Awti Advisory council for science, technology and innovation

# KNOWLEDGE IN CONFLICT

## STRIKING A BALANCE BETWEEN SECURITY AND LIBERTY

Awti Advisory council for science, technology and innovation

The Dutch Advisory Council for Science, Technology and Innovation (AWTI) publishes solicited and unsolicited advisory reports to the Dutch government. Its independent reports are strategic in nature and focus on the contours of government science, technology and innovation policy. Council members are drawn from knowledge institutes and the business world. AWTI's work is founded on the principle that knowledge, science and innovation are vital for the economy and society, and will become more important in the future.

The Council is made up of the following members:

Dr. E.E.W. (Eppo) Bruins (Chair)
Dr. Ir. S. (Sjoukje) Heimovaara (Vice-chair)
Dr. Ir. J.P.H. (Jos) Benschop
Prof. K. (Koenraad) Debackere
Prof. E.H.M. (Ellen) Moors
C. (Chokri) Mousaoui
Dr. h.c. M. (Marleen) Stikker
P.W.J. (Patrick) Essers (Secretary)

The office is located at:

Prins Willem-Alexanderhof 20
2595 BE Den Haag
t. +31(0)70 3110920
e. secretariaat@awti.nl
w. http://english.awti.nl

# Knowledge in conflict

Striking a balance between security and liberty

November 2022

| | |
|---|---|
| Photography | Capuski, via iStock |
| Design | 2D3D Design; Kate Snow Design |
| Printing | Quantes |
| | November 2022 |
| ISBN | 978-90-77005-92-7 |

All publications may be downloaded free of charge from www.awti.nl.

## Copyright

All rights reserved. Subject to the inclusion of a correct, specific source reference, this publication or parts thereof may be reproduced, stored or made public without the prior written consent of AWTI. A correct source reference must as a minimum state clearly the name of the organisation as well as the name and year of the publication.

# Contents

# Summary

The combination of geopolitical, technological, and societal trends is making international collaboration between knowledge institutes increasingly complex. The rewards are many, but there are risks, too. Governments and knowledge institutes have taken a number of steps in recent years to mitigate these risks. While these steps have been useful, the rapid pace of developments constantly throws up new challenges. Against this backdrop, in this report the Dutch Advisory Council for Science, Technology and Innovation (AWTI) addresses the following question:

**How can the Netherlands best deal with the risks associated with international collaboration in building knowledge at Dutch knowledge institutes, including in higher education?**

The focus of the analysis and advice set out in this report is on wholly or partly publicly funded knowledge institutes in the Netherlands, including higher education institutions, and their immediate ecosystem of funding, regulation, and impact. The essence of our analysis is that an effective approach requires the balancing of a growing number of interests, thus precluding simple conclusions. The dilemmas facing knowledge institutes are complex and demand a nuanced approach. AWTI argues that it is embracing that nuance will open the way for progress and the advancement of policy and practice in relation to knowledge security. However, AWTI also argues that, notwithstanding the complexity and the need for nuance, it is absolutely possible to (continue to) take steps.

### Need for a learning approach, with ongoing attention for nuance and more awareness-raising

AWTI believes that ensuring secure, high-quality knowledge development in the Netherlands requires an ever more effective approach to knowledge security, with more attention for the nuance demanded by the complexity of the situation. More also needs to be done to raise awareness and develop the necessary knowledge and skills in relation to knowledge security among all stakeholders.

Our interviews and analyses revealed several issues around the policy on knowledge security. An underdeveloped conceptualisation and an as of yet unevaluated knowledge security policy pose a threat to both the theory and practice in relation to knowledge security. Although the policy steps taken to date are welcome, there is a danger of the necessary nuance being lost in the future. Rather, the approach is dominated by a reflex of avoiding as many risks as possible, often using preconceived, binding lists of knowledge domains, access to which is to be denied to certain state or non-state entities. How effective this policy is, is open to question. Binary lists of this kind are inadequate for

dealing with the diversity of risk determinants: they are either relatively long, leading to an unnecessary large number of restrictions and eroding the achievements of international collaboration; or they are fairly short, impeding the growth of knowledge security. The current knowledge security policy also produces a number of second-order effects, which are insufficiently acknowledged and taken into account, such as the reactions of other countries to the policy, opportunistic behaviour by stakeholders, or an ineffective 'box-ticking culture'.

It also emerged from our interviews and analyses that several stakeholders – specifically researchers, administrators, and government – devote too little attention to knowledge security in the context of social, technological, and geopolitical developments and their relationship to knowledge security. There is insufficient awareness of the increased complexity of the risks around international collaboration and often of how to deal with those risks. There is also a widespread lack of action perspectives.

### Three recommendations for a learning approach to knowledge security

AWTI makes three recommendations for improving the policy around knowledge security. They give the report a layered structure aimed at developing a leaning approach to knowledge security which devotes permanent attention to nuance and awareness-raising. The recommendations focus on conceptualisation, differentiation, and realisation, and target several areas in the ecosystem.

Adopting a learning approach to knowledge security will improve the ability of the Netherlands to meet the complex challenges of international collaboration in knowledge development, now and in the future. Improving Dutch knowledge security policy by implementing the recommendations is likely to be a process rather than a quick win; that is not a problem provided the approach is designed in such a way that lessons learned can be incorporated in the policy and that the policy is adaptable. A leaning approach offers an answer to the growing complexity whilst still recognising the value of international collaboration. By definition, this approach demands continual attention and focus.

AWTI believes that improving knowledge security is primarily a responsibility of government, working in collaboration with knowledge institutes. It is within government that the different national interests and perspectives in relation to knowledge security and associated themes are brought together and weighed against each other. The central focus of this report is therefore on the government. However, the report is also aimed at knowledge institutes, since it is here that the learning process in relation to knowledge security must take place. Additionally, an effective and nuanced approach to the issues benefits from input and leadership from the sector itself. The danger is that if this learning

approach is developed insufficiently, this will increase the pressure on government to adopt a less nuanced, more restrictive approach.

This leads us to make the following recommendations, which need to be implemented simultaneously:

**Recommendation 1. Conceptualisation: improve understanding of knowledge security**

Theory and practice in relation to knowledge security are in their infancy, and are therefore vulnerable to one-sided criticism from specific perspectives. The government should take the lead in further developing and improving the conceptualisation of knowledge security and striking a balance between the different values and interests. This requires two specific actions from government:

- Action 1. Promote and share the findings of research on knowledge security in a broad sense.
- Action 2. Encourage a broad, nuanced debate on this topic.

**Recommendation 2. Differentiation: in risks, measures, and organisations**

Knowledge security needs to be approached in a way that provides clarity to researchers about what is and is not possible whilst also facilitating differentiation by research type, data used, social context and collaboration partners, and which also targets both conscious and unconscious unsafe behaviour. Top-down, binary, binding rules fail to acknowledge this need for differentiation. The government must work together with knowledge institutes to clarify the risks and mitigating measures, whilst recognising the need for differentiation. We recommend the following specific actions:

- Action 1. Develop a sector-wide model for professionalising the approach to knowledge security.
- Action 2. Explore how better use could be made of the organisational diversity of Dutch knowledge institutes to foster knowledge security.

