National knowledge security guidelines

Secure international collaboration

National knowledge security guidelines

Secure international collaboration

January 2022

Universiteiten van Nederland

KNAW

Vereniging Hogescholen

NFU

TO2 federatie

Rijksoverheid

NWO

Contents

Executive summary

- Knowledge security is first and foremost about the **undesirable transfer of sensitive knowledge and technology.** Transfer is undesirable if it compromises our country's national security. Knowledge security also entails the **covert influencing** of education and research by state actors. Such interference places academic freedom and social safety in jeopardy. Finally, it involves **ethical issues** that can be at play in collaboration with countries that do not respect fundamental rights.
- World-class higher education and science cannot exist without international cooperation and scientific talent from all over the world. These National Knowledge Security Guidelines can help to ensure that **international collaboration** can take place ***safely***.
- **Proportionality** is essential in the adoption of any measures. The basic principle is always 'open where possible, protected where necessary'.
- The approach to knowledge security is built around **self-regulation** by the knowledge sector. Organisations such as the Netherlands Association of Universities of Applied Sciences (VH), Universities of the Netherlands (UNL), the Royal Netherlands Academy of Arts and Sciences (KNAW), the Dutch Research Council (NWO), the Netherlands Federation of University Medical Centres (NFU) and the federation of applied research organisations (the TO2 Federation) serve as initiators and facilitators.
- The protection of national security is one of the core duties of the government. For this reason, the Dutch **central government plays an active role** in knowledge security by providing knowledge institutions with information and scope for action, in addition to setting frameworks as needed. For example, beginning in 2022, knowledge institutions will be able to contact the National Contact Point for Knowledge Security for expertise and advice.

Core academic values as the basic principle

- Core academic values, like **academic freedom** and **research integrity** constitute the foundation of higher education and science in the Netherlands.
- These values also play a decisive role in activities **with foreign partners**. They provide guidance for entering foreign collaborations. Like their Dutch colleagues, foreign **researchers and lecturers (including visitors)** are required to subscribe to and abide by the code of conduct.
- **Open science** is the standard within Europe, with the goal of making the results of publicly funded research accessible to all. In some cases, however, there may be legitimate reasons for refraining from such disclosure, such as the protection of **national security**. It is important to make good agreements in advance in order to avoid tension between striving for maximum openness and taking legitimate protective measures.
- **Ethical dilemmas** can play a role in the case of collaboration with countries that do not respect fundamental rights. One important issue concerns the prevention of the use of research results for the purpose of repression or violation of human rights in those countries. It is advisable to have an **ethics committee** within the institution to advise on ethical use of research results.
- Knowledge institutions have a duty of care towards employees and students when it comes to their **social safety**. In the case of students and researchers from countries in which fundamental rights are not respected, security can be seriously compromised by the actions of the state of origin.

- It is important to ensure that measures relating to knowledge security do not 'go overboard' and lead to arbitrary exclusion, suspicion or discrimination.

Threat assessment

- State actors use a variety of methods **to acquire knowledge and technology** that they can use for military purposes or for objectives that are not consistent with our fundamental values. Examples include centrally controlled talent programmes, applying pressure to compatriots (or former compatriots) who have emigrated, digital espionage and the recruitment of individuals in strategic positions.
- **Inter-institutional partnerships** are also used as tools. In such cases, the academic partner acts as an extension of the government. This assigns a **double agenda** to what is ostensibly an academic partnership.
- Finally, state actors may undertake activities aimed at **influence and interference**. For example, they may attempt to influence opinions (about the country) or to impede research on objectionable topics. These countries attempt to **maintain control over their compatriots**. The knowledge that they are being watched from their countries of origin causes anxiety for the researchers and students involved. Such anxiety can lead to self-censorship and the impairment of core academic values.

Legal frameworks and codes of conduct

- Legislation and regulations exist to prevent and address threats, and institutions ought to comply. For example, within the European Union, there are strict rules for the export of **dual-use products and technology** that have both military and civil applications. They include all forms of transfer, and thus also **by email or cloud services**. Basic scientific research and technology that is already in the public domain is exempt from export controls. In case of uncertainty about whether the export rules apply, a classification request can be submitted to the **Central Import and Export Office** (CDIU).
- In addition, **international sanction regimes** are in place against countries, organisations and individuals. The current overview is available at www.sanctionsmap.eu. The sanctions against **North Korea** and **Iran** are particularly relevant to knowledge institutions, as they form the foundation for the **enhanced supervision** that applies to a limited number of disciplines.
- The Dutch government is developing measures to further increase the scope for action for knowledge institutions and government bodies. For example, the government is developing an **assessment framework** that provides a targeted assessment of individuals seeking access to domains of knowledge with a high risk to national security. The government aims for this framework to enter into force in the course of 2023. In addition, the government has presented a legislative proposal on **foreign investments**, mergers and takeovers. The legislation focuses on vital suppliers and organisations that have access to sensitive technology.
- Various **codes of conduct** on knowledge security exist as well. Although they are non-binding, they do provide direction. Examples include the Universities of the Netherlands (UNL) knowledge security framework and the European Commission's guidelines on tackling R&I foreign interference. Several countries have since elaborated similar codes of conduct. These codes facilitate conversations about knowledge security with foreign partners.

Risk analysis

- The accurate identification of **sensitive domains of knowledge** within an institution is important. Examples include dual-use technologies and knowledge that can be used for unethical purposes. It is also important to chart the institution's '**crown jewels**': the domains that pose risks associated with knowledge transfer and within which the institution is an international leader. A brief risk analysis should be conducted for each sensitive domain of knowledge.
- Public threat information—including the State Actors Threat Assessment (*Dreigingsbeeld Statelijke Actoren*) published by the National Coordinator for Security and Counterterrorism (NCTV), the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD)—can be used to estimate **a country's risk profile**. International rankings can also be consulted. For example, a poor score in rankings for academic freedom and respect for the rule of law **should raise red flags**. A poor score does not necessarily rule out the possibility of collaborating with institutions in the country in question, but it is important to take proper precautionary measures.
- Thereafter, as part of **due diligence**, it is important to examine the background of the foreign partner or client. This involves paying close attention to **signals**, like a lack of information on the internet or the fact that the institution is not known to anyone. Consider what the motives of clients or research funders might be and what interest they might have in specific outcomes. It is important to be aware of the possibility of being gradually brought into a situation of **financial (or other forms of) dependence**. In case of security risks, it is important to involve the security coordinator and ensure that decisions concerning engagement with the partner are included in the partner acceptance policy by the organisation's board.

Risk Management

- It is advisable to **regulate a number of standard processes at the central level**. Depending on the level of risk, stricter risk analyses may be needed, and decision-making should be taken at a higher, more central level.
- Risk management starts with the appointment of a **portfolio holder at board level** and the establishment of a **Knowledge Security Advisory Team** consisting of experts with relevant expertise to assist the portfolio holder. As part of an open security culture, employees should have access to counsellors of a wellbeing team to whom they can report signals of security risks. These counsellors should be well-informed regarding risks relating to knowledge security.
- A current, central **overview of security-sensitive partnerships, funding and foreign PhD students and visiting researchers** should be provided at board level. This 'dashboard' forms the foundation for effective risk management within the institution. It also provides insight into the cumulative effect of developments that may not seem problematic in isolation.
- Consideration should also be given to **physical and digital protection measures**. Which floors or rooms have a restrictive access policy? Who has access to research data? For work involving highly sensitive data, it could be advisable to work according to document classifications (e.g. 'confidential' or 'secret').

- The creation of an **open security culture** within the institution is essential. **Awareness-raising campaigns** can be useful in this regard. Whenever possible, such campaigns should be linked to the experiences of the target groups through training modules, team sessions and simulations.

International partnerships

- Cooperation agreements provide a good starting point for considering opportunities and risks. For high-risk collaborations, standard agreement templates may not be sufficient. It would be wise **to bring in legal and security expertise**.
- Once an agreement has been concluded, it would be advisable to evaluate the partnership regularly and address any problems at an early stage. **High-risk agreements should never be renewed automatically**. Within the organisation, it is important to be alerted well before the renewal moment, in order to allow for a critical review of the agreements.
- Knowledge security can also play a role in **procurement and contracting**. The timely identification of risks can make it possible to take appropriate measures (e.g. including additional contract requirements).

Human resources policy

- The **recruitment and selection** of new staff members constitutes a crucial moment for assessing security risks. It is therefore important for HR staff to be conscious of security and to pick up on any signals of increased risk.
- New staff members should receive **information and training** to make them conscious of security. In addition, refresher modules and special training programmes can be provided for visiting researchers from countries with increased risk profiles.
- It is advisable to develop a **visitor protocol** to reduce risks during visits to sensitive sites. Conversely, **business trips** to countries with increased risk profiles (e.g. to participate in conferences) require careful preparation and alertness.

Cyber security

- **Digital threats are increasing**. Knowledge institutions in the Netherlands are also regular targets of cyber attacks. The greatest threats are posed by state and criminal actors.
- **Coordinated cyber attacks** involving states are persistent and can go unnoticed for long periods. State actors also use cyber attacks to disseminate **disinformation**. It is important to remember that digital risks from companies or services (e.g. cloud services) with which the institution works can also affect the organisation.
- The first step in countering these threats is to invest in **awareness**, as human behaviour can override all technical and procedural measures. It is important to pay continuous attention to cyber security at the board level and to organise risk management in such a way that cyber attacks can be detected and countered in a timely manner. **Chain cooperation** is crucial to effective crisis management and the restoration of regular education and research processes.

Section 1

Introduction

World-class higher education and science cannot exist without international cooperation and scientific talent from all over the world. The leading position and good academic reputation of Dutch knowledge institutions are related to the academic freedom that is guaranteed in the Netherlands, as well as to the openness of our knowledge institutions towards the world. Our prosperity is due in large part to scientific collaboration. At the same time, geopolitical power shifts are taking place, with economics, geopolitics and security intertwined. Within this context, knowledge and innovation are increasingly regarded as a strategic means of power that can be used alongside or in combination with traditional means (e.g. espionage). These developments affect everyone who is active in the Dutch knowledge sector. It is therefore a joint challenge to better safeguard knowledge security.

Rationale for these guidelines

We are pleased to present the guidelines for knowledge security of the Dutch knowledge sector and the Dutch central government. The guidelines are intended as a guide for anyone who is involved in international cooperation within knowledge institutions and who weighs opportunities against risks (including security risks). Although the primary focus is on the board members of knowledge institutions, the guidelines can also provide useful suggestions for others, including security coordinators, project managers and individual researchers.
Can international partnerships lead to undesirable knowledge transfer? Is there a possibility of covert influence? Does the collaboration raise ethical issues (e.g. could the research results be misused in the partner's country)?

The aim is to ensure that international scientific cooperation can take place safely, with an appropriate balance of opportunities and risks, and with respect for and adherence to our core academic values

These guidelines provide a starting point for addressing these types of questions. The aim is to ensure that international scientific cooperation can take place *safely*, with an appropriate balance of opportunities and risks, and with respect for and adherence to our core academic values by all parties involved. Proportionality and customisation are essential when taking protective measures. Regarding knowledge security, therefore, the basic principle should always be 'open where possible, protected where necessary'.

What is knowledge security?

