendations aiming to better protect the Dutch core interests. These general recommendations are accompanied by some non-exhaustive examples to illustrate how the recommendations can be put into practice. The authors have deliberately chosen to provide only a few examples and suggestions to prevent them from taking on the role of policy makers. Taking the recommendations a step further by translating them into actions and allocating them to action owners is explicitly left to the departments, institutions and companies concerned. The recommendations listed below can be used as guidelines for drawing up policies, for example when developing further policy in the context of the National Safety and Security Strategy. In addition, this report enables the responsible professionals in companies and government bodies to better identify and protect their own core interests and vulnerabilities. The three themes identified in the conclusions contain opportunities to further reinforce resistance to espionage. Although the analysis is confined to state espionage in the areas of economic welfare and technological and scientific potential, public administration and critical infrastructure, the recommendations can be applied more widely, within other sectors. In addition, improved protection to state espionage might reduce vulnerability to industrial espionage.

## 10.1 Awareness of value

Our research shows that organisations and individual workers sometimes fail to realise or insufficiently realise the value of the information they possess or to which they can obtain access. This can lead to the unaware leaking of core interests, insufficient security measures to protect core interests or insufficient importance being attached to security measures that have been put in place. The leaking of core interests may, but does not necessarily have to, harm the organisation. The leaking of core interests may also affect national security.

Based on the findings of our research, the following recommendation is therefore made: **Actively increase awareness (among managers and workers) of governments, companies and institutions as regards the value of the information they have at their disposal and as regards the fact that foreign governments may be interested in this information.**

Governments, companies and institutions have their own responsibility for the awareness of information as a core interest. Based on the outcome of the analysis, some concrete suggestions can be made as to how the awareness of value of organisations and the individual employees can be improved:

- Give sector-specific awareness presentations, both at management and employee levels, where the core interests and vulnerabilities that apply to the sector in question are specifically addressed.
- Give instruction or arrange for instruction to be given to high-risk organisations about how foreign intelligence services recruit and cultivate human sources. The objective of this instruction is to make sure that the people involved in these organisations learn to better recognise when they are dealing with foreign intelligence officers.
- Make transparent how the Netherlands and Dutch companies are or can be harmed as a result of espionage by foreign intelligence services. This could be done by means of a scenario that forms part of the national risk assessment (part of the National Safety and Security Strategy).
- Start by strengthening the awareness of value among managers at senior levels in the organisation to make sure that this awareness becomes a part of policy.
- Draw up a checklist that enables companies and institutions to verify whether any technologies they develop for scientific or consumer purposes might also be valuable to foreign intelligence services, including in connection with their application to other areas (like dual-use applications). If necessary, adjust regulations accordingly.
- Identify the technical/scientific studies and research areas in the Netherlands with a high risk of espionage. This report makes an initial attempt at this. Next, start awareness projects for these studies.
- Make agreements between the government and companies and institutions about when and how to alert other government institutions, companies and institutions to increased interest from a foreign intelligence service.
- Create a visible and recognisable registration centre that governments, companies and institutions can turn to with any questions about and suspicions of espionage by foreign intelligence services.

## 10.2 Awareness of safety and security

The analysis has shown that security is not always a consideration when deciding on a software system, outsourcing physical security or hiring external staff. The pre-conditions for safeguarding core interests do not always get sufficient attention within organisations. Limited attention to safety and

security can lead to a lack of understanding on the part of individual employees who will not accept that they have to visibly wear their badges at all times or that they cannot just bring people from outside the organisation into the office. When choosing between security or user-friendliness, the latter is often given priority. In combination with a limited awareness of value this may even result in people deliberately evading security measures because they are not as user-friendly as they would like them to be.

In addition, users have much, maybe too much, trust in the level of safety offered by the technologies and ICT applications they use. This is often expressed by people's behaviour, such as in how they use ICT (opening e-mail attachments or downloading files from internet). Other examples are when people take a laptop on a trip, conduct phone calls in public areas and use smartphones and PDAs when working on sensitive information.

This leads to the following recommendation:
**Try to achieve a change in culture as regards to security. Important points of attention in this respect are users, the organisation of data flows and databases and the technologies used to detect incidents.**

To further improve security awareness the following actions can be taken:

- Perform periodic security audits and system penetration tests within government organisations, companies and institutions, paying explicit attention to the risks of espionage.

- Ensure or even increase the compartmentalisation of sensitive information in high-risk organisations.

- Make agreements with ICT service providers that data systems (servers) which contain sensitive, confidential or secret information must be physically located in the Netherlands and must have been fitted with the proper security facilities.