**Recommendation 3. Realisation: increase awareness and capacity**

Knowledge institutes need to improve the awareness, knowledge, and skill levels around knowledge security. The knowledge sector needs to relate to social, technological, and geopolitical trends. This creates a need to recognise knowledge security as a subject. Knowledge institutes will also need to work to raise awareness of the risks, develop knowledge and expertise and broaden the perspectives for action. This requires the following actions:

- Action 1. Broaden and deepen the awareness, knowledge, and skills at knowledge institutes to mitigate risks and grasp opportunities.
- Action 2. Expand the knowledge security teams at knowledge institutes.

**Advice.** Simultaneous implementation of the three recommendations by government and knowledge institutes will lead to a shared learning approach.

1

# Growing complexity of international collaboration demands attention

**Geopolitical, technological, and societal trends make international collaboration between knowledge institutes ever more complex. That collaboration brings benefits, but also risks.**

Both the government and knowledge institutes have taken a number of steps in recent years to mitigate the risks associated with international collaboration. Those steps have been useful, but the pace of developments creates a constant stream of new challenges. With this in mind, in this report AWTI explores the question of how the Netherlands can best deal with the risks of international collaboration in knowledge development at Dutch knowledge institutes, including higher education institutions.

In essence, our analysis shows that there are no simple solutions which do full justice to all the conflicting interests. The dilemmas facing knowledge institutes are complex and demand a nuanced, learning approach. AWTI believes that embracing nuance is the key to the progress and advancement of policy and practice in relation to knowledge security. On the other hand, despite the complexity and the call for nuance AWTI sees opportunities to continue moving forward.

## 1.1 International collaboration brings benefits, but also risks

International collaboration is an essential part of knowledge development, including in higher education, and is highly developed in research and education as well as with regard to the societal impact of research. This delivers many benefits for the Netherlands, such as international mobility of students and researchers and enrichment of the Dutch knowledge base. International collaboration also fosters the circulation of knowledge, which can therefore be incorporated more quickly in high-value products and services. International collaboration thus brings added value for society, including in the form of innovative and earning capacity. Finally, knowledge-sharing is important for tackling global societal challenges.

At the same time, there have been several incidents and undesirable situations around international collaboration, for example undesirable transfer of knowledge to other countries or covert influencing of research in the Netherlands. Security services are also seeing an increase in the threat from state actors. A few examples are given below.

### Undesirable situations in international collaboration

Several studies in recent years have shown that state and non-state actors pose a threat to the security of knowledge development and higher education in the Netherlands. In 2020 the General Intelligence and Security Service of the Netherlands (AIVD) foiled the activities of a Russian intelligence officer who was running an espionage network with access to high-tech companies and a knowledge institute.[1] There is also evidence of foreign interference in Dutch higher education and research,[2] in the form of (self-)censorship due to threats and restriction of access to research material. And an international team of research journalists exposed evidence of collaboration between European universities and knowledge institutes affiliated with the Chinese armed forces on topics with military relevance.[3] In addition to influence and threats, international collaboration can jeopardise the integrity of research. In 2019, for example, the journal *Human Genetics* withdrew a research project involving researchers from Erasmus University Rotterdam, because it was insufficiently clear whether the genetic material from Uighurs that was being used in the research had been provided voluntarily.[4]

Similar incidents also take place outside the Netherlands.[5] In the United Kingdom (UK), a number of individuals were identified who were employed by the Chinese armed forces whilst at the same time working at British universities on potential dual use[6] technology.[7] And a researcher was recently arrested in Norway on suspicion of spying for Russia.[8]

## 1.2 Collaboration is becoming increasingly complex

While international collaboration is an essential part of knowledge development and delivers many benefits, then, it also carries potential risks to national security. The balance to be struck between the opportunities and risks differs depending on the situation, making international collaboration extremely complex. Below we describe five dilemmas which illustrate this complexity. They arise from broader geopolitical, technological and social trends and differences in ethical standards. The dilemmas have varying implications for knowledge institutes, which have to deal with incoherent or even contradictory signals and demands.

---

1 (AIVD, MIVD, and NCTV, 2021)
2 (d'Hooghe & Dekker, 2020)
3 (De Bruijn et al., 2022)
4 (Kempes & Strijker, 2021)
5 (Nouwens & Legarda, 2018; Long, 2019)
6 *Dual use* refers to goods or knowledge which have both a civil and a military application. An example is biometric knowledge about pathogens which can be used both in medicine and in biological warfare.
7 (Clark, 2022)
8 (Myklebust, 2022)

### Collaboration with top scientists

Collaboration with leading researchers in key knowledge domains is of great strategic importance. If the Netherlands falls behind in the race for international leadership in knowledge and technology,[9] this will impede our innovative strength and create strategic risks, for example due to one-sided dependencies.[10] In the past, most world-leading research was carried out in 'friendly' countries, but today more and more emerging countries are at the cutting edge of science.[11] Collaboration with top scientists from those countries is important to retain the Netherlands' knowledge position, but can at the same time help new rivals in their quest for technological leadership.[12]

### Tackling global challenges

Global challenges pose another dilemma in relation to knowledge development.[13] Researchers are warned not to collaborate with countries where human rights are not respected and where different values apply than in the Netherlands. Such collaboration can undermine the scientific integrity of research. At the same time, in order to tackle global challenges such as poverty, inequality, climate change and public health, it is important to collaborate with countries where much of the solution is to be found. To ensure maximum impact of our knowledge, it is often necessary to ensure maximum dissemination and utilisation of that knowledge, even though the countries where these problems occur sometimes adhere to different norms and values. In fact, collaboration can sometimes help scientists in those countries in their difficult relationships with the local authorities, depending on how those researchers conduct themselves and how much freedom they have. Collaborating with (researchers from) countries where different values apply thus creates risks to scientific integrity, but is still an indispensable part of tackling global problems.

### *Open science* and security

The trend towards more open science is leading to complex dilemmas with regard to increasing knowledge security. Open science is based on the belief that science is a global public good and that more openness, transparency and collaboration is needed in the relationship between society and science.[14] This is achieved by making datasets and other research material more accessible for outsiders and by placing research outcomes

9 (Inspectie der Rijksfinanciën, 2020, p. 13; Molthof, Zandee & Cretti, 2021; Teer, 2021, 2022; Huotari & Jean, 2022; Johnson et al., 2022).
10 (Sue-Yen Tjong Tjin Tai et al., 2018; AWTI, 2020a; CSR, 2021; Van Wijnen, 2022)
11 (Brainard & Normile, 2022)
12 (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020; AIVD, MIVD, and NCTV, 2021; AIVD, 2022)
13 (Ghodsvali, Krishnamurthy & De Vries, 2019; AWTI, 2020b)
14 (Boulton, 2021)

in the public domain and actively disseminating them. Open science also implies collaboration with non-scientific stakeholders, such as citizens and practical specialists. However, openness, free access and transparency also make research vulnerable to interference and espionage by parties with malign intentions. Conversely, closing off research in order to increase security goes against the very essence of the open science movement.

### High expectations and many conditions

Against the backdrop of social challenges, economic growth and national security, society places high expectations on knowledge institutes in the Netherlands, for example demanding solutions for social problems and high-grade knowledge to support innovative industry.[15] The demands placed on knowledge institutes and individual researchers are moreover increasing; this in turn leads to an increase in the standards and conditions imposed. On top of this are the concerns about integrity and security – important aspects which create extra work in the knowledge sector where pressure of work is already high. This could make it even harder to attract and retain talent, thereby further increasing the pressure of work on those actively engaged in research. That in turn makes it even more difficult for them to meet the expectations placed upon them.