In these guidelines, knowledge security refers primarily to preventing the undesirable transfer of sensitive knowledge and technology with negative implications for our national security and ability to innovate. It also involves covert activities aimed at influence and interference activities on the part of state actors within the context of higher education and science. Such foreign interference can lead to forms of censorship (including self-censorship), thereby resulting in the impairment of academic freedom.
Finally, knowledge security concerns ethical issues relating to collaboration with individuals and institutions from countries in which fundamental rights are not respected. For example, researchers from an institution might become involved in the development of technology that could be used in these countries to oppress their own citizens.

Threats from state actors aimed at knowledge institutions

With the intention of increasing their own military, technological, political and economic power, various state actors are also actively seeking knowledge and technology in the Netherlands. Some applications of this knowledge and technology might not be compatible with Dutch interests, while others might go against our fundamental values. Examples could include application in conventional arms programmes or programmes for weapons of mass destruction (e.g. nuclear, biological or chemical weapons), including the means of transporting them (e.g. ballistic missiles and uncrewed aircraft). Such threats could also involve knowledge and technology that could be applied within mass surveillance programmes and for digital attacks, or other sensitive and emerging technologies that could potentially pose a threat to national security. Undesirable dependencies could also emerge from such threats.

State actors also acquire knowledge and technology in ways that abuse the openness of Dutch knowledge institutions and the academic freedom guaranteed in the Netherlands. There is a sliding scale, in which it is not always easy to distinguish between illegal activities, covert intentions and legitimate collaboration. In some cases, illegal and covert means could be deployed (e.g. digital or other forms of espionage). In other cases, these activities are legitimate (e.g. the international exchange of students, researchers or staff members), but involve the influence of state actors with covert intentions. Yet other situations may involve legitimate academic collaboration without any covert intentions on the part of the person coming to the Netherlands, where the knowledge and information developed through the exchange is later acquired by a state actor to be used for objectionable purposes. In addition to the acquisition of knowledge and technology, state actors may also engage in activities aimed at influencing and interfering in the operations of knowledge institutions. For example, such actors may use these activities to influence scientific research or censor publications.

A further elaboration of the threat assessment is provided in *Section 3* ↗.

A joint challenge

It is of great importance to achieve a structural increase in security awareness and in resilience against knowledge security risks faced by Dutch universities, research institutes and universities of applied sciences. Self-regulation plays a central role in the approach to knowledge security, proceeding from the institutional autonomy of the knowledge institutions. This means that, within the existing legal frameworks, the knowledge sector monitors safety risks itself, formulate its own approach and develop its own instruments, thereby actively investing in the resilience of knowledge institutions.

Organisations such as the Association of Universities of Applied Sciences (VH), Universities of the Netherlands (UNL), the Royal Netherlands Academy of Arts and Sciences (KNAW), the Dutch Research Council (NWO), the Dutch Federation of University Medical Centres (NFU) and the federation of applied research organisations (the TO2 Federation), can serve as initiators and facilitators in this regard, through such efforts as bringing institutions into dialogue with each other and charting and exchanging best practices. For example, UNL, NWO and the TO2 Federation have their own working groups for knowledge security.

However, knowledge security also affects our country's national security. The protection of national security is one of the core duties of the government. For this reason, an active role is reserved for the Dutch central government. The central government is working with the knowledge sector to provide scope for action that will help knowledge institutions to fulfil the responsibility associated with their institutional autonomy, which is established by law in the Netherlands. These efforts involve providing information and advice, exchanging ideas and facilitating. They also entail setting frameworks as needed for purposes of national security, in addition to monitoring compliance with these frameworks.
For example, a National Contact Point for Knowledge Security is available to provide expertise and advice to knowledge institutions.

National Contact Point for Knowledge Security
www.loketkennisveiligheid.nl
To ensure that knowledge institutions have a single point of contact for questions about knowledge security, a National Contact Point for Knowledge Security has been established. All relevant departments of the Dutch central government are connected to this service. This will improve the ability to share the broad expertise of the ministries and service agencies with those individuals within knowledge institutions who are involved in international collaboration and who encounter dilemmas in the process. The national contact point will be able to provide information and advice. Institutions will be able to use this information when weighing opportunities against risks.
The basic functions of the contact point have been operational since early 2022, with further development taking place throughout the course of the year. The contact point will simplify contact with the various ministries and services by providing a single point of access. The National Contact Point for Knowledge Security is part of a coherent package of measures and initiatives announced by the government at the end of 2020 [1].

These guidelines are explicitly intended as a living document that can serve as a basis for discussions with peers and experts

These guidelines are another example of the cooperation between the knowledge sector and the Dutch central government to strengthen security awareness. It is a joint initiative of the Dutch knowledge sector (KNAW, NWO, UNL, VH, NFU and the TO2 Federation) and various departments of the central government (OCW, EZK, NCTV, BZ, AIVD and MIVD). This broad cooperative effort reflects the fact that knowledge security is a challenge for which we all bear responsibility.

The threat assessment is dynamic, and increasing attention is being devoted to the risks associated with it. New policies are being developed both nationally and internationally. These guidelines are explicitly intended as a living document that can serve as a basis for discussions with peers and experts. It will be updated according to new experiences and insights.

Document structure

All relevant aspects of knowledge security are addressed in these guidelines. We proceed step by step from the various risks and threats to taking mitigation measures and from negotiating good cooperation agreements to increasing resilience against cyber attacks by state actors.

The guidelines proceed from the core academic values (including academic freedom and research integrity), as outlined in Section 2. In Section 3, we address the various risks and threats that can occur. Section 4 provides a description of the legal frameworks and codes of conduct that are intended to provide a starting point to knowledge institutions.
In Section 5, we discuss the preparation and performance of risk analyses, with particular emphasis on the identification of an institution's 'crown jewels' and sensitive domains of knowledge. Section 6 explains what you can do within your organisation to better safeguard knowledge security. In Section 7, we address establishing and managing partnerships with foreign institutions and companies, with Section 8 being devoted to the role that human resources and visitor policies play in this regard. Section 9 concerns cyber security in relation to state-actor threats.

Finally, we provide a list of sources and contacts, with references to additional information on relevant topics and subtopics.

Section 2

Protecting core academic values

Within the knowledge sector, core academic values (e.g. academic freedom and research integrity) constitute the touchstones for our actions. State-actor threats can undermine these core values.
This section concerns academic freedom, research integrity and openness, as well as how these values can be compromised in international collaboration. It also explores the ethical aspects of knowledge security. At the same time, measures relating to knowledge security should never lead to discrimination or arbitrary exclusion.

2.1 Academic freedom and research integrity

Research in the Netherlands should be conducted in accordance with nationally and internationally accepted standards of academic performance

Core academic values (e.g. academic freedom and research integrity) constitute the foundation for higher education and science in the Netherlands. Research in the Netherlands should be conducted in accordance with nationally and internationally accepted standards of academic performance. Respect for these core values is a prerequisite for full participation in the academic community.

Academic freedom is essential to proper academic practice, and it is therefore guaranteed by law in the Higher education and Scientific Research Act (WHW).

What does academic freedom entail?

The Royal Netherlands Academy of Arts and Sciences (KNAW) defines academic freedom as the principle that staff members at academic institutions are free to conduct their scientific research, disseminate their findings and teach. This freedom extends to aspects including the following:

- *The choice of topics to be investigated*
- *The choice and application of research questions and methods*
- *Access to sources of information*
- *The publication and sharing of information through conferences, lectures and membership of academic groups*
- *The choice to enter collaboration with academic partners*
- *The realisation of academic higher education*

The boundaries of academic freedom are determined by the extent to which five basic principles are observed: fairness, diligence, transparency, independence and responsibility. Particular attention should be directed towards responsibility in this regard. Responsibility also means that researchers are aware that they are not operating in isolation and therefore should take into account the interests of all individuals, clients and funding bodies involved in research, as well as the context within which the research takes place. The knowledge sector is committed to including knowledge security as an aspect to be taken into account within the context of international scientific collaboration.

The Dutch knowledge sector has committed to national and international codes of conduct with regard to research integrity. These codes serve as guiding principles for education and scientific practice in the Netherlands, including with regard to activities with foreign parties.

They thus provide guidance for entering international partnerships or research projects (e.g. when developing a collaboration contract with an international partner; see Section 7 ↗). As a result, foreign lecturers (including visiting lecturers) and researchers must also endorse and comply with these codes when working in the Netherlands.

Codes of Conduct for Research Integrity

To clarify the meaning of research integrity, the collective Dutch knowledge field (KNAW, NFU, NWO, the TO2 Federation, VH and UNL) has established the Netherlands Code of Conduct for Research Integrity[2]. In this code, the five principles that form the foundation for integrity in research (e.g. honesty, diligence, transparency, independence and responsibility) are elaborated into 61 standards of good research practice. The code also contains guidelines for addressing alleged violations of research integrity.

There is also a European code of conduct: European Code of Conduct for Research Integrity, elaborated by the European Federation of Academies of Sciences and Humanities (ALLEA), in which the Netherlands is represented by the Royal Netherlands Academy of Arts and Sciences/KNAW[3]. The European Commission recognises this Code as the reference document for research integrity for all EU-funded research projects and as a model for organisations and researchers throughout Europe.

Various knowledge institutions have their own codes of conduct, in which their internal rules concerning research integrity and/or security are further elaborated. For example, the University Medical Centres have 'research codes'.

Activities of state actors can result in the impairment of academic freedom and research integrity. The ways in which this can be manifest are discussed in Section 3 ↗. Failure to respect core academic values can have far-reaching consequences for the quality of education and research, as well as for the academic reputation and international standing of the researchers involved and the institutions they work for.
In addition, covert influence on higher education and science by state actors can result in censorship (or self-censorship) by students and researchers who no longer feel free to talk about certain topics, thereby impairing social safety.

These guidelines are intended to draw attention to the importance of including not only purely scientific considerations, but also considerations of knowledge security when contemplating entering international collaboration

The Netherlands Code of Conduct for Research Integrity specifies the implications of integrity from the academic perspective. These guidelines on knowledge security are intended to draw attention to the importance of including not only purely scientific considerations, but also considerations of knowledge security when contemplating entering international collaboration.

2.2 Open science

The Netherlands endorses the European aim of making the results of publicly funded research accessible to all. Examples include providing open access to publications and ensuring that research data are 'FAIR' (findable, accessible, interoperable, reusable). The free sharing of scientific insights is an important principle of scientific practice and an important driver for the development of new knowledge and innovations.

Within the European Union, it has been agreed that open science should become the standard in scientific research, and this practice is already becoming more commonplace within the knowledge sector. This does not mean, however, that all international partners also practice open science. Moreover, there may be legitimate reasons to protect some research results and to make them public only in part, if at all. These include privacy, national security, intellectual property and commercial reasons.

There may be legitimate reasons to protect some research results and to make them public only in part, if at all. These include privacy, national security, intellectual property and commercial reasons

It is important to consider whether research at your own institution involves such aspects and, if so, what agreements can be made with international partners. For example, agreements can be made regarding the extent to which data is to be shared or only viewed (data visiting). Making sound agreements with regard to these aspects in advance can prevent tension from arising later in the process between the desire for maximum openness and legitimate reasons for taking protective measures.

2.3 Ethics in science

Ethical dilemmas can also arise in international collaboration. For example, such dilemmas could occur during collaboration with individuals and institutions from countries in which fundamental rights are not respected. Think of the fundamental rights as established in the Universal Declaration of Human Rights and the European Convention on Human Rights (ECHR).

