Ministerie van Onderwijs, Cultuur en Wetenschap

>Return address P.O. Box 16375 2500 BJ The Hague

The President of the House of Representatives P.O. Box 20018
2500 EA The Hague

Higher Education and Student Grants and Loans Rijnstraat 50
The Hague
P.O. Box 16375
2 5 00 BJ The Hague
www.rijksoverheid.nl

Our reference
3 1 177117

Annexes
2

Date 31 January 2022

Subject Progress and a preview of the action plan for knowledge security in higher education and science

Collaboration in higher education and science at an international level is crucial. World class excellent research simply cannot do without. At the same time, we recognize that knowledge institutions are faced with a range of threats from state actors. Knowledge security thus encompasses various aspects. Knowledge and technology may unintentionally be leaked and used in ways that compromise our national security or is at odds with what we in the Netherlands consider ethical. Also covert influence by state actors may take place within knowledge institutions which compromises academic freedom and scientific integrity.

Knowledge security therefore requires a robust approach with core values such as academic freedom and scientific integrity as guiding principles. Proportionality and tailored supervision are key ('open where possible, protected where necessary'). It is crucial that Dutch knowledge institutions continue to collaborate on an international basis with foreign knowledge institutions and companies and that transparency is the norm; at the same time it is also essential that the collaboration itself is secure.

In the letter to Parliament on knowledge security in higher education and science of November 2020 (hereinafter: letter to Parliament on knowledge security)[1] the government set out a coherent package of measures to systematically increase knowledge security in the Netherlands. The action plan is country neutral, which is to say that it can be applied to any state actor posing a threat. Since then both the government and the knowledge community have taken the necessary steps. The topic is firmly on the agenda, awareness has increased. Both the central government and the sector itself feel a sense of urgency to take action together.

This letter aims to inform your Parliament about the progress made on the implementation of the measures announced in the Letter to Parliament on knowledge security.

[1] Letter to Parliament dated 27 November 2020 (link)

1. Threat assessment in relation to Dutch knowledge institutions

Over the past year, time and effort has been spent to assess in greater detail the threats and risks that the Dutch knowledge sector faces. For that reason, the State actor threat assessment (*Dreigingsbeeld Statelijke Actoren*, DBSA) by the AIVD, MIVD and NCTV of February 2021[2] and the 2020 annual AIVD report and the MIVD report of April 2021[3] have also addressed this issue. They show that there has not yet been a decrease of the threat touched upon in the Letter to Parliament on knowledge security, explained briefly in more detail below.

Various state actors are in fact actively seeking knowledge and technology in the Netherlands with the intention of increasing their own military, technological, political and economic power. In the Letter to Parliament on knowledge security, the government describes some of the current methods used by state actors against knowledge institutions, including 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 the DBSA, the AIVD, MIVD and NCTV warn of structural and centralized activities by certain state actors, that could compromise Dutch interests. The picture that emerges is that institutions of higher education and science are targets for influence, interference and unwanted knowledge transfer.

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 purposes). In addition, our country's ability to innovate may be compromised by the unwanted transfer of sensitive knowledge, technology and intellectual property to other countries. The Netherlands must also keep to the sanctions imposed by the UN and EU as regards Iran and North Korea.

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, 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 state actors monitor their citizens to prevent them voicing disagreeable opinions about their homeland. 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 (e.g. freedom of expression) and core values (e.g. academic freedom and research integrity).

The National Knowledge Security Guidelines published today (see below, section 2.2) looks in more detail at the intentions and methods used by state actors and provides the knowledge institutions with a scope for action on how to handle these challenges.

2. Enhanced self-regulation within the knowledge sector

[2] State actor threat assessment dated 3 February 2021 (link)
[3] 2020 Annual Report AIVD (link) and 2020 Annual Report MIVD (link)

The knowledge sector is characterized by a high degree of autonomy. When it comes to knowledge security, institutions make a risk assessment and organize their internal policy themselves based on existing legal frameworks, codes of conduct and guidelines. The government advises and assists these institutions. The measures announced by the government in the Letter to Parliament on knowledge security are intended to help the knowledge sector strengthen its self-regulatory activities and, where necessary, develop frameworks. We have described the progress made for each measure below and take a look ahead to the coming period.

2.1 Knowledge security dialogue

The knowledge security dialogue commenced in the second half of 2020: a series of talks at board level held between the central government and almost all knowledge institutions in the Netherlands.