### STI diplomacy

The role of science, technology and innovation in diplomacy[16] creates a dilemma of a different kind. There is an inclination to end the economic and scientific collaboration between rival countries or power blocs..[17] With regard to trade and other forms of collaboration, this is often unavoidable; but in science and research some form of collaboration is often desirable[18] because this can offer an opening in conflicts and lead to mutual understanding.[19] Moreover, this form of collaboration generates insights into the underlying causes and interests at play in the conflict.

15 (KNAW, 2019, 2021)
16 (AWTI, 2017b; Fägersten, 2022)
17 (Hudson et al., 2022)
18 (Fägersten, 2022), see also https://www.nwo.nl/en/science-diplomacy
19 (Kissinger, 1995)

**Dilemmas.** International collaboration is becoming ever more complex.

| | |
|---|---|
|  **Collaboration with top research(ers)** is important to maintain our strong knowledge position. | Can help new rivals in their quest for technological leadership. |
|  **International collaboration** is crucial for tackling global challenges. | Collaborating with partners with different values poses a risk to scientific integrity. |
|  **Open science** is an important development for the relationship between society and science. | Increases vulnerability to foreign interference and espionage. |
|  **High expectations** of knowledge institutes lead to many demands and conditions. | Reduced attractiveness of research makes it harder to meet expectations. |
|  **STI diplomacy** offers an opening in conflicts and leads to mutual understanding. | Rival countries are inclined to end scientific collaboration. |

The dilemmas above illustrate the challenge of recognising the benefits of international collaboration in knowledge development and higher education whilst at the same time facing up to the increased risks and threats. If we do not do this correctly, there is a risk that the quality, integrity and impact of knowledge development and higher education will be undermined. That in turn has repercussions for the welfare, security, and competitiveness of the Netherlands.

## 1.3 Request for advice: How do we deal with the risks associated with international collaboration?

Many Western countries are aware of the risks associated with international collaboration. This has led to the rapid emergence of a new policy domain in recent years, focused on

knowledge security.[20] This policy is concerned with protecting or securing knowledge development and higher education in relation to international developments. Knowledge security policy impinges on science policy, higher education policy, research policy, economic policy, foreign policy and domestic security policy. From an international perspective, the Netherlands - behind a few Anglo-Saxon countries and together with a number of Scandinavian countries - is at the forefront in taking measures in this area.[21]

However, this does not mean that the problems have been resolved, given the tremendous pace of developments not just in science, technology and innovation, but also at a geopolitical and economic level.[22] There has also been an enormous increase in global research collaboration in recent years.[23] These trends imply that the complexity will only increase in the future, requiring continual adaptation of the goals of knowledge security policy. The current geopolitical turbulence has moreover lent a new dimension to the public debate around knowledge security. This is leading to heated discussions and prompting several stakeholders to adopt radical positions.[24]

Against this backdrop, AWTI addresses the following question: ***How should the Netherlands deal with the risks of international collaboration in relation to knowledge development at Dutch knowledge institutes, including in higher education?*** In answering this question, we focus on (partly) publicly funded Dutch knowledge institutes, including in higher education, and their immediate ecosystem of funding and impact. Whilst acknowledging that private companies and civil-society organisations also face challenges in relation to foreign interference, espionage, or sabotage, these are not covered in this report. Although cybersecurity is a related theme, this again is not a key focus in this report, except where it forms part of knowledge

20 Several different labels are used to describe this, such as *research security* (OECD, 2022), *tackling foreign interference* (European Commission. Directorate General for Research and Innovation, 2022), *trusted research* (UKRI, 2021) and *knowledge security* (Rathenau Instituut, 2021). The description also refers to (*open*) *strategic autonomy*, research integrity and anti-coercion. We explore this divergent terminology in more depth in chapter 2.

21 See e.g., the OECD portal on *research security* https://stip.oecd.org/stip/research-security-portal, where the Netherlands is one of a limited number of countries engaging with this.

22 See also the warning about *normalcy bias* by the Netherlands Scientific Council for Government Policy (WRR): the psychological reflex to downplay a potential threat (Van der Dool, 2022).

23 More than ten years ago AWTI's predecessor, the Advisory Council for Science and Technology (AWT) published a report on the growing relevance of China in the field of science, technology and innovation (*De Chinese handschoen* – 'The Chinese glove'). Although that report devoted a good deal of attention to the opportunities and recommended an intensification of collaboration, it also highlighted the drawbacks and risks. AWT also noted the concerns about the leaching of knowledge and urged the government to reflect on which knowledge is crucial and how it can be retained (AWT, 2012, p. 5).

24 See e.g. the 'two-minute parliamentary debate' of 14 September 2022 on knowledge security at Dutch knowledge institutes and the discussion on the TV programme Op1 on 14 October 2022 on the dependence on China.

security. Cybersecurity is a topic that has been a focus of attention for some time and is more suited to the mission and expertise of other agencies.[25]

### Creation of this report

This report was compiled in a number of stages (see Appendix 1). Discussions were held with various experts and stakeholders in order to explore the topic (see Appendix 2), while information was also gathered using a number of analyses and case studies (see e.g. Appendix 3 and Appendix 4). The LeidenAsiaCentre (LAC) also carried out an international comparison of measures taken to support knowledge security in twelve countries.[26] The analyses were discussed during Council meetings in order to establish a focus for the report and recommendations. This was then discussed with various stakeholders and experts. We would like to thank all stakeholders for their time, openness and insights.

### Project group

This report was prepared by a project group consisting of Council members Chokri Mousaoui, Ellen Moors, Sjoukje Heimovaara and Koenraad Debackere, and staff members Chris Eveleens, Bart Gulden, Tara van Viegen and Sabine Jaegers.

### Message and layout of this report

Chapter 2 discusses the results of the analyses. Our principal conclusion is that a learning approach is needed in which there is permanent attention for nuance and greater awareness-raising. We observe that the policy in relation to knowledge security is vulnerable, the necessary nuance is sometimes lacking, the stakeholders are insufficiently conscious of the risks, and there is a lack of perspectives for action.

Chapter 3 then sets out three recommendations for improving the present approach. Despite the complexity of the topic and the need for nuance, AWTI does see opportunities to continue moving forward. The three recommendations and the underlying actions are an attempt to contribute to improving the conceptualisation, policy and practice in relation to knowledge security in the Netherlands.

25 E.g. the Cyber Security Council, the National Cyber Security Centre. See also (Bertuzzi, 2022)
26 (d'Hooghe & Lammertink, 2022). Accessible at www.awti.nl

# 2

# Learning approach needed, with attention for nuance and more awareness-raising

**AWTI believes that, in order to keep knowledge development in the Netherlands secure and maintain its high quality, it is important to continually improve the approach to knowledge security. That approach requires attention for the nuance demanded by the complex reality. Even more efforts also need to be made to raise awareness and develop knowledge and skills around knowledge security among all stakeholders.**

Our interviews and analyses revealed a number of pinchpoints in relation to knowledge security policy. The theory and practice in relation to knowledge security are for example vulnerable due to an underdeveloped understanding of them and a policy which has yet to be evaluated (section 2.1). The steps taken thus far are laudable, but there is a danger of the necessary nuance in the approach being lost (section 2.2). Current developments demand the attention of all stakeholders: researchers, administrators and government. However, there is a lack of awareness of the increased complexity and risks. There are also insufficient practical options (section 2.3). In this chapter we explore these issues in more detail, before setting out specific recommendations to improve the approach to knowledge security in chapter 3.