Questions could arise concerning how to deal with research commissioned by foreign parties that are likely to use the technology to monitor minorities in their own countries. Another possibility is that researchers from countries that do not respect fundamental rights might be forced to use their knowledge for purposes that violate fundamental standards and values during their research or upon returning to their home countries.

It is advisable to have an ethics committee within the institution

It is important to be and remain alert to this possibility at all levels within the institution, both when entering contact and in the further course of the collaboration. Many knowledge institutions already have ethics committees. One could think of ethical issues that could arise within a university medical centre (UMC) regarding medical-scientific research involving human subjects. An ethics committee can provide advice on these matters. It is advisable to have an ethics committee within the institution to which researchers can also report and discuss issues relating to international collaboration that pose ethical dilemmas.

This means that ethics committees should not focus solely on the way in which research is carried out, but also on potentially unethical application of research results.

2.4 Inclusiveness and non-discrimination

Dutch higher education institutions provide their students with a safe learning environment. Knowledge institutions provide their staff members with a safe working environment, regardless of their position. Knowledge institutions have a duty of care regarding the social security of their staff and students. There is no place for discrimination at Dutch knowledge institutions.

Duty of care for knowledge institutions

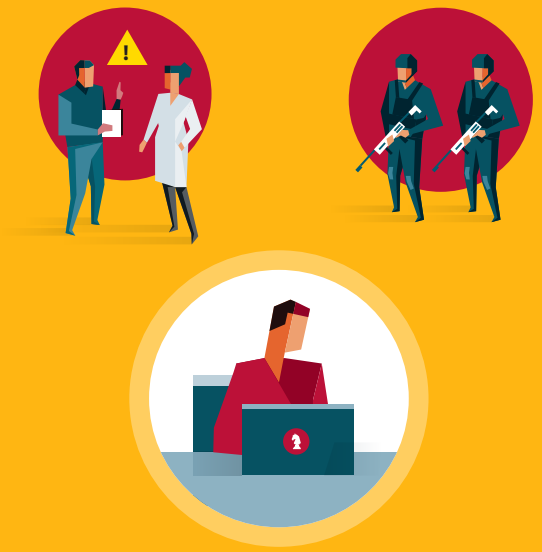
The Netherlands Code of Conduct for Research Integrity describes the duty of care for researchers as follows: 'Institutions provide a working environment that promotes and safeguards good research practices. They ensure that researchers can work in a safe, inclusive and open environment where they feel responsible and accountable, can share concerns about dilemmas and can discuss errors made without fearing the consequences ("blame-free reporting")'. [...] The duties of care relate to training and supervision, research culture, data management, publication and dissemination, and ethical norms and procedures'.

Any measures taken should always be objective, proportional and related to an actual danger

Especially with regard to a subject like knowledge security, in which threat analyses and risk profiles play an important role, there is a danger that an approach will 'go overboard' and lead to forms of arbitrary exclusion, imputation and discrimination. This should be avoided at all times. Any measures taken should always be objective, proportional and related to an actual danger. It is important to engage in open discussion about this within the institution and to take any and all signals seriously. See also the National Action Plan for Greater Diversity and Inclusion in Education and Research[4].

Section 3

Threat assessment



What types of threats are involved in knowledge security? What are the motives and working methods of state actors? How can core academic values come under threat? This section provides a closer look at the nature of threats and how they may manifest themselves.

3.1 Which threats are involved?

The Netherlands runs the risk that any knowledge that has been transferred will later be used for purposes that directly affect our national security or for purposes that conflict with our fundamental values

Various state actors are – also in the Netherlands – actively seeking knowledge and technology with the intention of increasing their own military, technological, political and economic power. The Netherlands runs the risk that any knowledge that has been transferred will later be used for purposes that directly affect our national security (e.g. in the form of military resources) or for purposes that conflict with our fundamental values (e.g. for mass surveillance resources).

In addition to the acquisition of knowledge and technology, state actors may also engage in activities aimed at influencing and interfering in the operations of knowledge institutions. In doing so, an actor might try to influence opinions and publications or to censor scientific research and research results. To this end, actors may make use of financial dependencies. Some actors also keep an eye on their compatriots in order to prevent them from voicing objectionable opinions about the homeland for instance at lectures or conferences.

The pressure of these activities can lead to self-censorship, with individuals and groups not always daring to be openly critical or with academics being prevented from publishing research results that are unwelcome to a particular state actor. This poses a threat to fundamental liberties such as freedom of expression and core values such as academic freedom and research integrity. The most important threats are elaborated below.

3.2 Acquisition of knowledge and technology

Transfer by individuals

State actors purposefully send students, researchers and staff to foreign knowledge institutions in order to acquire knowledge that the state actor is looking for. This occurs at Dutch knowledge institutions as well. This could, for instance, occur as part of a centralised talent programme. Another possibility is that an actor might require *quid pro quo* for funding a foreign internship, training place or (temporary) job in the form of reporting back the research findings, or by claiming ownership of the research findings. Students and researchers do not always disclose that they have ancillary activities or obligations to other knowledge institutions, for instance as part of the aforementioned talent programmes.

Several state actors are known to be willing to force their compatriots (current or former) who have emigrated to cooperate with the interests of that state

Several state actors are known to be willing to force their compatriots (current or former) who have emigrated to cooperate with the interests of that state. In such cases, foreign students, researchers and staff members of Dutch institutions could unwittingly be used or abused by state actors for the transfer of knowledge. In such cases, pressure is exerted on certain students, researchers or staff members. Such pressure could be further exacerbated if the state actor also exerts pressure on people close to them such as relatives, friends or colleagues.

Individuals in strategic positions within the knowledge institution can be interesting targets for state actors, either because of their own knowledge or because of their access to knowledge, technology or laboratories. State actors use a variety of working methods to recruit such individuals, including social engineering, bribery, blackmail and intimidation. Depending on the working method used, it is important to realise that an individual who has been recruited is not necessarily cooperating with the state actor out of free will. In some cases, the dividing line between conscious and unconscious cooperation is likely to be quite thin. Students, researchers or staff members are not always aware that they are actually cooperating with parties that have ties to a foreign government. Certain forms of recruitment such as social engineering are very gradual. The target is slowly 'reeled in', sometimes over an extended period, until there is no way back for the one who has been recruited.

State actors actively use practical and financial means to recruit and facilitate talented students and scientists to come and study or work in their countries. This can be made attractive through such means as providing grants and creating favourable research facilities (e.g. with large, specialised centres of innovation). State actors often do this in close and coordinated cooperation with research institutions in their own countries, which can offer good working conditions and high-quality research facilities to scientists, with the help of state support provided by these actors. There is a risk that research results or data from research initiated and/or funded by a Dutch knowledge institution will be copied by a state actor.

In some cases, the dividing line between conscious and unconscious cooperation is likely to be quite thin

Like any other potential targets who possess valuable digitised knowledge and information, students, researchers and staff members of knowledge institutions can become targets of digital espionage activities by state actors. Intelligence and security services have acknowledged that several state actors have offensive cyber programmes that are also directed against Dutch interests. These countries are also in the vanguard with regard to economic or other types of espionage. Some state actors conduct extensive and structural espionage campaigns aimed at obtaining high-level knowledge and technology. If such knowledge and technology is available from specific individuals (e.g. researchers and staff members of a knowledge institution), espionage activities will be directed towards them. For example, phishing (or spear-phishing) attacks aimed at specific targets can be used to gain access to systems and files.

Links between knowledge institutions and state actors are not always clear, which in practice could mean that Dutch knowledge institutions enter collaborations that appear to be academic in nature but in fact have a double agenda

Transfer by partnerships

In various countries, state actors are working in close cooperation with research institutions. In some cases, knowledge institutions (e.g. universities) may even belong directly to the government. If this is the case, a state actor may also use financial support or official control in order to have a decisive say in which national or international partnerships the institution will enter. Such collaborations can be used as an extension of a country's own public policies, for example the development of the military, the improvement of digital attacks or for use in mass surveillance.

Links between knowledge institutions and state actors are not always clear, which in practice could mean that Dutch knowledge institutions enter collaborations that appear to be academic in nature but in fact have a double agenda. The connection to a knowledge institution, whether through funding or control, allows the state actor to make a claim on research results or intellectual property.

3.3 Activities aimed at influence and interference

Some state actors use resources in order to influence how they are seen, understood or portrayed internationally. Some state actors also attempt to seek global legitimacy for their policies. From this perspective, students, researchers and staff members in Dutch knowledge institutions can be targeted by state actors for purposes of influencing opinions and publications and censoring scientific research and research results. Such activities may target institutes (or individual students, researchers and staff members) in which research is conducted on topics that are inconvenient to a state actor (e.g. human rights violations) or topics that a state actor fears will result in the publication of unwelcome findings. With regard to these activities, an actor may deploy financial resources either as an incentive or as a means of applying pressure.

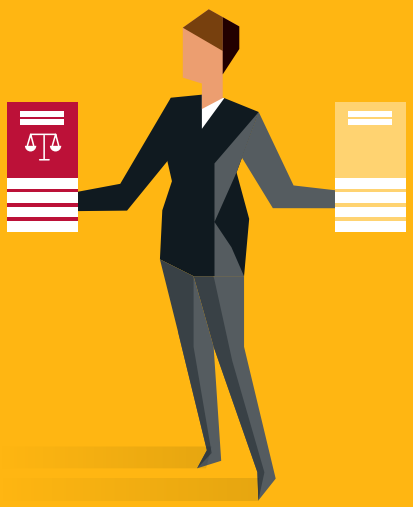
In addition, some state actors stand to benefit from keeping an eye and a grip on their compatriots for instance in order to prevent them from voicing 'dissident' or disagreeable opinions about the country of origin. From this perspective, students, researchers and staff members of knowledge institutions could also be targets of state actors, notably those who are studying or teaching potentially disagreeable subjects. There have been cases in which students were afraid of being reported by their peers in the country of origin. The mere knowledge that they might be being watched from the country of origin can create a sense of insecurity amongst students, researchers and staff members. This can lead to self-censorship, the erosion of social safety and the undermining of our core academic values.

Scientific experts can be attractive to state actors to serve as credible mouthpieces when, by virtue of their expertise, they are able to express views that are in line with the actor's interests

Finally, scientific experts can be attractive to state actors to serve as credible mouthpieces when, by virtue of their expertise, they are able to express views that are in line with the actor's interests. For example, they might be invited to write articles in certain foreign media or to speak at symposiums.

Section 4

Legal frameworks and codes of conduct



National and international legal frameworks and codes of conduct exist that contribute to the security of the Netherlands. Institutions are required to comply with legislation and regulations, which constitute the 'hard' frameworks within which collaboration with international partners must take place. In this section, we address export control and sanction regimes, as well as legislation that is currently in preparation. Additionally, we turn our attention to the various codes of conduct that have been developed within the knowledge sector and that provide guidance and can be helpful for purposes of decision-making.

4.1 Export rules for dual-use products and technology

When entering international cooperation, European export rules regarding dual-use products and technology are relevant. This includes goods, software and technology used for civilian purposes, but that may have military applications or contribute to the production or proliferation of weapons of mass destruction (e.g. nuclear, chemical warfare agents or biological weapons) or their means of delivery.