In that context, the Ministry of Education, Culture and Science, in collaboration with the NCTV and the AIVD, held talks with the Universities of the Netherlands (UNL) and its fourteen affiliated universities, with the Royal Netherlands Academy of Arts and Sciences (KNAW) and the Dutch Research Council (NWO) and its nineteen affiliated research institutes and with the Dutch Federation of University Medical Centres (NFU) and its seven affiliated university medical centres. Talks were also held with the Netherlands Association of Universities of Applied Sciences (VH) and a selection of twelve universities of applied sciences.
In addition, the Ministry of Economic Affairs and Climate Policy organized administrative and technical workshops for the five institutions for applied research (the TO2 institutions TNO, Marin, NLR, Deltares and Wageningen Research) and Wetsus. A follow-up series of in-depth thematic sessions were then organized.

The general picture that emerges is that there is a varying degree of awareness in the sector. Those differences can for the larger part be explained by the differences in the institutions' risk profiles. Governors of knowledge institutions generally share the sense of urgency about knowledge security and are prepared to assume responsibility and take measures. For example, the universities have developed a joint knowledge security framework[4] and have appointed administrative initiators of knowledge security, both the UNL and NWO have set up work groups for knowledge security to promote learning from one another and awareness campaigns are being held.

The knowledge security dialogue has already contributed to security awareness at board level within the knowledge institutions. At the same time, the series of talks have shown the government what else knowledge institutions are in need of and where further steps are required. The governing boards of knowledge institutions reported that they need a clear framework from the government and a national contact point for information and advice.[5] Those experiences have been included in the development and elaboration of the policy measures.

It is the express intention to continue the dialogue and to prevent it from being a one-off round of talks. The ultimate goal is to ensure that knowledge security permeates through all parts of the knowledge institutions. We will consult with the stakeholders involved (VH, UNL, KNAW, NWO, NFU and the federation of applied research organizations (TO2-federatie)) this Spring to discuss which additional steps to take in that direction.

[4] 'Knowledge security framework for universities', Universities of the Netherlands (link)
[5] These points were also made at the round table talks about scientific collaboration with non-free countries held on 14 October 2021 in the House of Representatives

2.2 National Knowledge Security Guidelines

The Dutch knowledge sector and the Dutch central government have worked together over the past months to produce the National Knowledge Security Guidelines, formally published today. The stakeholders in the field (VH, UNL, KNAW, NWO, NFU and the federation of applied research organizations (TO2-federatie)) and various central government ministries and services contributed to its creation.

These guidelines are a national reference document for both the governors of knowledge institutions and researchers as well as the government for all aspects of knowledge security. The guidelines are intended to help knowledge institutions and researchers on their way, by pointing out the risks and threats and thereby outlining frameworks and possible courses of action. It provides a basis to the governing boards of knowledge institutions to define or redefine their institutional policy. Thus the guidelines contribute both to awareness and resilience of the knowledge sector.

The guidelines are also an important source document for the National Contact Point for Knowledge Security (see below, section 2.4). The National Knowledge Security Guidelines will play a major role in the awareness campaigns and board-level talks about knowledge security. The guidelines are translated into English so that they can be used in an international context as well. The guidelines will be updated whenever developments in the threat assessment and/or policy developments of knowledge security so demand.

2.3 Administrative agreements on knowledge security

All measures announced in the letter to the Parliament on knowledge security stand or fall with cooperation. Active cooperation with and full commitment by the stakeholders in the field of for higher education and research as well as all involved sections of central government is absolutely key. To that end the Ministry of Education, Culture and Science set up a collaborative structure at the beginning of this year consisting of regular meetings between all involved parties both at board level and at technical level. In addition to developing measures collectively, an important objective
of this structure is the discussion of their follow-up.

In the context of that collaborative structure, the stakeholders in the field and the central government have voiced their commitment to each other and made agreements in the past . The stakeholders contributed actively to the National Knowledge Security Guidelines and committed themselves to the document's contents. They will work on the organization-specific implementation of the guidelines, taking into account their particular characteristics and basic principles. The central government's contribution is to share information and expertise, for example through the National Contact Point for Knowledge Security (see below) and by offering tools and setting frameworks. Progress can be monitored and - where necessary - adjusted through the aforementioned collaborative structures.

2.4 National Contact Point for Knowledge Security

Knowledge institutions indicated that they need information and advice from the central government in weighing the opportunities and risks of international cooperation. The National Contact Point for Knowledge Security[6] , officially launched today, aims to meet that need. The contact point is intended to be an accessible central point of contact for knowledge institutions, where they can ask their questions related to knowledge security. That includes questions about accepting foreign PhD students and about

[6] www.loketkennisveiligheid.nl The current basic website will be expanded in the coming months

forming inter-institutional partnerships with foreign knowledge institutions and companies. The contact point functions as an interdepartmental centre of national government. It is comprised of representatives from various ministries. The central government shares information and offers advice but the knowledge institutions retain responsibility, in line with their institutional autonomy.