## 2.1 Theory and practice in relation to knowledge security are vulnerable

**Knowledge security is broadly speaking about avoiding or mitigating a number of risks and threats which ensue from international relations or collaboration. Their importance is recognised and there is a growing familiarity with them. Nonetheless, theory and practice in relation to knowledge security are vulnerable.**

There are a number of reasons for this vulnerability. The conceptualisation of knowledge security is underdeveloped and will continue to be both a moving and a movable target. Different perspectives on knowledge security, such as an academic perspective, a security perspective and an economic perspective, moreover quickly push the discussion towards the extremes. In addition, the measures taken in the context of knowledge security at both national and international level are still relatively new, and the functioning and effectiveness of the policy has therefore not yet been evaluated.

### Usable description of knowledge security, but conceptualisation underdeveloped

There is a broadly endorsed description of knowledge security in the Netherlands, which is used by the government and knowledge institutes.[27] It states that knowledge security is about avoiding or at least mitigating a number of risks and threats which ensue from international relations and collaboration. According to this description, there are broadly three types of risks (see Box below): a) undesirable transfer of knowledge and technology with negative consequences for national security or innovation performance; b) undesirable influence and interference in higher education and research; and c) problematic ethical issues.

#### Description of knowledge security

Knowledge security is generally defined by Dutch knowledge institutes and government as follows:

*"Knowledge security is first and foremost about preventing 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 other states. Such interference places academic freedom and social safety in jeopardy. Finally, knowledge security involves ethical issues that can be at play in collaboration with countries that do not respect fundamental rights."*[28]

Several interviewees stated emphatically that this description of knowledge security is not intended to be a formal definition.

Although this description of knowledge security has proved useful in gaining a better understanding of the challenges and the joint interventions needed to meet them, it is not unproblematic.[29] First and foremost, it leaves considerable scope for interpretation. The boundaries between what does and does not qualify as knowledge security are vague: precisely what constitutes 'undesirable', and who decides that? In combating climate change, for example, the sharing of sustainable technological knowledge between knowledge institutes can be of great importance, but from a commercial standpoint it may be desirable to continue developing that knowledge into innovative applications which

27 Snetselaar (2022) shows how the term 'knowledge security' was introduced in order to arrive at a shared problem definition in a complex social world ('rendering'). It provided a label for a set of emergent problems. By naming the risks and causes, it was possible to take action.
28 (Universiteiten van Nederland *et al.*, 2022, pp. 9–10)
29 This follows from the discussions we held about the concept, both within the Council and with various stakeholders. It transpires that different knowledge institutes emphasise different aspects and set different boundaries in what they understand by knowledge security. See also Snetselaar (2022, p. 11).

bring not just social but also economic benefits. The causal connections between decisions in research practice and the ultimate, possibly negative consequences, are also uncertain. Although researchers have a responsibility for the knowledge they develop, the way that knowledge is ultimately used cannot be predicted in advance; it depends not only on the topic on which knowledge is being developed and the immediate collaboration partners, but also on the broader social and political context within which that knowledge is acquired and disseminated.

A further problem is that the description formulates the various risks broadly, with no distinction made between risks that are taken deliberately and (unconscious) naivety (see Box below). Undesirable knowledge transfer can moreover take place in both a legal and illegal manner, yet both fall within the description. The ethical dimension of knowledge security relates to the integrity of the research itself (ethics dumping), but also to what is subsequently done with the research outcomes (misuse). In short, it is by no means always clear whether or not a situation forms a risk to knowledge security, making intervention difficult. Put differently, the lack of a clear conceptualisation acts as an impediment to an effective approach.[30]

**Conscious and unconscious behaviour**

In this report we distinguish between conscious and unconscious behaviour with regard to knowledge security. Unconscious infringement of knowledge security is often the result of a degree of naivety, for example if someone travelling abroad fails to secure their computer or telephone adequately or shares knowledge online which can be misused in the foreign country. A researcher can also be unknowingly fed with misinformation or subjected to covert influence.

An example of conscious behaviour that leads to infringement of knowledge security might be where researchers from the Netherlands receive an attractive offer from another country to collaborate on topics which are known to be sensitive. If a researcher has several affiliations, including in other countries, but deliberately fails to disclose these to Dutch agencies or research funders, this also jeopardises knowledge security.

Furthermore, the Dutch description of knowledge security is in line with, but not identical to, the descriptions used in the international discourse.[31] That need not by definition be a problem but, particularly where there are calls for international liaison or even a

30 (Gort, 2011)
31 For a more detailed discussion of the differences and correspondences, see (d'Hooghe & Lammertink, 2022)

coordinated approach, it is good to be aware of the differences. Moreover, the terminology used by (groups of) countries reflects the specific local focus and approach.[32] The OECD, for example, uses the term 'research security',[33] meaning avoiding undesirable interference by a foreign state or non-state actor in a country's research practice, with the aim of safeguarding that country's research ecosystem and the associated national and economic interests.[34] The OECD thus places the emphasis more on the practice and processes of research, and to a lesser extent on the knowledge itself. In the United States, by contrast, the emphasis is placed mainly on technological and economic dominance.[35] The European Commission uses the term 'foreign interference in research and innovation.'[36] According to the Commission, 'Foreign interference occurs when activities are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU)'.[37] This definition thus mainly corresponds with the second aspect in the Dutch description of knowledge security, which is concerned with avoiding the covert influencing of research and education. The G7 group of countries also use the term 'research security'. The emphasis here is on protecting the research community, and is also linked to public safety. The G7 consistently uses the term 'research security' in combination with the term 'scientific integrity' or 'research integrity',[38] defined as "the adherence to the professional values, principles, and best practices that ensure and uphold the validity, social relevance, responsibility, and quality of research".[39] The description contains an internal component (concerning the validity and quality of research) and an external component (relevance and responsibility). The internal component is not strongly reflected in the Dutch description of knowledge security, but the external component is covered in the section on ethical issues.

### Different perspectives on knowledge security push discussion towards extremes

Knowledge security can be approached from at least three perspectives:[40] a security perspective, an academic perspective, and an economic perspective. The different standpoints and arguments in the debate about international collaboration in knowledge

32 The international comparative study by the LeidenAsiaCentre (LAC) shows clearly how the terminology used in different countries is related to the national context and selected approach (d'Hooghe & Lammertink, 2022). It thus matters which words are used.
33 (OECD, 2022)
34 (OECD, 2022)
35 (National Security Commission on Artificial Intelligence, 2021)
36 (European Commission. Directorate General for Research and Innovation, 2022)
37 (European Commission. Directorate General for Research and Innovation., 2022)
38 (G7, 2022; Scientific integrity fast-track action committee, 2022)
39 (G7, 2022, p. 7)
40 These perspectives are clearly reflected in documents and in the discussions we held. We describe the three perspectives in more detail in Appendix 4.

development can often be traced back to these perspectives (see also Appendix 4). Each perspective offers a particular take on the values applied in the debate about knowledge security. In any approach to knowledge security, these different values need to be weighed against each other. There are both mutual touchpoints and differences.

Stability and sovereignty play an important role in the security perspective. These values also occur in the economic and academic perspectives, mainly in the form of autonomy. In the economic dimension, for example, there is the importance of (open) strategic autonomy in the economic dimension, referring roughly to the ability to act and decide autonomously and to be self-sufficient and self-reliant with regard to industry, technology and diplomacy.[41] In the academic perspective there is the core value of institutional autonomy, encapsulating the guarantee of academic freedom for scientific institutions.[42] In combating undesirable interference, there is common ground between these perspectives.