The EU Dual-Use Regulation[5] imposes strict rules for the export and transit of such products and technology. A licence is required for export outside the European Union and, in some cases, for transfer within Europe. The dual-use rules may also apply to products and technology that might not initially be expected to fall under these rules, such as certain frequency converters, as they could be used in the proliferation of weapons of mass destruction. In addition, the term 'export' is quite comprehensive. It covers all forms of transfer, regardless of the means, and thus also by email or cloud services[6].

The term 'export' is quite comprehensive. It covers all forms of transfer, regardless of the means, and thus also by email or cloud services

It is therefore important to remain alert to the potentially undesirable use and sharing of your research, knowledge or technology. Knowledge institutions are responsible for complying with these EU rules and, apart from the security risks involved, breaches of these rules can lead to prosecution.

The export control rules do not apply to fundamental scientific research. That having been said, it is not always clear where fundamental research ends, and applied research begins. The Technology Readiness Level (TRL) methodology is a helpful tool in this regard. The TRL methodology is a scale from 1 to 9 that expresses the economic applicability of the technology, and it is also used within Horizon Europe. Levels 1 and 2 are considered fundamental scientific research, Levels 3 and 4 must be considered on a case-by-case basis, and Levels 5 and above are application-oriented and therefore potentially subject to export controls. Various tools are available for determining the TRL level of research. For example, see the 'TRL Assessment Tool' of the Canadian government, which is equally applicable to the European situation[7].

Another factor that plays a role in determining whether a research project does or does not constitute fundamental science is the source of funding. If most or all the funding is from a company, it is likely that the research is aimed at commercial development of technology. This may be an indication that the research results generated by such a research project do not fall within the definition of basic scientific research and may therefore be subject to export controls.

A second exception to the export control rules that is relevant to the scientific community concerns whether the technology is already 'in the public domain'. This means that the technology is accessible to anyone who wants it, regardless of whether a fee is charged, or registration is required. Examples could include classical control technology or aerodynamics.

For the purpose of export controls, the Dutch government uses the European list for dual-use products and technology. It is the responsibility of the institution to be aware of any dual-use classifications. It is necessary to apply for a licence in order to export anything that is included on this list. A practical EU recommendation for knowledge institutions is available regarding establishing internal compliance procedures[8].

Which technology is involved?

The EU regulation on export control is highly detailed and therefore not easy for laypeople to understand. To provide an impression of the fields of knowledge that may be covered, products and technology are divided into the following 10 categories:

- Nuclear materials, facilities and equipment
- Special materials and related equipment
- Materials processing
- Electronics
- Computers
- Telecommunications and 'information security'
- Sensors and lasers
- Navigation and avionics
- Marine
- Aerospace and propulsion

When making a risk assessment, the end-user is an important factor

When making a risk assessment, the end-user is an important factor. In some cases, an end-user statement (EUS) may be requested. This is a document signed by the end-user, declaring that the goods will not be used other than for civilian purposes.

In case of doubt or questions, please contact the Central Import and Export Office (CDIU). It is also possible to submit a request for classification[9]. in case of uncertainty concerning whether the materials, software, technology or services to be exported are or are not covered by the dual-use legislation. The CDIU and the Ministry of Foreign Affairs conduct a risk assessment for each licence application. In addition, the Ministry of Foreign Affairs organises biannual seminars on export control for companies and knowledge institutions that would like to know more about this issue.

In the life sciences, biosecurity is an important issue. Scientific research on high-risk pathogens is essential to the development of diagnostics, vaccines and therapies. The results of such research are nevertheless subject to abuse. To help knowledge institutions counter this form of dual use, the National Institute for Public Health and the Environment (RIVM) has established the Biosecurity Office[10] as a contact point for government knowledge and information on biosecurity. A part of the website is specifically directed towards researchers. Resources available on the site include an online tool for identifying potential dual-use aspects of research, as well as the KNAW code of conduct for biosecurity.

4.2 International sanction regimes

When there is a threat to international peace and security, for example due to violations of international law or human rights, the United Nations (UN) and the European Union (EU) can impose sanctions on countries, organisations, companies and individuals as needed in order to maintain or restore international security. Sanctions can be aimed at stopping the spread of nuclear weapons, as well as at countries, individuals and organisations that violate human rights or that are involved in terrorist activities. Sanctions are mandatory. The infringement of a sanction regulation is a criminal offence. Current information about the applicable sanction regimes is available at the following website: www.sanctionsmap.eu.

The infringement of a sanction regulation is a criminal offence

The UN and EU sanctions against North Korea and Iran, which prohibit the transfer of certain technology and expertise to these countries, deserve special attention within this context.

Sanctions against North Korea and Iran

In the case of North Korea, the sanctions concern matters including the transfer of knowledge that could contribute to North Korea's proliferation-sensitive activities or to the development of systems for the transport of nuclear weapons. Within this context, the government decides whether exemptions can be granted to individuals so that they can access specialised knowledge, based on the North Korea Sanctions Regulations 2017.

In the case of Iran, there is a prohibition on the transfer of materials or technology that could contribute to the development of objectives including the ballistic missile programme, as well as on the provision of technical assistance relating to such materials and technology for use in Iran. Examples include gas turbine engines, ceramic powders, composites with certain properties and oxidisers suitable for rocket engines. Sanctions have also been imposed on a number of knowledge institutions, due to their contributions to proliferation-sensitive activities. Collaboration with these knowledge institutions is not permitted. Collaboration with individuals who have worked indirectly, or in the past, at sanctioned institutions must be assessed on a case-by-case basis. The list is included in Annexes VIII, IX, XIII and XIV of the Iran Sanctions Regulation[11].

Under these sanctions, several fields of knowledge at Dutch knowledge institutions are subject to 'enhanced supervision', meaning that anyone seeking to obtain access to them is subject to screening by the government. This assessment applies irrespective of nationality (and thus also to Dutch citizens) and for as long as the international sanctions are in force. Screening is conducted only in areas of education and research in which there is a risk of violation. The list of fields of knowledge that are subject to enhanced supervision is available on the government's website[12].

In case of doubt or questions concerning the applicable sanction regimes, please contact the Central Import and Export Office (CDIU) of the Customs Administration.

Policy in development

Policy development relating to knowledge security is in full swing. Various measures are being developed in order to expand the scope for action and the resilience of Dutch knowledge institutions, companies and government bodies. Two relevant government initiatives are briefly explained below. It is important to emphasise that these are proposals that have yet to be addressed by parliament.

Screening framework for undesirable knowledge and technology transfer

In late 2020, the government announced a coherent package of measures and initiatives aimed at further increasing the security awareness and resilience of the Dutch knowledge sector[13]. These measures place strong emphasis on self-regulation within the sector, in keeping with the autonomy of knowledge institutions.

For disciplines in which the risks to national security are greatest, the government does not consider self-regulation sufficient. It is therefore developing a screening framework for individuals seeking to obtain access to these specific disciplines. The design and scope of the assessment framework are still the subject of consultation, in which the government is also involving the knowledge community. The government aims for this screening framework to enter into force during the course of 2023, thereby replacing the current enhanced supervision (see above).

Act on the security assessment framework for investments, mergers and acquisitions

State actors can also acquire sensitive knowledge through foreign investments in, mergers with or acquisitions of Dutch companies. The 'Act on the security assessment framework for investments, mergers and acquisitions (the 'Wet Vifo') is being developed in order to prevent such acquisition activities from posing risks to national security. This legislation will be aimed at vital suppliers and companies that possess sensitive technology. The legislative proposal was presented to parliament for debate in June 2021.

This act is unlikely to affect knowledge institutions in the performance of their research and education tasks. In some cases, however, knowledge institutions have an equity stake in start-ups operated by current or former students or staff members. Recruitment activities in these companies could fall within the scope of the investment assessment.

4.3 Codes of conduct for knowledge security

As a rule, codes of conduct are not binding, although they do provide direction

As a rule, codes of conduct are not binding, although they do provide direction. Such instruments are well-suited to the knowledge sector, which is characterised by a high degree of autonomy and self-regulation.

Universities of the Netherlands (UNL) Knowledge Security Framework

To assist universities in decision-making and policies concerning knowledge security, the Universities of the Netherlands (UNL) have drawn up a Knowledge Security Framework for universities[14]. The text provides a framework to which Dutch universities can express commitment and within which they may shape their own institutional policies.
The framework addresses opportunities and risks associated with international cooperation, governance and policy frameworks, in addition to providing concrete recommendations for risk management. It thereby enables universities to take well-informed, justified decisions about international collaboration.

EU guidelines on tackling foreign interference in research and innovation.

The European Commission has developed guidelines aimed at countering foreign interference within the European knowledge sector[15]. They were written for a broad target group: national authorities, research institutions and organisations, higher education institutions and individual researchers and other staff members of knowledge institutions. The European guidelines are explicitly intended as a foundation and source of inspiration for security policies of Member States, sector organisations and knowledge institutions.

The guidelines cover four themes: values, governance, partnerships and cyber security. An integral approach is presented for each theme, along with examples of possible measures that could be taken.

Knowledge security in other countries

Other countries are also taking measures to increase knowledge security. Guidelines and checklists are being developed in a variety of countries. These initiatives serve the same purpose as the Dutch guidelines for knowledge security: to provide insight into aspects that should be considered with regard to international collaboration and to obtain an overview of their own resilience and scope for action. Examples include Australia[16], Germany[17], the United Kingdom[18], Sweden[19] and Canada[20].

The fact that both the EU and individual partner countries have such texts makes it easier to discuss these issues when collaborating with them. After all, our partners are also looking for ways to increase alertness and resilience to state-actor threats in higher education and science.

Section 5

Risk assessment

This section provides guidance on how to identify risks of undesirable knowledge transfer. The following three factors play an important role in this regard: the content of the research, the country in which the relevant collaboration partner is based and details concerning the actual collaboration partner. These factors are related to each other and should be addressed as a whole when taking inventory of risks.

5.1 Which knowledge areas within your institution are at increased risk?

Effective risk reduction requires the accurate identification of sensitive knowledge areas. For these areas, risks to national security are associated with the undesirable transfer of knowledge.

Examples include knowledge that has been developed specifically for military applications or dual-use technologies (see Section 4.1 ↗). Although the list of dual-use technologies provides useful suggestions, it is not exhaustive. Knowledge areas that fall outside the scope of export control can also be sensitive. Examples include the domains (or sub-domains) of artificial intelligence, advanced robotics and quantum technology. Here, an increased risk of unethical application of research results may exist, for instance related to mass surveillance programmes.

These risks are even greater for domains in which the Netherlands occupies a unique knowledge position or for technologies that affect the continuity of vital processes in the Netherlands and/or on which the Netherlands is dependent, due to a lack of viable alternatives. Within this context, reference is often made to 'crown jewels': the sensitive domains of knowledge within which your institution has built a reputation and within which research is conducted that is internationally recognised as excellent.

You can conduct a brief risk analysis for each sensitive knowledge area —not only because of national security concerns, but also in the interest of the safety of your institution's staff and in order to safeguard academic core values and reputation. One question to be considered in this regard concerns whether the research (actual or proposed) could potentially be used in an inappropriate or unethical manner and/or whether it could affect our national security, for example due to the military or unethical application of the results.

Identify where unique, sensitive knowledge is located within your institution, which threats exist and the measures that you can take to counter such threats

Identify where unique, sensitive knowledge is located within your institution, which threats exist and the measures that you can take to counter such threats. In this regard, it is important to note that technological developments can render technology either more or less sensitive over time. It is therefore advisable to work with a dynamic list of sensitive knowledge areas, which is revised periodically. The Dutch General Intelligence and Security Service (AIVD) can help with such considerations when carrying out risk analyses within your institution.