After the exploratory phase early in 2021, the Netherlands Enterprise Agency (RVO) was asked to conduct a quick survey among the knowledge institutions to obtain as clear a practical picture as possible of the knowledge institutions' wishes and needs. Annexed to this letter you will find their end report.

The survey showed that there is a need for information and advice about various themes such as IT/cyber, collaborations with foreign institutions and admission of foreign PhD students and researchers. There is a need for general information but also specific information relating to countries and fields of expertise and the opportunity to brainstorm about ambiguous cases. The RVO's advice therefore is to emphasize that the contact point helps to answer questions about various third countries and a wide range of themes concerning knowledge security. The contact point's staff must be interlocuters with real expertise and should not simply refer cases. The outcomes are used to determine the scope and working method of the contact point.

After the summer the RVO was asked to set up the contact point's front office where questions come in and, where possible, to answer them directly. The back office consists of experts from the ministries and services involved: OCW, EZK, BZ, LNV, NCTV, AIVD and MIVD. Other central government sections can be brought in on an *ad hoc* basis. The aim is to provide fast substantive responses to the queries submitted by the knowledge institutions.

The basic functions of the contact point are now operational. Work on an independent website is still ongoing and the website is expected to go live this Spring. The starting phase is being used to gain experience on the job as it were. A first review is scheduled for June of this year, which will include the responses and experiences of all parties involved (front office, back office and field parties). After the summer 2022, the contact point will be developed in more detail to include things as active and proactive sharing of knowledge, the development of practical tools and training modules, and arranging awareness activities and providing support for this.

3. Screening Framework for undesirable Transfer of Knowledge and Technology

3.1 Assessing individuals

Where the risks to national security are greatest, far-reaching measures are necessary and self-regulation is insufficient. As announced in the Letter to Parliament on knowledge security, the government is working on a screening framework to prevent unwanted transfer of knowledge and technology. This involves the screening of individuals who want access to those areas of knowledge where the risks to national security are greatest - the risk domains. One example is knowledge that can be used for both civilian and military purposes (dual-use). This measure is being developed from various viewpoints.

Existing legislation and processes are being looked at, such as Enhanced Supervision[7] and experiences of other countries such as the United Kingdom[8], France[9] and Germany[10]. Paramount is that the screening framework is legally tenable and that the non-discrimination principle is upheld.

One fundamental question when working out a legal basis is whether everyone is to be screened regardless of nationality or that the screening will only apply to third-country nationals. From the perspective of proportionality and based on the current threat analyses, the government is examining a version in which the knowledge security check applies only to third-country nationals, citizens from outside the EU. That means that third-country nationals looking to gain admission to a risk domain at a Dutch knowledge institution must first undergo a knowledge security screening.

A second fundamental question is how to define the risk domains to which the screening framework is to apply. Which knowledge and technology is considered high risk from a national security perspective? That question also plays a role in other policy instruments, such as export controls[11] and the legislative bill for the investment assessment[12].

Given the fact that in terms of content, the means of defining sensitive technologies for the investment assessment is similar to the means of defining risk domains for the screening framework, the government will in principle run both processes in parallel. That contributes to synergy between the tools and consistency of policy.

The intended result of that process is a list of risk domains that are confirmed politically and updated when necessary. The government will include the knowledge community when drawing up the list and when translating it to the sections of the individual knowledge institutions.

While the legal basis is being worked out in more detail and the risk domains are being defined, a start will be made to develop various forms of implementation. A screening unit will be set up to handle the assessment applications and aspects of supervision and enforcement will also be addressed. That includes an implementation test and impact assessment which also looks at the impact on the knowledge community.

As announced in the letter to Parliament on knowledge security, the screening framework will realistically become operational in 2023 at the earliest. That is still the government's striving given the complexity and scope of the measure. The government underlines the importance of due care and support from the Dutch knowledge institutions.

3.2 Screening of cooperation agreements

Cooperative partnerships by Dutch knowledge institutions with foreign knowledge institutions or companies may entail risks for national

[7] The government last informed your House on Enhanced Supervision as part of current sanction regimes against North Korea and Iran by letter of 9 July 2021 (link). The assessment framework intends to replace that Enhanced Supervision.
[8] See https://www.gov.uk/guidance/academic-technology-approval-scheme
[9] See http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/
[10] See https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_awareness_academia.html
[11] Export control strategic goods (link)
[12] Security test for investment, mergers and acquisitions (Vifo) bill submitted on 30-06-2021 (link)

security. It is important that these risks are mitigated as much as possible in the underlying cooperative and funding agreements.

Previous studies[13] have shown that knowledge institutions do not always have a complete picture of the cooperation agreements entered into in the name of their institution or of sections of their institution. The National Knowledge Security Guidelines (see section 2.2) state that a governing board of a knowledge institution should always know about the significant collaborations the organization enters into, without having to consult the parties involved within the organization. The guidelines also describe the aspects the knowledge institutions must address when entering into cooperative partnerships.