But there are also differences. The security perspective is characterised by the desire to 'retain' or 'protect' our way of living and working, whereas the economic and academic perspectives are characterised more by 'improvement' or 'change'. In an economic sense, this is expressed in the free movement of goods, services and people in order to improve the economic potential. In the academic perspective, it is reflected in the free movement of persons, data, research collaborations and results with a view to increasing the social impact of science and research. These contradictions in the different perspectives explain the quest for and the importance of a balance between an open and closed approach. The security perspective tends to encourage a closed position, whereas the economic and academic perspectives predominantly call for openness.

It is therefore important to be clear which perspective sets and influences the tone of the debate. If the values of academic freedom or institutional autonomy are pursued in an academic perspective to the absolute degree, this impinges negatively on values such as security and stability which dominate the security perspective. Similarly, if strategic autonomy is taken too far from a security perspective, this creates tensions with the desire for openness, which is a key value (and value-creating dimension) within the academic and economic perspectives. If all these different values are to be taken properly into account, therefore, it is important not to pursue absolutes. This implies that when developing knowledge security policy, a continual balance needs to be struck between the different values.

41 See e.g. De Jager et al. (undated)
42 (KNAW, 2021)

If the values inherent in a particular perspective become dominant and the discussion is pushed to the extreme, this impedes policy development. Without consensus, the legitimacy and feasibility of policy measures are undermined, in turn making implementation more difficult. If an extreme position is taken as a starting point for policy and measures, experience in practice shows that this undermines other values. This then leads to a correction, giving rise to 'vacillating' policy-making, which in turn acts as a barrier to international collaboration and adversely affects research quality.

### Relative newness of the policy domain makes it difficult to determine impact

A letter to Parliament at the end of 2020 marked a recognisable starting point for knowledge security policy in the Netherlands.[43] The resultant policy extends across different ministries. Against the background of existing statutory measures (such as export regulations and knowledge embargos imposed on Iran and North Korea) and non-statutory measures (such as the Code of Conduct for Research Integrity), new measures have been taken in the last two years to promote knowledge security.[44] At the heart of the policy is a raft of measures taken by the Ministry of Education, Culture and Science, the Ministry of Economic Affairs and Climate Policy and the Ministry of Justice and Security. They include a national guideline and a Knowledge Security Resource Centre, administrative agreements and a systematic risk analysis at knowledge institutes.[45] The aim of the knowledge security policy is to 'ensure safe and secure international collaboration, with attention for the attendant opportunities and risks'."[46] The Ministry of Education, Culture and Science is the lead ministry and plays a coordinating role. Other ministries take the lead on a number of related measures such as the Investment, Mergers and Acquisitions (Security Screening) Act ('Wet veiligheidstoets, investeringen, fusies en overnames')[47] and the enhanced legislation on espionage.[48] The security and intelligence services are also concerned with knowledge security. They operate under the Ministry of the Interior and Kingdom Relations and the Ministry of Defence, with the task

43 We treat the letter to Parliament, 'Knowledge security in higher education and research' ('Kennisveiligheid hoger onderwijs en wetenschap') as marking the start of the policy (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020). Naturally, this policy did not arise in a vacuum, and other relevant activities can be noted. These earlier activities are incorporated in the policy analysis (see Appendix 3).

44 Appendix 3 contains an annotated overview of a large number of measures (policy instruments, codes of conduct, legislation, etc.) which are related to knowledge security.

45 The Ministry of Education, Culture and Science generally takes the lead on knowledge security policy (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020; Minister van OCW, 2022b, 2022a; Minister van OCW, Minister van EZK, and Minister van J&V, 2022).

46 (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020, p. 1)

47 (Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid, 2022b)

48 (Ministerie van Justitie en Veiligheid, 2022)

of safeguarding national security.[49] Finally, the Ministry of Foreign Affairs also pursues policy which impinges on knowledge security policy, for example through its network of diplomatic postings and the China strategy.[50] Overall, therefore, a fairly new and varied package of measures is evolving, developed and implemented by different government ministries and intended to provide a response to global developments.

Policy is also developing rapidly in other countries. The study carried out by the LeidenAsiaCentre (LAC) for AWTI provides an in-depth and comprehensive picture in this regard.[51] It reveals a wide variety of different approaches, in terms of both structure (governance) and actual measures. One dimension where this variation manifests itself is in the difference between a more top-down approach, as in Japan and France, and a more bottom-up approach as in Finland and Germany.[52] There are also countries which combine top-down legislative measures with bottom-up initiatives, for example Australia and the United Kingdom. Another dimension concerns the degree of coercion or enforcement encapsulated within the measures; some countries adopt a more coercive, juridical approach, for example with mandatory registration of collaborations (Australia), public disclosure of research funding (the US and the UK) or mandatory screening of contracts (France). In the United Kingdom and Australia, official agencies have been set up to oversee this.[53] The other countries have not opted for such coercive, legalistic measures.

The OECD has carried out research on research integrity and security.[54] As well as an inventory of the risks, its report contains an overview of policy initiatives and activities in OECD member states. Many of the case studies are taken from Anglo-Saxon countries, but the report also describes policy instruments in Germany, Sweden, and the Netherlands. The researchers conclude that the responsibilities for research integrity and security are divided among a variety of actors, such as national governments, research funders and institutes. The OECD has launched a ‘security portal’ to increase the insight into the measures being taken.[55]

As well as being new and taking a variety of forms, knowledge security policy has barely been evaluated. That makes it difficult to determine its impact. At the time of writing this report, not a single one of the 120 measures listed on the OECD portal had been formally

49 See e.g. the public annual reports of the General Intelligence and Security Service (AIVD) (AIVD, 2022) and MIVD (MIVD, 2022), and the Threat Assessment for State Actors (AIVD, MIVD, & NCTV, 2021).
50 (Ministerie van Buitenlandse Zaken, 2019; Minister van Buitenlandse Zaken, 2021)
51 (d’Hooghe & Lammertink, 2022)
52 (d’Hooghe & Lammertink, 2022, pp. 49–50)
53 (d’Hooghe & Lammertink, 2022, p. 50)
54 (OECD, 2022)
55 https://stip.oecd.org/stip/research-security-portal

evaluated, although parliamentary inquiries have been carried out on knowledge security policy in Australia and Finland, while the interviews and analyses in the LAC study also offer some insights.[56] These analyses suggest that the awareness-raising campaigns in Australia, Germany, Finland, the UK and the US have been effective. The LAC study shows a correlation between the effectiveness of the policy and its extensiveness, coherence and pragmatism in terms of the degree of coordination between government and knowledge institutes. Nonetheless, more research is needed. The OECD researchers call on governments, research funding organisations, research institutes and higher education establishments to carry out regular audits to determine whether their security strategies are sufficiently mature, and if necessary to adjust their policies to increase their effectiveness and monitor any unintended consequences.

## 2.2 Positive steps have been taken, but there is a risk of the necessary nuance being lost

**The steps taken so far to increase knowledge security are laudable. However, a balance needs to be struck between openness and freedom on the one hand and a closed, regulated approach on the other. That balance is not the same in every case, but depends among other things on the field of research, the potential applications and the partner countries. We observe that the necessary nuance in seeking that balance is sometimes lacking, owing to extreme positions being taken in the debate and the automatic reflex of seeking to minimise risks. This does not help the effectiveness of the approach.**

The recently developed knowledge security policy builds on an existing mix of policies (see Appendix 3 for an annotated overview of existing and new policy). The government and knowledge institutes have taken positive steps, and that is welcome. The policy developments take into account key values for knowledge development and exploit the existing consultative culture and structures around science, technology and innovation. Moreover, we note that the Netherlands is among the countries which is setting an example to others.