5.2 Which countries present an increased risk?

Which countries call for additional attention and, perhaps, additional measures when considering collaboration with partners who are based there? What can you do to assess the risks?

It would be wise to proceed from a risk management policy that addresses threats, regardless of the countries from which they emerge. Significant drawbacks are associated with the decision to focus policy on only a few 'high-risk' countries. In addition to overlooking threats from other countries, which could nevertheless pose a risk, such policies could incriminate everything associated with the selected 'high-risk' countries. The latter is bad for science and contrary to the principle of non-discrimination.

If you would like to assess the risk profile of a specific country, you can make use of the threat information that is publicly available. For example, the National Coordinator for Security and Counterterrorism (NCTV), the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) published a joint 'Dreigingsbeeld Statelijke Actoren' early 2021[21]. In addition, the annual reports of the AIVD[22] and the MIVD[23] contain current information on threats. Another example is www.sanctionsmap.eu which lists countries that are subject to sanctions (see also Section 4.2 ↗).

You could also consult relevant international rankings and indices of NGOs, research institutes and international organisations. Poor scores on such overviews should raise red flags. For example, consider the status of academic freedom, or of freedom in general, democracy and respect for the rule of law. The overviews listed here are intended only as illustrations. What matters is that any risk judgements should be substantiated and supported.

Examples of international rankings and indices

- *Academic Freedom Index: https://www.gppi.net/2021/03/11/free-universities*
- *Freedom in the World Report van Freedom House: https://freedomhouse.org/report/freedom-world*
- *Democracy Index van The Economist Intelligence Unit: https://www.eiu.com/n/campaigns/democracy-index-2020/*
- *World Justice Project Rule of Law Index van World Justice Project: https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2020*

If a country scores poorly on such rankings, that does not necessarily rule out the possibility of collaboration with institutions from that country. In principle, it is possible to cooperate with researchers from such countries, as long as appropriate precautions have been taken and as long as the context within which the intended partner operates is understood.

You can contact the Dutch central government's National Contact Point for Knowledge Security that will provide additional information on the risk profiles of specific countries. The contact point is connected to all relevant departments of ministries and services, including the country experts at the Ministry of Foreign Affairs and the Netherlands Enterprise Agency (RVO).

5.3 Know your collaboration partners, clients and funding bodies

When entering or renewing an agreement, it is important for the researcher or project manager involved to be familiar with the background of the foreign partner organisation or client. 'Due diligence' is the term that is used internationally in this regard. What is the institution's scientific reputation? Who exactly will be involved in the project? What about the costs involved? In this context, it is important to consider knowledge security as well.

Although it is always advisable to pay attention to these aspects, it is absolutely necessary to do this for institutions or companies from countries with high risk profiles (see Section 5.2 ↗) and for collaborations on sensitive domains of knowledge (see Section 5.1 ↗). Here too, it is not a matter of categorically excluding institutions or companies in advance. It means that the staff members involved must be aware of the risks and threats and consciously take measures to prevent them.

They do not have to be security experts: alertness and open sources can go a long way. It calls for keeping a sharp eye out for signs that something may be amiss. One example could be a partner about whom hardly any information is available on the internet and who is not known to anyone. If the intended partner is already known within the organisation or to colleagues at other institutions, these sources can be approached for information. Which experiences have they had? Have any incidents occurred? The institution's security coordinator can provide assistance in retrieving this type of information. The following are a few examples of factors to be considered:

- Is the partner affiliated with the government? One could think of state-operated companies or institutions.
- Is the partner affiliated with the military or the defence industry?
- Do sanctions apply to the partner?
- Does the institution have a demonstrable reputation in the relevant discipline? If expertise is lacking or if it is unclear how the intended collaboration relates to the partner's usual activities, this provides cause for alertness.
- What other research do the researchers involved in the collaboration perform? Are they affiliated with multiple institutions/organisations?
- Does the contact proceed through an entity other than the actual partner organisation (different name, different address), or has this changed during the process?
- Does the partner give vague answers to questions about the intended application of the research findings, have unclear reasons for objecting to standard contract provisions or propose excessive confidentiality provisions?

Safety-related analyses produced by specialised research agencies can also be useful. Examples include the *China Defense Universities Tracker* published by the Australian Strategic Policy Institute (ASPI)[24].

The same cautions apply for clients and research funders as for research partners. In principle, the type of funding body does not matter, it could for instance also concern gifts from donors. Considerations should begin with questions like: 'Where does the money that the partner wants to invest come from?' and 'Which motives might the partner have for funding the research?' Does the funding body have economic or political interests in a particular outcome of the research? The following are a few examples of factors to be considered:

- Little or no information can be found on the client or funding body (e.g. no website).
- The entity being used for funding is atypical for this type of research.
- The client or funding body makes exceptionally large sums of money available or proposes particularly favourable funding conditions and hardly asks anything in return.
- The client or funding body does not want the results to be published, imposes exceptionally strict intellectual property requirements or stipulates confidentiality with regard to end-users and specifications.

It is also advisable to bear in mind that researchers may gradually find themselves in a situation of financial or other forms of dependence

It is also advisable to bear in mind that researchers may gradually find themselves in a situation of financial or other forms of dependence. In such situations, there may be little wrong with the projects and activities individually, but taken together, they allow the funding body to assume a position that makes it possible to take control of the collaboration and its content. The funding body could exert pressure on the institution and/or the researchers involved, whether through positive incentives (e.g. the prospect of rewards) or through negative incentives (e.g. threats).

If the assessment reveals that security risks are associated with the intended collaboration partner, client or funding body, it is important to involve your organisation's security coordinator. Subsequent steps can be considered in consultation with this official. The final decision on whether to enter a collaboration is the responsibility of your organisation's central authority (for universities, the Executive Board). In such decisions, the institution's partner-acceptance policy should include explicit consideration for security risks.

We recommend contacting the Dutch central government's National Contact Point for Knowledge Security. The contact point can share information and expertise available in the ministries and services of the central government and consult on possible mitigation measures that could be taken. Section 7.1 provides further details of aspects that deserve particular attention when entering international partnerships.

Section 6

Risk management

Knowledge security makes great demands on the responsibility that knowledge institutions bear based on their institutional autonomy. Within the institution, risk management is a joint task, for which the entire organisation must feel responsible. The goal is always to ensure that awareness of knowledge security permeates to the very heart of your institution. In this chapter, we discuss various aspects that contribute to a security culture and thus to the resilience of your organisation.

Within a knowledge institution, the Board bears ultimate responsibility for risk management. This also applies to the risks associated with knowledge security. Knowledge institutions should therefore have internal procedures and protocols in place, so that they can identify and address risks in a timely manner.

It is important to emphasize that these guidelines should emphatically not be interpreted as a call to avoid all risks. It is nevertheless essential to have a good understanding of existing threats and risks and to manage them effectively. To this end, this section provides several suggestions related to governance and internal procedures.

6.1 Organise risk management within your organisation

Knowledge institutions, and particularly universities, are characterised by a layered administrative structure. Action is needed at both the central institution level and the decentralised level (e.g. faculties, departments, research groups and individual researchers). Clear agreements should therefore be made with regard to who is to be responsible for what. Based on the principle that ultimate responsibility rests with the Board of the knowledge institution, this means that decision-making authority is delegated by the Board. Formal documentation of such delegation is advisable. This also makes it possible to act quickly in the event of incidents or irregularities.

As the level of risk increases, the required risk analyses and controls are stricter and the decision-making authority lies at a higher, more central level within the organization

As with other forms of security (e.g. cyber security and social safety), it is important to establish a number of standard processes at the central level. This can be done according to the aspects discussed in previous sections. Do you have a clear overview of all threats (Section 3 ↗)? How is compliance arranged within your organisation (applicable legislation, regulations and codes of conduct; Section 4)? Are you aware of the sensitive domains of knowledge within your organisation and the countries that call for particular alertness with regard to state-actor threats (Section 5 ↗)?

All these factors and considerations should be translated into roadmaps that take into account the specific characteristics of the organisation. Risk management calls for customisation. As the level of risk increases, the required risk analyses and controls are stricter and the decision-making authority lies at a higher, more central level within the organisation.

Two comments are important in this regard. First, proportionality is essential when elaborating knowledge security measures. The threat and risks should be in a healthy balance with the measures to be taken. It is obviously undesirable to take too few measures. However, there may be negative consequences related to taking too many measures and/or measures that are too far-reaching too. Consider for instance the bureaucracy associated with an excess of control and distrust. Other disadvantages could involve damage to your academic reputation due to excessive restrictions on openness and accessibility. The principle of 'open where possible, protected where necessary' provides a good summary of the importance of proportionality.

A second comment concerns the risk of unfair treatment and discrimination of students and staff members from certain countries. It is essential to ensure that awareness of risks does not generate hostile images or the arbitrary exclusion of certain groups of students and staff members. The academic values of freedom, respect and open academic discussion must be promoted and exemplified, especially in the training of researchers and in education in general.

6.2 Organisational measures

The goal is ultimately to arrive at an integrated security policy at the institutional level—a policy that brings together the various forms of security (e.g. social safety, cyber security and knowledge security). The first step towards such a policy is to create the necessary awareness of knowledge security and to ensure that this issue is embedded within the administration.

More specifically, it starts with designating a portfolio holder at board level for the theme of knowledge security. Given its strategic and geopolitical nature, it would be a mistake to treat knowledge security as a purely operational issue. This requires attention at board level.

A second recommendation is that the portfolio holder for knowledge security should be assisted and advised by an internal Knowledge Safety Advisory Team, i.e. a team consisting of several experts with different types of expertise. This could essentially consist of: (1) the security coordinator or integral security advisor; (2) an expert in the field of information security (e.g. the Chief Information Security Officer/ CISO); and (3) an expert in the field of internationalisation/ international collaboration. Depending on the case, other expertise may be added (e.g. a human resources consultant). This advisory team should ideally have a formal mandate to provide solicited and unsolicited information and advice to the Board with regard to issues of knowledge security. Particularly for smaller knowledge institutions, it can be interesting to pool certain expertise, for instance with regard to certain countries or knowledge fields, and to work with a shared service.

It is important to work with counsellors of a wellbeing team or ombuds officers, in addition to having good whistle-blower regulations in place

In general, it is important to have an open security culture within your organisation (see Section 6.5 below↗). In addition, it is important to work with counsellors of a wellbeing team or ombuds officers, in addition to having good whistle-blower regulations in place. This can ensure that staff members are able to report suspicions of illegal or unethical practices within the institution, anonymously

and in confidence. Staff members who have concerns about knowledge security, for instance with regard to an overly optimistic assessment of a partnership agreement, should know that they can turn to a counsellor to discuss these concerns in confidence. The counsellors and Ombud officials themselves should be aware of the risks associated with knowledge security, and they should periodically refresh their knowledge in this regard.

As described above (see Section 2.3 ↗), it is advisable for the institution to have an ethics committee that can advise on issues related to the possible use of research results in other countries that contravenes fundamental standards and values, such as human rights.

Note: If the research findings are likely to be used for military applications in the collaboration partner's country, the implications extend beyond ethical considerations to include the legal obligations arising from European export regulation (see Section 4.1 ↗) or international sanction regimes (see Section 4.2 ↗). The infringement of such rules is a criminal offence.