The government is therefore repeating its previous call[14] to knowledge institutions to re-examine their existing cooperation agreements with foreign partners (knowledge institutions or companies) and to check whether fundamental values are adequately guaranteed. If that is not the case, it is advisable to review the respective agreements. In some cases, knowledge institutions can contact the National Contact Point for Knowledge Security (see section 2.4) for information and advice.

In the course of the year we will review whether additional measures are necessary, besides this form of enhanced self-regulation, in order to mitigate risks.

4. Developments in partner countries and the EU

Knowledge has no boundaries and higher education and science have a strong international focus. As the government wrote in the letter to Parliament on knowledge security, the approach can only be effective if we work together with our international partners. That certainly is the case within the EU, where there is a common area of research and education and freedom of movement.

Against that background, the government has invested in an international network to learn from the approach taken by other countries and to work together in the international context. Consideration is given to key EU and international partners such as Germany, France, the United Kingdom, Australia and the United States of America. The international talks are inspiring and provide an understanding of what works and what does not.

Within the EU important steps have been taken to put knowledge security on the agenda. On 19 May 2021, the European Commission presented its communication 'Global approach to research and innovation'[15] which includes many elements from the national government's approach to knowledge security.
The Council of the EU endorsed these principles through Council Conclusions that were adopted by the Competitiveness Council.[16] Thus there is common ground on which to take further steps at EU level.

The European Commission recently published its Guidelines on tackling foreign interference in R&I,[17] with the purpose of encouraging member states and the European knowledge sector to develop similar guidelines themselves. The National Knowledge Security Guidelines presented today is consistent with that.

[13] Report "Exploring scientific collaboration in Dutch and Chinese knowledge institutions", 2020 (link)
[14] Letter to Parliament "Collaboration with China in the field of education and science" of 18/12/2020 (link)
[15] See the following link for the BNC file on this notification (link)
[16] Competitiveness Council conclusions dated 28 September 2020 (link)
[17] See https://ec.europa.eu/info/files/tackling-ri-foreign-interference

Finally, the European Commission issued the communication 'European strategy for universities'.[18] That communication looks in more detail at international cooperation in higher education and the importance of safeguarding values such as academic freedom. Your Parliament will be informed separately on this via the regular BNC process.

The Netherlands will continue to pursue knowledge security in the EU and further afield. In terms of the EU, the Netherlands will specifically focus on setting the agenda both for the member states and the European Commission. The Netherlands could take a more active role with likeminded countries in the EU in furthering the debate and ensuring that other countries also take steps to better safeguard knowledge security. The education and science attachés and the innovation attachés at the Dutch embassies could play a key role in expanding and utilizing the international network and the exchange of information with international partners.

The EU-efforts of this government are mainly directed at the following:
- actively setting the agenda for knowledge security at EU level;
- increasing awareness on knowledge security among EU member states and the European knowledge community;
- making specific agreements, with respect for the competences, and setting up forms of cooperation at EU level on knowledge security;
- mutual sharing of knowledge and experience and seeking commitment within the EU collectively and bilaterally.

5. In conclusion

Since the government announced its action plan for knowledge security in November 2020, much has been undertaken both by the knowledge sector and the central government. Security awareness has unmistakeably increased and there is now a broadly supported sense of urgency for knowledge security. Both the central government and the knowledge institutions have launched initiatives to increase the scope for action. That in turn has increased resilience.

Concomitantly, that does not mean we can become complacent as regular incidents remind us of the hard fact that we are not there yet. Therefore important steps still need to be taken. The Guidelines presented today will be converted by the knowledge institutions into internal procedures and processes. The goal is to incorporate the guidelines into practice. Only then can security awareness pervade the very fabric of the knowledge institutions.
The National Contact Point for Knowledge Security opened today will rapidly have to develop into an accessible and effective information desk for knowledge institutions. The dialogue with the knowledge institutions will be continued next year and the announced assessment framework will, in time, safeguard knowledge security in cases where self-regulation does not suffice.
This government will continue its commitment and work with likeminded countries both bilaterally and at EU level.

These efforts by the government and the knowledge sector combined must ensure that international cooperation in higher education and research can take place safely, taking into account both the opportunities

[18] See https://education.ec.europa.eu/document/commission-communication-on-a-european-strategy-for-universities

and the risks, and where academic values such as academic freedom are always safeguarded.

The government will inform your Parliament in more detail about progress in its presentation of the proposals for the screening framework, anticipated at the end of this year.

The Minister of Education, Culture and Science,

Robbert Dijkgraaf

The Minister of Economic Affairs and Climate Policy

Micky Adriaansens

The Minister of Justice and Security

Dilan Yeşilgöz-Zegerius