The words and actions of the Dutch Minister of Education, Culture and Science reveal that policymakers in The Hague are well aware of the sensitivity of intervening in science and research for the purpose of knowledge security.[57] Unsurprisingly, the policy they have developed therefore comprises several elements. The common thread of knowledge

56 (d'Hooghe & Lammertink, 2022, p. 51)
57 Committee debate on internationalisation and knowledge security, 9 February 2022 (https://debatgemist.tweedekamer.nl/debatten/internationalisering-en-kennisveiligheid) and (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020)

security contributes to increasing the understanding of the concept, as well as to enhancing knowledge and awareness in relation to knowledge security. The Knowledge Security Resource Centre gathers and brings together information from the government and advises knowledge institutes. At the behest of Parliament, the government has also asked all knowledge institutes in the Netherlands to carry out a knowledge security risk analysis. The analyses carried out by universities are subjected to an external audit.[58] An assessment framework for individuals is also being developed; this is discussed later in this section. The policy has to date been based largely on self-regulation; however, the introduction of the audits goes a step further and is more of a top-down measure. The introduction of the assessment framework for individuals changes the relationship between the government and knowledge institutes as regards recruiting researchers from certain countries.

Broadly speaking, the approach makes good use of the existing consultative structures in the sector.[59] The national knowledge security guideline was formulated by a large group of organisations, viz. Universities of the Netherlands (UNL), the Royal Netherlands Academy of Arts and Sciences (KNAW), the Netherlands Association of Universities of Applied Sciences, the Netherlands Federation of University Medical Centres (NFU), the Dutch Federation of Applied Research Organisations (TO2-federatie), the Dutch Research Council (NWO) and central government.[60] Great value is attached to dialogue; the Minister of Education, Culture and Science has made administrative agreements with the knowledge institutes and regular consultation takes place between institutes and the Minister on the knowledge security policy.[61] A portfolio-holder has been appointed at administrative level, as well as a 'knowledge security advisory team'.[62] In practice, knowledge institutes have a full-time or part-time knowledge security 'policy adviser', 'project manager' or 'programme manager' whose brief concerns the development, implementation and monitoring of the policy around knowledge security. Among other things, this involves carrying out the risk analyses referred to earlier at the request of the Minister.[63]

Internationally, the Netherlands is seen as being fairly advanced in developing an approach to knowledge security.[64] Although less advanced than the Anglo-Saxon

58 (Van der Woude & Van der Molen, 2022)
59 (van der Meulen & Rip, 1998)
60 (Universiteiten van Nederland *et al.*, 2022). The guideline builds on a knowledge security framework for universities developed by the Association of Universities in the Netherlands (VSNU), the predecessor of UNL (VSNU, 2021).
61 See e.g. (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020) and (Minister van OCW, 2022a)
62 (Minister van OCW, 2022b, p. 1)
63 (Minister van OCW, 2022b)
64 This was evident from our discussions with interviewees outside the Netherlands.

countries in this regard, a good deal of knowledge and expertise has nonetheless been built up about knowledge security in a short space of time. The input of Dutch experts and policymakers, and especially of the Knowledge Security Resource Centre, is accordingly valued internationally. Although no evaluation has yet taken place, the Resource Centre was described as an example of good practice by many of our interviewees in the Netherlands and in other countries.[65]

### Balance and differentiation are crucial

Many stakeholders, including the Minister of Education, Culture and Science, have stressed the importance of proportionality in the approach to knowledge security.[66] The key is to strike a balance between securitisation (going too far in pursuit of security) and naivety. Both extremes lead to dangers and losses. A naïve approach runs the risk of abuse of the openness and transparency of knowledge development and higher education in order to influence them or appropriate the knowledge that has been developed. Conversely, over-regulation or an excessive focus on security also creates an undesirable situation,[67] in particular the risk of stigmatising people from certain countries,[68] undermining the use of the positive outcomes of research as a form of soft power for diplomacy,[69] and restricting competitiveness and progress.[70] These second-order policy effects are significant and need to be considered before and during the evaluation of the policy.

Striking the right balance in decisions depends on the context in which knowledge development takes place. Everyone understands that stricter conditions than average will apply in defence research. Similarly, a relatively large number of security measures apply to biomedical research. These measures are also increasingly being applied to technology research, for example quantum and encryption technology. But the context entails more aspects than the sector in which the knowledge ends up,[71] for example the

---

65 *E.g.*, the European Commission's Mutual Learning Exercise. According to our international interviewees, Dutch input is also valued in the EU-Knowledge Network on China (EU-KNOC).

66 See e.g. the letter to Parliament on knowledge security in higher education and science ('Kennisveiligheid in hoger onderwijs en wetenschap'), in which the motto 'open where possible, protected where necessary' forms the basic principle: it is all about proportionality and customisation.' (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020, p. 3). The G7 framed the question as: "How to keep science open, but also secure?" (Hudson, 2022).

67 Even, or precisely, in the most sensitive social and geopolitical situations, calls have been made in the past for openness and freedom (Stone *et al.*, 2022). These values have proved and remain an essential element in the (scientific) research system.

68 See e.g. (Ellis & Gluckman, 2019; Fischer, 2021, 2022b). There is also a visible and intensified remigration to China by researchers from the US (Xie *et al.*, 2022).

69 (AWTI, 2017b; Fägersten, 2022; Hudson *et al.*, 2022)

70 (Baker, 2022)

71 Note that the ultimate use to which knowledge will be put is often uncertain at the time that knowledge is developed, let alone when the research proposals are written (see Van der Meulen

specific field or discipline, the type of research organisation, the type of data used, the technology used, the 'application-readiness' of the knowledge, the nature of the collaboration partners, the country with which researchers are collaborating and the type of funding.[72] Moreover, research projects and programmes do not take place in isolation, but generally form part of a broader, often international system of actors (e.g. researchers, companies, civil-society actors) and institutions (legislation and regulation).[73] Intervening in this system has direct and indirect consequences, and it is therefore vital to apply a differentiated approach which takes account of the context within which the research takes place.[74]

### Signs that the necessary nuance is lacking

As the foregoing makes clear, nuance is important in the policy developments, measures, and discourse around knowledge security. However, we note that this nuance is currently not always sufficiently present. This view is based on four observations.

First, we gleaned from our interviews and from public sources[75] that there is a degree of scepticism among several actors. There is a heated debate not just in the Netherlands,[76] but also internationally.[77] This leads to extreme positions being adopted and to proposals for far-reaching measures lacking in nuance, with concomitant undesirable effects. There are examples in the US of researchers who were – as it transpires wrongly – prosecuted because of alleged undesirable links with China.[78] This has a negative impact on the social safety of researchers and contributes to their remigration.

Second, some stakeholders develop a reflex of avoiding risks as far as possible. Several instruments are currently being developed with a view to gaining a grip of the risks described earlier. The most prominent is the proposed assessment framework, which is likely to cover sensitive knowledge fields to which individuals from certain countries will be denied access.[79] Permission will then be required from the government if people from

---

in (Graaf, de, Rinnooy Kan & Molenaar, 2017)). There are also indications that the dividing line between military and civil use is becoming increasingly blurred (Diercks, Deuten & Diederen, 2019).