6.3 Ensure an accurate evidence base for decision-making purposes

It is important for central overviews to be available with regard to collaboration with partners and clients outside the EU as wel

Within the framework of internationalisation policy, figures are already existing with regard to student mobility and international PhD students. It is important for such central overviews to be available with regard to collaboration with partners and clients outside the EU as well. Such a current overview provides the foundation for effective risk management. A governing board (the Executive Board in case of a university or university of applied science) should always have insight into the significant collaborations the organisation enters into, without having to consult the parties involved within the organisation.

At the board level, this creates a dashboard – a central overview of security-sensitive partnerships, funding and foreign PhD students and visiting researchers. An additional advantage of such a central overview is that it also makes it possible to see the cumulative effect that, taken together, could create an undesirable dependency (e.g. when working primarily with a single institution or when funding comes mainly from a single client or funding body). Once you have identified such undesirable developments, you will be able to make timely adjustments as needed.
The data registered at the aggregate level can also be used as a factual basis for annual knowledge security reports, for example as part of the annual report.

6.4 Physical and digital protective measures

It is important to ensure that access to areas in which sensitive research is performed (e.g. laboratories) is restricted to those involved in the research

In addition to organisational and administrative measures, relatively simple measures in the physical environment can also be effective. Which buildings are freely accessible, and which floors or spaces are subject to a restrictive access policy? It is important to ensure that access to areas in which sensitive research is performed (e.g. laboratories) is restricted to those involved in the research.

The same applies to research data. Who has access to such data within the system? Which data and results should also be shielded from colleagues and peers who are not involved in the research? Protecting data (through digital or other means) and restricting access to those who have been authorised is an effective and relatively simple way of preventing undesirable leaks.

If highly sensitive research data or results are being processed within the institution, it might be advisable to work with document classification. This entails dividing documents into sensitivity classes, such as 'confidential' or 'secret'. The classification of documents ensures that all staff members are aware of the sensitivity of the information and the measures to be taken in this regard. It helps to ensure that everyone within the organisation is speaking the same 'language' with regard to the confidentiality of information, thereby reducing the risk that sensitive knowledge will be leaked.

General Security Requirements for Defence Contracts (ABDO)

The Ministry of Defence cooperates with companies and a few institutions for applied research. When handling sensitive information these partners must meet the security requirements of the Ministry of Defence. These requirements are specified in the 2019 General Security Requirements for Defence Contracts, ABDO 2019[25]*. The MIVD checks whether companies and institutions are in compliance with the ABDO, and any staff member who has access to state secret information must hold a valid Certificate of No Objection. A company or institution can obtain ABDO authorisation only by entering a state classified contract with the Ministry of Defence.*

Knowledge institutions working with the ABDO have highly robust risk management processes. For this reason, they can serve as a source of inspiration for knowledge institutions that might not be carrying out defence contracts but that would nevertheless like to strengthen their internal procedures and processes.

6.5 Security culture: Awareness and alertness

The creation of an open security culture within the organisation is essential with regard to awareness (incident and risk detection) and resilience. People should be able to discuss possible risks openly and in confidence, and they should be aware that internal safety procedures exist for a reason. Space should be allowed for expressing concerns and engaging in active consideration of possible improvements. This should not be something that is addressed solely by board members and the security coordinator.

Campaigns can make a useful contribution, particularly during the initial phase, when awareness is still limited. They can ensure that the message of these guidelines is conveyed in a way that suits the needs of the organisation. Awareness-raising should never be a one-off exercise: continuous attention is needed in order to keep everyone alert and to bring new staff members on board. Moreover, because knowledge security (and its consideration) is constantly changing, it is important to ensure that knowledge is kept current.

The input and expertise available within the central government and in organisations such as UNL and the TO2 Federation can be used for this purpose. For example, they can provide a platform for learning from experiences within other knowledge institutions and, possibly, for imitating useful tools and checklists.

Awareness-raising should never be a one-off exercise: continuous attention is needed in order to keep everyone alert and to bring new staff members on board

Any awareness-raising campaign should be customised to the intended goals and target groups (e.g. researchers, project managers, support services). They should correspond as closely as possible to their perceptions and realities. An effective campaign uses multiple channels and points of entry. Examples could include providing information through posts on the intranet, emails and e-learning modules, as well as through interactive meetings and team sessions. Simulations in which cases (real or fictitious) are played out are especially well-suited for training aspects of attitude and behaviour.

It is also useful to consider who is to convey the message within the organisation. One essential point in this regard is that managers should set a good example and demonstrate that they are convinced of the importance of knowledge security. In addition, 'ambassadors' could be appointed within the organisation to take an active role in the further dissemination of the message. Finally, briefings can be provided by the Dutch central government (e.g. OCW, EZK, BZ, NCTV, AIVD or MIVD, depending on the approach). Additional information is available from the National Contact Point for Knowledge Security.

Section 7

International partnerships, procurement and contracting

Agreements with foreign partners deserve special attention in the risk management systems of your institution. Setting up clear agreements up front can help mitigate risks and provide a solid base to fall back on in case things do go wrong. When it comes to procurement and contracting there are also important knowledge security related risks. There are measures that can be taken to mitigate these risks provided they are identified in time.

7.1 What to bear in mind when entering a collaboration

Collaboration with foreign institutions or companies can come about in various ways. A collaboration may arise informally through the personal contacts of researchers. Once substantive or financial commitments are made, however, it is important for the agreements to be documented in some form. One common means of concluding a partnership is through a Memorandum of Understanding (MoU). Collaboration can also take the form of a research assignment awarded to a knowledge institution by a foreign contractor.

Collaboration agreements provide a good starting point for considering opportunities and risks

For the purpose of this document, we are referring to all forms of collaboration, ranging from formal to informal, and from broad to specific. Collaboration agreements provide a good starting point for considering opportunities and risks. The conclusion or renewal of an agreement, as well as and the acceptance of new assignments, are particularly suited moments to perform analyses to help mitigate potential risks.

When an institution (or a part thereof) enters collaboration with a foreign institution or a foreign company, the priority should be to conduct a thorough investigation into with whom exactly the institution will be doing business. (see Section 5.3 ↗). Thereafter, it is important to make clear agreements, which prevent risks concerning knowledge security, academic core values and the unethical use of research results. This will ensure that there will always be recourse against any objectionable developments that might occur throughout the collaboration. The partner can then be called to account and, if the risks persist, the collaboration can be terminated prematurely (exit strategy).

Numerous existing formats and standard agreements for collaboration are currently in use. Your organisation most likely also makes use of such a standard template. These provide a certain level of basic protection against the most common legal and financial risks. However, such standard provisions may not suffice for a collaboration that concerns a sensitive domain with a partner from a country that has an increased risk profile. Such cases call for customisation, and it would be advisable to call in legal and security expertise. The organisation should ideally have a specific procedure in place for such situations (see also Section 6 ↗). In some cases, it might be necessary to conclude that no collaboration is possible, not even with a good contract. For example, if the residual risks would not be acceptable to the responsible party (in most cases, the Executive Board).

In some cases, it might be necessary to conclude that no collaboration is possible, not even with a good contract

The following are several questions that deserve close attention in all cases:

- Is there a clear and exact description of who the partners are? Are entities listed that are either unknown or whose involvement is unclear?
- Are the research areas or topics of collaboration clearly defined? This can help to prevent situations in which the partner's interest shifts to a sensitive domain during the course of the project.
- Who will be responsible for which expenses? For example, if the foreign party will be paying all the costs for personnel and research facilities, this creates a dependency. This could cause you to lose control ('the payer decides'), in addition to making it more difficult to cancel the agreement due to the severity of its implications.
- Is the agreement based on reciprocity? The accessibility and use of research data are particularly important in this regard. Provisions concerning confidentiality and secrecy, as well as on dissemination and publication should be considered as well.
- Is the collaboration subject to Dutch law? It is important to note that, in the Netherlands, core academic values (e.g. academic freedom and institutional autonomy) are guaranteed in the Dutch Higher Education and Research Act (WHW).
- One stipulation is that the research must be conducted in accordance with internationally accepted standards of scientific conduct, as laid down in national and international codes of conduct, such as the Netherlands Code of Conduct for Research Integrity (see Section 2.1 ↗).
- Does the agreement contain clearly formulated resolutive conditions? These provisions grant the right to terminate the collaboration prematurely if matters should arise that you deem unacceptable. A dispute-settlement provision is also desirable.
- Do you know the level of access desired by the partner? To which buildings, information or internal networks will the partner have access? What will be shared with the partner? Will access be granted to a complete product, or to a 'light' version without sensitivities?
- Does the collaboration involve dual-use technology (see Section 4.1 ↗)? If so, an end-user statement (EUS) is desirable. This is a document signed by the end-user, declaring that the goods will not be used other than for civilian purposes.

Once the contract has been concluded, the agreements that have been made will be decisive. This requires regular consultation with the collaboration partner, paying close attention to both substantive progress and the manner in which the collaboration is taking shape. Problems and incidents should be charted and addressed promptly. It is recommended to schedule periodic evaluations of the collaboration and to specify in advance the topics to be addressed in the evaluations.

Cooperation agreements often continue automatically after the initial term. If the collaboration has proceeded without major problems, there is a tendency not to pay attention to such moments for renewal. For collaborations involving increased risk (due to the field of expertise, the collaboration partner and/or the country in which the partner is based), this is undesirable. It is recommended to arrange the internal organisation to include a timely alert well in advance of the renewal date, in order to allow for a critical review of the agreement. Developments may have taken place since the initial agreement was concluded that require additional mitigation measures or stricter delineations.

7.2 Knowledge security in procurement and contracting

Some contracts are accompanied by security risks. This depends on the type of product or service, the client and the company to which the contract is awarded. For example, depending on these factors, there may be a risk that high-value or sensitive knowledge and information will be leaked, that vital business processes will be disrupted or that strategic dependencies will arise. Examples include the contracting out of digital infrastructure, cloud services and software or the replacement of systems that are used to store large amounts of personal data. In addition, some procurement assignments require physical access to sensitive locations, where it is appropriate to take protective measures.

When contracting out, it is therefore important to start by identifying the presence of any such risks. The National Security Quick Scan can help to identify risks in procurement and contracting[26]. Although this instrument was developed for the Dutch central government and the critical sectors, it can also provide inspiration for other sectors. The quick scan consists of several questions aimed at quickly determining whether a contract poses a risk to national security or whether further research is required in order to determine this. If the results of the quick scan indicate possible risks, a risk analysis must be performed. A risk analysis establishes exactly which risks are present and which actions can be taken to mitigate them. It is important to draw on both substantive expertise regarding the contract and legal (procurement law) expertise. This will allow measures to be taken under procurement law or in the actual contract (product/service).

The following questions serve as examples:

- Is the intended contractor equipped to handle the information needed to carry out the assignment?
- Does the contractor know what to do if security incidents occur, and do sub-contractors also meet the security requirements for the assignment?
- Could a collaboration or agreement with such a company create a strategic dependency?
- Could sensitive information (e.g. personal data) be leaked?
- Could the continuity of supply be jeopardised and, if so, what would the consequences be?
- Will staff members encounter sensitive information?
- What will be done with the information after the contract has expired?

Once an overview of the potential risks of a contract has been developed, measures can be taken. Examples include setting additional contract requirements or other measures aimed at risk management (see Section 6 ↗) and increasing digital resilience (Section 9 ↗).