- Strengthen the position of departments, government staff and company employees who are responsible for security. Make sure that before business decisions are taken, advice is always sought from a security expert within the organisation. This will prevent omissions from occurring in the security policy which cost more to repair at a later stage or may even never become visible.

- The position of the department responsible for security can be strengthened by having the task included in the responsibilities of a senior manager or a member of the Executive Board.

- Increase knowledge of the vulnerabilities of ICT applications and technologies. Make it clear where specific vulnerabilities occur and how they can be recognised and prevented.

- Draw up a transparent framework of considerations for governments, companies and institutions as regards the transmission of sensitive information. This framework can be used to choose how (encrypted or not encrypted) certain information (core interests or other information) can best be transmitted and by which means (internet, telephone or otherwise).

- Only grant subsidies and budgets to research institutions with a higher risk profile on the condition that these institutions provide information about the security measures that will be taken and the activities that will be performed to improve the awareness of value in advance. Perform a risk analysis of the risk of espionage by foreign intelligence services. Such a risk analysis helps to identify the core interests surrounding the research and the corresponding risks. A similar 'espionage risk analysis' could be required as a precondition for the granting of innovation subsidies by SenterNovem and other subsidy providers with respect to innovations.

- Strengthen the position of supervisory bodies, such as the Agentschap Telecom (Telecommunications Agency) for the telecommunications sector, in order to identify and limit the risks of espionage in the sectors mentioned.

- Have the registration centre mentioned above give advice to governments, industry and institutions about the way in which they can protect themselves against espionage by foreign intelligence services.

- The government should set the right example:
  - Ensure adequate compliance with the policy frameworks that are in force, such as the regulations on information security for the Dutch central government: *Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR) and Voorschrift Informatiebeveiliging Rijksdienst bijzondere informatie* (VIR-BI) from 2004.
  - Promote the usage by government bodies of high-quality security products that are suitable for their intended purpose. Security products evaluated by the *AIVD/NBV* and approved by the Minister of the Interior could be used to protect classified information. Assessment systems for ICT devices are also available for non-classified information; an example of such systems is the internationally accepted 'Common Criteria'.
  - Users at a political level and senior civil servants should refrain from using PDAs with only producer-integrated security systems to send e-mail of a sensitive to secret nature. These devices are still used on a large scale, even for sending sensitive and confidential information.

Obligatory logging of systems that contain sensitive, confidential or secret information. This is not yet the case everywhere.

## 10.3 Weighing up interests

*Short-term versus long-term or longer-term interests:*
The research has shown that short-term organisational interests and/or government interests are often given precedence over long-term interests. Sometimes, if the sale of a company or a part of a company generates money in the short term, little attention is paid to the fact that giving up control of this company or the relevant part may constitute a security problem in the future. Three examples:

### Market operation versus national interests

At the moment, selling Dutch companies to foreign companies meets with little resistance and few restrictions. This is in keeping with the Dutch liberalisation and anti-protectionist policy. Having such companies transferred to foreign owners may harm the national security of the Netherlands in due course. Liberalisation of the energy market has resulted in some energy suppliers becoming part of large foreign organisations. It is questionable whether the certainty of energy supply in the Netherlands was a main priority for the companies concerned when weighing up their interests. Other Western countries also understand these risks and have set up national review frameworks that are used to approve or refuse takeovers by foreign companies.

### Sharing knowledge versus protecting knowledge

At present, many foreign students are recruited to do research in the context of technical/scientific studies where Dutch core interests can be found whose leaking would harm the economic welfare of the Netherlands. After their studies the majority of these students return to their country of origin and take the knowledge and skills they have gathered in the Netherlands with them. Strategic and economic knowledge which should contribute to the economic potential of the future Dutch knowledge economy is thus able drain to foreign competitors. The resulting economic damage may affect national security.

### Giving up control versus keeping control

Many companies and institutions decide to outsource or offshore such activities as systems and server management, data warehousing and data processing. This entails espionage risks. Outsourcing obscures the information on the access level of external actors to systems and data that are being outsourced. The possible short-term cost saving is hardly ever set against the possible economic and other damages which the company or institution faces if data becomes accessible to espionage activities.

The following recommendation is made on the basis of these considerations:
**When drawing up policy, pay explicit attention to the protection of core interests and the effects that policy has on the interests of the Netherlands in the long run.**

To find a better balance when weighing up short and long-term interests, the following actions can be taken:
- Expand analyses of the benefits to Dutch economic welfare of sharing technical/scientific knowledge with analyses of the costs resulting from this knowledge being leaked.
- When considering whether to outsource or offshore activities pay explicit attention to the risks of espionage and its economic and/or financial consequences.