72 (Wellerstein, 2021).

73 See also (Fransman *et al.*, 2021).

74 (Committee on Protecting Critical Technologies for National Security in an Era of Openness and Competition *et al.*, 2022)

75 See also (Snetselaar, 2022)

76 See e.g. (ScienceGuide, 2022a, 2022b)

77 See e.g. (Baker, 2022) and (Foy, 2022)

78 (Fischer, 2021)

79 The assessment framework, announced in the first parliamentary letter on knowledge security (Minister van OCW, Minister van J&V, and Staatssecretaris van EZK, 2020) is still being developed, so it is unclear yet precisely what form it will take. Our view is based on information from the letter to Parliament (Minister van OCW, 2022b) and our interviews. The original

those countries wish to work in specific knowledge fields or with specific technologies. Another instrument is a resolution governing the application scope of sensitive technology; this is prepared for the Investment, Mergers and Acquisitions (Security Screening) Act ('Wet vifo'),[80] which contains a list of technologies categorised as non-sensitive, sensitive or highly sensitive.[81] Investments in companies which possess sensitive technology must first be approved by the Ministry. Lists of this kind are tempting and offer apparent clarity, but in reality suffer from a number of second-order problems. First, by definition they lag behind scientific and technological developments; this creates the temptation to define the categories broadly, so that future developments will also fit within them.[82] This could unnecessarily constrain future research. A second problem is that such lists can lead to a sort of 'box-ticking culture' (see also Box below): instead of recognising the complexity, the situation is simplified to a list of countries and knowledge categories.[83] This can give rise to a false sense of security, because risks can emerge outside the categories or as a result of strategic behaviour, whereby high-risk collaboration is described in such a way that it falls outside the categories. Thirdly, such lists can lead to the debate about values not being held. The multidimensional weighing of academic, economic and security values is then reduced to a binary list of what is and is not permitted. A fourth and final problem with this policy response is that the security of research and education is separated from efforts to encourage and strengthen research.[84] This leads to separate, inconsistent policy pathways which target the same organisations but with different goals. That in turn exacerbates the dilemmas highlighted in chapter 1.

**The example of accountancy**

Some years ago, the accountancy sector came in for heavy criticism in the wake of a number of fraud and corruption scandals. This led to the setting up of numerous committees and working groups, which published reports on how to address the problems in the sector. While it was agreed that change first needed to come from within the sector itself, the Monitoring Committee for Accountancy (MCA) observed in 2020 that the same problems were recurring continually, with no sign of improvement.

intention was that collaborative partnerships and funding flows would also be assessed, but more recent reports only refer to the assessment framework for individuals.

80 (Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid, 2022a)

81 The effectiveness of these restrictive lists has also been criticised (Van den Broek, 2022).

82 The new espionage legislation has also been criticised, mainly because of its general nature and lack of clarity, e.g. by the Council of State (Geurts, 2022), lawyers and a former security expert (Versteegh, 2022).

83 (Shih, 2022)

84 (d'Hooghe & Lammertink, 2022, p. 49)

The Committee accordingly proposed a set of 30 new measures, on top of the 53 measures proposed by the previous committee. Ultimately, this led to the Ministry of Finance publishing the Future of the Accountancy Sector Act (Wet toekomst accountancysector).[85]

As soon as the different measures and the bill were published, warnings were raised that over-regulation would lead to a 'box-ticking culture'. One of the proposals was that accountants should be required to report on their activities. However, critics disputed the effectiveness of this, arguing that it would do no more than address the symptoms rather than tackling the underlying problem.[86] An excess of rules (compliance) moreover impedes the individual's own critical insights, according to a professor of audit and assurance writing in the *Financieele Dagblad* financial newspaper.[87] It was also argued that such a box-ticking culture creates a paper reality that serves as an excuse if things go wrong.[88] The sector is currently faced with an acute shortage of accountants.[89] For various reasons, a career in accountancy is clearly insufficiently attractive to generate an adequate influx of young people. The suspicion is that the regulation plays a role in this.

As well as the distrust and scepticism between different actors and the risk-avoidance reflex, there is a third factor, namely the call for 'clarity'. In our interviews, several stakeholders referred to the 'grey area' where it is unclear whether and how scientists should collaborate. This grey area stems from conflicting expectations and signals received by knowledge institutes and researchers regarding international collaboration. It is tempting for knowledge institutes to ask for more clarity, primarily from the government. What they would like is a relatively simple set of decision rules on what is and is not permitted. This 'utopia of clarity' was mentioned in several interviews, and underestimates the problem.[90] It is a utopia because it is unlikely that the government will be able to create the desired clarity from its central position. Given the complexity highlighted earlier, decisions on international collaboration depend on so many factors that they cannot be taken on the basis of simplistic decision rules. If the government heeds the

85 (Monitoring Commissie Accountancy, 2020; Pols, 2020)
86 (Pheijffer, 2021)
87 (Baurichter & Pols, 2020)
88 (Pols, 2022)
89 (Bruins, 2022)
90 See also this quote from the Dutch universities in 2021: "There is, of course, a call from politics for a clear and unambiguous answer, [but] there just isn't one. Moreover, politics always lags behind new developments, which is logical because it needs to follow a certain trajectory. Universities, by definition, want to respond to new developments. [Thus], what is needed is a very differentiated answer, one in which there is room for universities to act." (Snetselaar, 2022)

calls for clarity, there are broadly two options: either the government develops rules that are so restrictive that many of the benefits of international collaboration are lost and the quality of knowledge development is compromised; or the government develops considerably looser rules which contribute little to knowledge security. Clarity then quickly becomes pseudo-clarity. These two sides of the coin clearly illustrate the dilemma and the importance of striking the right balance.

Finally, we have seen a number of clearly political interventions in the practice of science in the recent period, especially the calls following Russia's invasion of Ukraine to sever all ties with Russian and Belarusian scientists.[91] Restrictive, top-down interventions such as these put pressure on other values, such as institutional autonomy.

## 2.3 Awareness-raising and action perspectives not yet adequate

**Awareness-raising among researchers and administrators, and the available tools, are under development, but this process is not yet adequate. Geopolitical, economic, and technological developments in the world mean that knowledge institutes are increasingly confronted with challenges in relation to knowledge security. Continuous development of knowledge and skills in this area is therefore vital.**

Since the development and implementation of the national guideline on knowledge security in January 2022, attention for knowledge security at knowledge institutes has increased considerably.[92] Partly under prompting from the government, responsibilities have been allocated to knowledge institutes and existing collaborations and partnerships are subject to critical scrutiny.[93] This has led to increased awareness and the development of tools by knowledge institutes.[94] Knowledge, insights and practical tips are also increasingly shared between knowledge institutes.[95]

### Awareness-raising and skills need to improve

The foregoing notwithstanding, based on our own observations and interviews with stakeholders we note that there is still a lack of risk awareness in many places and that skills around knowledge security are still underdeveloped. More and more research is

91 (Fischer, 2022a)
92 (Snetselaar, 2022)
93 The risk analysis called for by the Ministry and the announcement of the audit of that analysis were a major contributory factor here (Minister van OCW, 2022b).
94 For example the 'Partnering tools' at TU Delft (De Bruijn, 2021).
95 A group of European universities, including Leiden University, recently published a guide for evaluating partnerships between universities (The University of Copenhagen *et al.*, 2022)

classified as ‘dual use’,[96] and state actors are increasingly intervening in or covertly influencing research.[97] This is increasing the need for and importance of knowledge security. Administrators, policymakers, researchers and support staff need to be fully aware of this importance, able to recognise risks and threats and know how to act. The quest for nuance and balance called for in the previous section is not an argument for doing nothing. Hard choices can and must be made not to engage in certain forms of collaboration or sharing, if the balance of different values and interests turns out negative.