Section 8

The role of human resources policy

Security awareness should be included in your human resources policy. The policy should also address aspects of attitude and behaviour: a general security awareness should be present and be felt within the workplace. The management and project managers are responsible for supervision, and they serve an exemplary function.

8.1 Security checks in recruitment and selection

It is important for an institution to ensure good cooperation and communication between the hiring party at the decentralised level (e.g. faculty) and the HR departments at the decentralised (e.g. faculty) and central levels regarding human resources policy. In addition to being responsible for a decent subject-specific match the hiring party should also be aware of any risks relating to knowledge security and take them into account during the application process, including during interviews.

In the recruitment and selection of new staff members, it is important for the HR department to emphasise the core academic values, as described in the Netherlands Code of Conduct for Research Integrity. This is because, in some countries, institutions are under the direct rule of the authorities, and principles like fairness, diligence, transparency, independence and accountability are not observed.

All HR staff members should be aware of security

All HR staff members should be aware of security. They are the first point of contact for new staff members, and they can identify signals in the CVs or networks of new staff members. For example, have they worked at institutions in countries that pose increased risk? Does a CV contain other unexplained gaps which the HR consultant could point out to the individuals conducting the interview? Does the candidate hold a visiting appointment abroad at a questionable institution or does the candidate have remarkable ancillary activities?

Depending on the nature of the risks, a Certificate of Good Conduct (VOG) may be required for certain positions. During the process of applying for a Certificate of Good Conduct, it will be possible to assess specific job aspects that are relevant to the work that the new staff member will be performing. It is important to note that a Certificate of Good Conduct covers a period of only four years, and only Dutch systems are consulted in the certification process. It therefore says very little about foreign researchers who have only recently arrived in the Netherlands. In some cases, comparable certificates issued by foreign countries can be helpful.

An integrity assessment can also be used for recruitment to determine whether:

1. the candidate's conduct is consistent with rules and generally applicable values, including when under pressure or when the rules are unclear;
2. the candidate is not guided by improper motives, but by the general interest, and is not likely to be tempted to fail to apply rules or interpret them too broadly;
3. the candidate's exhibits and takes responsibility for consistency in conduct.

It is also advisable to provide some form of 'aftercare' when staff members who have been working with sensitive knowledge or technology leave employment. Such care could consist of maintaining contact with the individual in question. The confidentiality provisions in the employment contract can also be formulated in such a way that they remain in force even after leaving employment.

8.2 Courses and training

It is important to ensure that everyone receives adequate training and/or information in order to recognise challenges relating to security and take appropriate action. For example:

- Including relevant information and regulations as standard elements in the welcome package and providing a (mandatory) module or briefing on knowledge security for new staff members, and possibly for students who will be working with sensitive knowledge/technology
- Offering refresher modules given at the start of new research projects, in order to maintain the required level of awareness amongst project members
- Setting up an intranet platform where staff members can find information and where they can test their knowledge and alertness (self-assessment)
- Setting up a special training programme for visiting researchers and students from countries with increased risk profiles, focusing on the core academic values

8.3 Foreign visitors and business trips abroad

Undesirable knowledge transfer can take place within the framework of multiannual research projects in which foreign researchers work in the Netherlands for extended periods of time. It can also occur through contacts of short duration through foreign visitors to the Netherlands, such as conference participants or visiting lecturers/researchers. Given that there is no employment relationship in these cases, pre-screening is not an option, and precautions should be aimed at limiting risks when visiting sensitive sites.

It is advisable to prepare a visitor protocol that describes how to deal with foreign visitors in general, and especially those from countries with increased risk profiles

It is advisable to prepare a visitor protocol that describes how to deal with foreign visitors in general, and especially those from countries with increased risk profiles. They could be researchers, but also representatives of companies or governments. Visitor policies are not useful unless they are accompanied by physical and digital measures to protect the sites.

Elements for a visitor protocol

- *Require all visitors and delegations from abroad to be registered in advance by the staff members who will be receiving them. Do not grant access without registration. In addition, require all visitors to identify themselves upon entry and be registered and met at the reception desk.*
- *Know where certain visitors are and are not allowed to roam, so that it can be assessed in advance whether a visit can occur in a certain area.*
- *Announce visits to sensitive areas to colleagues in advance, so that they can take this into account.*
- *Never leave your visitors alone (and especially not in sensitive areas). They should always be accompanied while on your premises.*
- *Clearly inform visitors that they are not allowed to take photographs or videos at the site without permission or ensure that all equipment in sensitive locations is stored away (e.g. in a safe).*
- *Determine in advance what is and is not to be shared with the visitor and steer all information-related discussions during the visit away from subjects related to the security of information security or sites.*
- *For highly sensitive investigations/places/sites, it is better not to receive visitors, or to exclude visitors from countries with increased risk profiles.*

It would also be wise to have a protocol in place for the reversed scenario, in which researchers from the Netherlands are visiting other countries for work. Careful preparation and alertness are particularly important for countries with increased risk profiles. This is particularly relevant if the researcher in question is conducting research in a field that is regarded as a 'crown jewel' within your institution (see Section 5.1 ↗) and that is therefore likely to be of interest to the host country.

This applies to a wide variety of situations. One example could be if you are invited as a keynote speaker and received in grand style (e.g. accommodations in a luxury hotel, lavish dinners). This could be a sign of genuine hospitality. In some countries, however, it could unfortunately also be a deliberate attempt by actors (who you might not even meet) to convince you to do something in return.

Elements for a protocol for business trips to countries with increased risk profiles

Prior to departure

- *Take only a minimum amount of confidential (or other) data with you on the trip.*
- *Decide in advance what will be contained on the data carriers that you will take. If files containing sensitive information are stored on your laptop but will not be needed during the trip, transfer these files to another computer before you leave, or take another laptop with you on the trip.*
- *The same applies to your mobile phone. Delete the call history before you leave or take a different phone on the trip.*
- *Use passwords and/or access codes on all devices and turn them off whenever possible. If a device is activated, you are particularly vulnerable.*

En route

- *Always disable the Bluetooth function on your phone and laptop.*
- *Always take confidential information and data carriers (e.g. USB sticks, smart phones) in your carry-on bag, and not in your checked luggage.*
- *Exercise caution when conducting confidential conversations on board of planes, trains or in other public spaces. For example, some airlines or other transport companies have close ties to intelligence and security services. The same could apply to other passengers.*

At the destination

- *Protect confidential information. Do not leave confidential data behind in places where they could be seen by others. The same applies to your hotel room or hotel safe.*
- *Never simply hand over your laptop or telephone to others, and always make sure that you are able to check whether someone has seen your information.*
- *Be selective in providing information. Apply the 'need-to-know' principle with your contacts. Do not tell your conversational partner any more than is absolutely necessary. The same applies to conferences or meetings to which you have been invited as a speaker.*
- *Exercise caution with any USB sticks received (for free) at conferences or events. This is an easy way to install malware on your laptop.*

For those working in highly sensitive domains of knowledge and/or who regularly travel to countries with increased risk profiles, it may be wise to take a Hostile Environment Awareness Training (HEAT) course or to request a travel briefing from the AIVD. This can be requested through the National Contact Point for Knowledge Security.

Section 9

Cyber security in relation to state-actor threats

Digital threats are increasing, due to the efforts of parties including state actors and professional criminals. This is a national problem in which Dutch knowledge institutions are also targets for cyber attacks using methods ranging from attempts to reveal information and phishing emails to DDoS (Denial of Service) and ransomware attacks. Given that knowledge institutions often purchase services from several large tech companies, cyber attacks on these service providers can lead to widespread outages. This section is intended to help institutions to raise awareness of cyber security and devote increasing attention to chain cooperation and the measures that institutions can take to increase their digital resilience. It also addresses how security policies within institutions can be further embedded in order to ensure optimal organisational performance, as well as continuity of education, research and knowledge sharing while guaranteeing the integrity and confidentiality of the data available within the sector.

9.1 Threats and risks

Ransomware attacks account for the majority of reported cyber attacks in knowledge institutions. They are known for their specific working method of forcing the target to pay the requested ransom. These attacks differ from sabotage or espionage, in which malicious parties actively try to evade detection in order to achieve their goals. The SURF Cyber Threat Assessment provides a good overview of the threats that are manifesting themselves in higher education and research, along with their impact.

The greatest threat to most organisations in the Netherlands comes from state and criminal actors

Perpetrators could have different backgrounds and motives. The greatest threat to most organisations in the Netherlands comes from state and criminal actors. This certainly also applies to knowledge institutions. Spying provides countries with a relatively accessible manner of obtaining knowledge. The motives are often political, military or economic. Coordinated cyber attacks on knowledge institutions are often carried out by known Advanced Persistent Threat (APT) groups from or sponsored by particular states. They have sophisticated skills in employing a range of tactics and techniques to gain access to targeted digital infrastructure and intellectual property. They are persistent in carrying out operations that may be covert or go unnoticed for long periods in order to achieve their objectives. They pose a threat because they have the ability and intent to exploit the vulnerabilities of their targets. Such attacks may involve known or unknown vulnerabilities in the technical and support infrastructure of knowledge institutions. Targets can also include people visiting, studying or working at knowledge institutions.

Cyber attacks are also used by states as a means of disseminating disinformation. The mixing of reliable information with disinformation or the manipulation of information can raise doubts about certain issues.

In addition to potential threats from cyber actors, other causes may also result in digital risks. Examples include hardware failures, technical failures of components in the infrastructure, electricity failures, floods or fires. It is important to take also these possibilities into account.

Knowledge institutions could also be affected by digital risks posed by organisations with which they collaborate or from which they purchase services, hardware or software. Numerous examples have occurred, including those in which the services of other, often globally operating, companies have been manipulated in ways that allowed actors to access the infrastructure of other organisations as well. In addition, actors frequently exploit known or unknown vulnerabilities in commonly used products (e.g. the abuse of vulnerabilities in cloud services and mail servers for email traffic). Conversely, digital processes/ systems can be attractive as steppingstones to other 'targets'. Examples could include access to members of the opposition or dissidents from certain countries who are studying or pursuing a PhD at university and who may be conducting research that is sensitive for those countries. These countries could aim their digital arrows at these people, i.e. through student information.

In its 'Cybersecuritybeeld Nederland 2021' (Netherlands Cyber Security Assessment), the National Coordinator for Security and Counterterrorism (NCTV) recognises four risks to national security:

1. Unauthorised access to information (and, possibly, the publication thereof), particularly through espionage or data leaks
2. Inaccessibility of processes due to sabotage or the deployment of ransomware (or preparation for such activities)
3. Violation of digital space or the security thereof (e.g. through the abuse of global IT supply chains)
4. Large-scale outage: a situation in which one or more processes have been disrupted due to natural or technical causes, or due to non-intentional human action

The Netherlands Cyber Security Assessment also draws attention to the publication entitled Handreiking Cybersecurity Maatregelen- Stap voor stap naar een digitaal veilige organisatie [Manual of cyber security measures: Step by step towards a digitally secure organisation] [27], which lists basic measures that should be arranged in order to achieve a minimum level of digital security. These basic measures correspond to points for improvement emerging from various evaluations of incidents, as well as to the investments that some institutions have either already made or are planning to make. According to the National Cyber Security Centre (NCSC), these eight basic measures are the minimum required to protect against current digital threats. It is therefore important for your institution to apply these basic rules as much as possible, in addition to reporting them in the annual report. Your institution can discuss ways in which it can carefully apply these basic measures with other organisations, such as VH, UNL, KNAW, NWO, NFU and the TO2 Federation, within the framework of implementing risk management. It is also important to consider the diversity and differences in risk profiles between institutions.

Basic Cyber Security Measures

1. *Ensure that every application and every system generates sufficient log information.*
2. *Apply multifactor authentication as needed.*
3. *Determine who is to have access to your data and services.*
4. *Divide networks into segments.*
5. *Encrypt storage media containing sensitive operational information.*
6. *Check which devices and services can be accessed from the internet and protect them.*
7. *Make regular back-ups of your systems and test them.*
8. *Install software updates.*

9.2 Scope for action: What can you do?

What should be in place at the institutional level? Which processes and procedures should there be? How can you ensure that everyone is familiar with them? How can everyone contribute individually? How can you ensure sufficient 'digital hygiene'? Where is there a particular need for cooperation and sharing of knowledge and information?

To reduce the risk of a cyber attack, it is important to help students and staff members to develop safe behaviour and for institutions to take the necessary measures to this end

a. Awareness-raising

Human behaviour can override technical and procedural measures. The greatest primary cause of reported safety incidents is ignorance and incorrect action by people. People are thus also an important factor in cyber security. To reduce the risk of a cyber attack, it is important to help students and staff members to develop safe behaviour and for institutions to take the necessary measures to this end.

The following are examples of measures that your institution can take to raise awareness at the institutional level, as well as amongst students and staff members:

- Use a variety of communication channels (e.g. newsletters, special intranet pages, infographics and vlogs by experts and board members). Publish regular news items on best practices that describe cyber-security incidents, including items containing suggestions for behaviour and action;
- Develop educational programmes, training and recurring information sessions for researchers, students and administrative and support staff on the topics of cyber hygiene, risk identification and how to avoid or cope with such risks. This can also be done using physical and digital campaign activities (e.g. Cybersave Yourself by SURF[28]);
- Implement e-learning tools for students and staff members (e.g. the SURF Digital Privacy and Security Certificate);
- Participate in cyber-crisis exercices (e.g. OZON at SURF[29]).

b. Risk management and administrative and strategic attention

Which agreements do you make within your institution and with external stakeholders in order to optimise the performance of the organisation, the continuity of education, research and knowledge sharing, and to ensure the integrity and confidentiality of the data available within the sector?

Cyber criminals are becoming increasingly aware of the organisations that they wish to attack, and they are targeting specific officials within these organisations

It is crucial for knowledge institutions to be as well prepared as possible for a cyber attack. Cyber criminals are becoming increasingly aware of the organisations that they wish to attack, and they are targeting specific officials within these organisations. It is therefore important for institutions to continue to pay attention to security at board and strategic levels and to implement measures to detect and monitor possible attacks, in addition to raising awareness. The careful organisation of risk management is necessary in order to understand the risks and take appropriate measures to mitigate them in a cost-effective manner. This calls for sound governance and strategic positioning of security risk management within your institution. Concrete examples include incorporating security policy into your institution's annual reports, long-term vision and strategic plans and ensuring the structural discussion of this topic within the Supervisory Boards.

In addition to the basic measures proposed by the National Cyber Security Centre, your institution could consider the following technical and organisational measures to enhance security against risks:

- Join an Emergency Response Team (CERT) like SURFcert, in which member institutions receive 24/7 support in the event of a security incident. SURFcert is in direct contact with the National Cyber Security Centre (NCSC), as an affiliate of the Landelijk Dekkend Stelsel (national coverage system, or LDS). This is a system in which public and private parties exchange knowledge and information with each other. Affiliates include the CERTs, as well as sector and regional partnerships, the NCSC and the Digital Trust Center (DTC). The NCSC serves as a central information hub within the LDS.
- Join a Security Operations Centre (SOC) solution (e.g. SURFsoc), thereby ensuring 24/7 monitoring and threat detection for your networks. Continuous monitoring will make a major contribution to improving information security within your institution, as information is constantly gathered and quickly shared across the sector in the event of a potential threat.
- A shared framework of standards and an adequate system of prevention and response is necessary to establishing a proper system of risk management within your organisation. For example, a large proportion of higher education institutions use the framework of standards for information security in higher education. An assessment framework that complements the framework of standards then describes the requirements for meeting a particular level of maturity.
- Perform structural internal and/or external audits that generate greater insight into the extent to which your institution is in control of information security and identify priorities for improvement.

- To gain insight into the threat of cyber attacks and practical tips for recognising and preventing an attack, you could consult the AIVD and MIVD publication entitled 'Cyber-attacks by state actors' [30] on the seven moments at which you can stop a cyber attack by a state actor.

c. Attention to chain cooperation

Numerous international partnerships exist between academic and knowledge institutions, within which legitimate knowledge transfer takes place. Nevertheless, knowledge can inadvertently leak out due to cyber attacks and access to systems and files.

Because academic and knowledge institutions generate unique, high-quality knowledge and process personal data, they are popular targets for malicious actors. Effective efforts to combat cyber risks therefore depend on cooperation and the continuous sharing of knowledge and information about risks. For example, the SURF security community's SURFnet Community of Incident Response Teams (SCIRT) and the SURF Community for Information Security and PRivacy (SCIPR) provide a good platform where operational security experts from knowledge institutions can learn and share knowledge with colleagues. In doing so, they contribute to the professionalisation of information security within these institutions.

SURF is also affiliated with the national coverage system (LDS) on behalf of the education and research sector. The LDS is a system in which public and private parties exchange knowledge and information with each other and with which the NCSC can share information on vulnerabilities and threats. Affiliates include CERTs, sector and regional partnerships (OKKTs) and the Digital Trust Center (DTC).

Overview of contact information and sources

Contact details

National Contact Point for Knowledge Security (Dutch Central Government)
Telephone: 088-0424242
E-mail: info@loketkennisveiligheid.nl
Website: www.loketkennisveiligheid.nl

Export control - Central Import and Export Office (CDIU)
Telephone: 088 - 151 21 22
Website: https://www.belastingdienst.nl/wps/wcm/connect/bldcontenten/belastingdienst/customs/safety_health_economy_and_environment/cdiu_cluster/
Application form for request for classification [in Dutch]:
https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/programmas_en_formulieren/aanvraag_indelingsverzoek

Sources

S1: Introduction

1 Letter to Parliament on Knowledge Security in Higher Education and Research (2020): https://www.government.nl/documents/letters/2020/11/27/knowledge-security-in-higher-education-and-research

S2: Protecting core academic values

2 Netherlands Code of Conduct for Research Integrity: https://www.universiteitenvannederland.nl/en_GB/research-integrity
3 European Code of Conduct for Research Integrity: https://allea.org/code-of-conduct/
4 National action plan for greater diversity and inclusion (2020): https://www.nwo.nl/en/netherlands-code-conduct-research-integrity

S4: Legal frameworks and codes of conduct

5 EU dual-use regulation (2021): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0821&qid=1632830707418
6 Dutch Central Government factsheet on export via the cloud (2018): https://www.government.nl/documents/leaflets/2018/07/01/factsheet-export-via-the-cloud
7 Technology Readiness Level (TRL) Assessment Tool: https://www.ic.gc.ca/eic/site/099.nsf/vwapj/TRL-e.pdf/$file/TRL-e.pdf
8 EU Commission Recommendation on internal compliance programmes for dual-use trade controls (2019): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019H1318&rid=8
9 CDIU Aanvraagformulier indelingsverzoek [available only in Dutch]: https://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/themaoverstijgend/programmas_en_formulieren/aanvraag_indelingsverzoek
10 National Institute for Public Health and the Environment (RIVM) Biosecurity Office: https://www.bureaubiosecurity.nl/en
11 EU Council Regulation concerning restrictive measures against Iran: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02012R0267-20210731#M39-1
12 Dutch Central Government list of disciplines subject to enhanced supervision: https://www.government.nl/topics/secondary-vocational-education-mbo-and-higher-education/exemption-certain-engineering-or-nuclear-related-courses-of-study
13 Letter to parliament on Knowledge Security in Higher Education and Research (2020): https://www.government.nl/documents/letters/2020/11/27/knowledge-security-in-higher-education-and-research
14 UNL Knowledge Security Framework for universities: https://www.universiteitenvannederland.nl/en_GB/news-items.html/nieuwsbericht/766-universiteiten-presenteren-kader-knowledgesecurity
15 European Union guidelines on Tackling R&I foreign interference (2022): https://ec.europa.eu/info/files/tackling-ri-foreign-interference
16 Guidelines Australia: https://www.dese.gov.au/guidelines-counter-foreign-interference-australian-university-sector
17 Guidelines Germany: https://www.hrk.de/positionen/beschluss/detail/leitlinien-und-standards-in-der-internationalen-hochschulkooperation/
18 Guidelines United Kingdom: https://www.universitiesuk.ac.uk/what-we-do/policy-and-research/publications/managing-risks-internationalisation
19 Guidelines Sweden: https://www.stint.se/wp-content/uploads/2020/02/STINT_Responsible_Internationalisation
20 Guidelines Canada: https://www.ic.gc.ca/eic/site/063.nsf/eng/h_97955.html

S5: Risk assessment

21 NCTV/AIVD/MIVD Dreigingsbeeld Statelijke Actoren 2021 [State actor threat assessment; available only in Dutch] https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren
22 AIVD Annual Reports: https://english.aivd.nl/publications?keyword=annual+reports&start-date=&end-date=&element=All+elements&type=All+publications
23 MIVD Annual Reports: https://english.defensie.nl/downloads?keyword=annual+report&start-date=&end-date=&topic=All+topics&element=All+elements&type=All+downloads
24 ASPI China Defense Universities Tracker: https://unitracker.aspi.org.au

S6: Risk Management

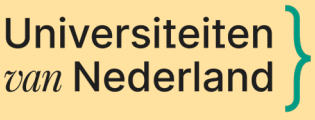
25 MIVD General Security Requirements for Defence Contracts (ABDO) (2019): https://www.defensie.nl/downloads/beleidsnota-s/2020/02/04/abdo-2019-english

S7: International partnerships, procurement and contracting

26 Quickscan nationale veiligheid bij inkoop en aanbesteden [available only in Dutch] https://www.pianoo.nl/nl/document/16908/quickscan-nationale-veiligheid-bij-inkoop-en-aanbesteden

S9: Cyber security in relation to state-actor threats

27 National Cyber Security Centre, Handreiking Cybersecurity-maatregelen (2021) [Guidelines for cyber security measures; available only in Dutch]: https://www.ncsc.nl/documenten/publicaties/2021/juni/28/handreiking-cybersecuritymaatregelen
28 SURF, Cyber security awareness toolkit: 'Cybersave yourself': https://www.surf.nl/en/cybersave-yourself-make-employees-and-students-aware-of-the-dangers-of-the-internet
29 SURF Whitepaper https://www.surf.nl/en/ozon-practice-how-to-respond-to-a-cyber-crisis/whitepaper-cyber-crisis-exercise-ozon
30 AIVD/MIVD Cyber attacks by state-actors (2021): https://english.aivd.nl/publications/publications/2021/11/29/cyber-attacks-by-state-actors-seven-moments-to-stop-an-attack


Universiteiten
van Nederland


KNAW


Vereniging
Hogescholen


NFU


TO2 federatie


Rijksoverheid


NWO