We observe wide differences between and within knowledge institutes. While the awareness and skills around knowledge security are well developed in specific disciplines and at certain knowledge institutes (see also the boxes below), there are also places where this is not the case. This is because in many respects knowledge security does not sit easily with the culture and working methods of most knowledge institutes. It seems that not everyone is sufficiently aware of the changing context in which international collaboration takes place and of the increasing complexity this brings. Being properly prepared means anticipating future changes in the world. In reality, however, the theory and practice in relation to knowledge security is still fairly ‘immature’.

**Inspiration from experiences with measures at the Royal Netherlands Aerospace Centre**

The Royal Netherlands Aerospace Centre (NLR) identifies, develops and prepares high-grade technology for practical application. It qualifies as a ‘Large Technological Institute’ (GTI) in the Dutch Federation of Applied Research Organisations (TO2-federatie), acting as a linchpin between research, industry and government. In this role, NLR regularly works on commission for industrial companies (including Airbus and many others), the Ministry of Defence or the Ministry of Infrastructure and Water Management. These clients all take a different view of dissemination and openness. In particular, certain projects carried out for the Ministry of Defence entail major risks to national security if information ends up in the wrong place. NLR is configured in such a way as to manage these risks adequately, making it an interesting case study.

In a bid to avoid undesirable knowledge transfer, NLR takes a number of visible and invisible measures. For projects where commercial interests are at play, non-disclosure agreements (NDA) are used in almost all cases. An NDA may be drawn up unilaterally or bilaterally, on the initiative of NLR or of a client or stakeholder. Projects which are carried out in collaboration with the Ministry of Defence are often assigned

96 (Diercks, Deuten & Diederen, 2019; Evans, 2022)
97 (AIVD, MIVD, & NCTV, 2021)

a classification (national or NATO), which means they are subject to specific regulations. In practice, the classification is often Departmental Confidential, but projects are also carried out with a stricter confidentiality classification.

Between around 350 and 400 NLR staff are permitted to work on defence contracts, a significant proportion of whom regularly work with classified information. All NLR employees who work on defence contracts must therefore be vetted and hold a 'Declaration of No Objection' (VGB). To obtain a VGB, employees must undergo security screening; this is carried out by the national security services and therefore goes considerably deeper than a Declaration of Good Conduct (VOG). In 2021 the Security Screening Unit (UVO) and authorised agents carried out VGB screening on 51,354 individuals, of whom 388 were rejected.[98] Persons with a foreign nationality are almost never eligible for a VGB, implying de facto forced selection for entry to NLR.

The VGB for employees in research roles forms part of the regulations of the General Security Standards for Defence Contracts (ABDO),[99] which apply for NLR. This means there must be physical protection of the building (e.g. sufficient distance between the building and the perimeter fencing, building security and an identification requirement for visitors) and imposes standards for the digital environment (e.g. virus scanners, spam filters and an ICT environment managed entirely in-house). NLR also has ISO 27001 certification.[100] The reliability of the network (cybersecurity) is continuously monitored, including externally using a Bitsight score. Employees must also change their passwords every three months. These measures ensure that the sharing of technological knowledge held at NLR is kept to an absolute minimum (need-to-know), thereby reducing the risk of undesirable knowledge transfer.

No specific measures have been taken at NLR to prevent covert influencing. Equally, no special measures are in place to combat unethical practices during collaborative research (other than the Code of Conduct for Research Integrity) or on the use of research outcomes. The government is the lead partner at NLR, which means that the organisation aligns with government policy on ethical issues concerning technological developments. Ethics is an increasingly common topic of conversation among employees, for example in relation to research collaboration with countries with a doubtful human rights record. The Code of Conduct for Research Integrity also

98 (AIVD, 2022)
99 (Ministerie van Defensie, 2019)
100 https://www.iso.org/isoiec-27001-information-security.html

applies for (employees of) NLR. The Code was publicised when it was introduced, but it is not known how many NLR staff are actively familiar with it.[101]

### Lack of options for action

The measures currently being taken are primarily focused on prevention: identifying and mitigating risks in advance. This is the theme of many of the queries received by the Knowledge Security Resource Centre. A next step is to give people the skills to act in international collaborations that are not risk-free but are still desirable. The stakeholders must then be capable of breaking off a collaboration in an orderly manner in the event that a high-risk trajectory emerges. This can be compared with the approach to cybersecurity, in which the initial focus is on raising awareness and subsequently shifts turn to detecting and intervening in incidents that arise.

At present, proportionally less attention is devoted to the skills needed to detect and intervene in relationships or projects which have the potential to become problematic. What should a researcher do, for example, if he or she suspects that a colleague in the Netherlands or abroad is unable to perform research freely or is being put under pressure? What are the financial and relational consequences of terminating contracts or collaborative projects? These questions are taken seriously in Australia, for example, where universities are encouraged to organise training for researchers in strengthening scientific integrity and recognising and logging foreign interference.[102]

As well as improving the awareness, skills and action perspectives, attention is also needed for identifying and grasping (safe) opportunities.[103] The question then is what type of collaboration can be entered into without significant risks.

#### Inspiration from experiences with measures and skills at the Advanced Research Center for Nanolithography (ARCNL)

The Advanced Research Center for Nanolithography (ARCNL) is a public-private organisation which was set up in 2014 by the Dutch Research Council (NWO) in partnership with the University of Amsterdam, VU Amsterdam and ASML (producer of equipment used in the manufacturing of semiconductors). Groningen University joined the partnership in 2022. ARCNL commenced after winning a tender put out by ASML in 2013 in a bid to found a new research institute that could supply the company with fundamental knowledge. Since 2015 it has been an autonomous research institute

101 (KNAW *et al.*, 2018)
102 (d'Hooghe & Lammertink, 2022, p. 49)
103 (d'Hooghe *et al.*, 2018)

and part of the NWO institutes portfolio. ARCNL engages in fundamental physics and chemistry research focusing on technologies for (nano)lithography, mainly for the semiconductor industry.

ARCNL is at the interface of the academic and industrial fields. Scientific articles are published and peer-reviewed, research group leaders deliver lectures at universities, and the institute submits scientific contributions to international conferences. The research questions addressed are driven primarily by applications used by the industrial partner ASML, which benefits from the flow of ideas generated by the research.

Its unique (knowledge) position means ARCNL acts like a spider in a web which extends beyond (nano)lithography. ARCNL works with a large number of partners from a range of fields. Its researchers are also drawn from all over the world. The sensitive knowledge and technology on which ARCNL carries out research means that knowledge security is a topic that receives a lot of attention.

ARCNL deals with potential risks in various ways. New staff are subject to pre-screening, and a risk assessment is carried out based on a set of signals or triggers. This determines not only whether someone is taken on, but also the areas of research and the meetings to which they are given access. This is discussed in advance with the new colleague.

ARCNL employs the same approach when it comes to safeguarding knowledge and technology. Before research results are published, they are screened by a board of experts from a variety of disciplines. They consider whether the results could lead to commercially relevant applications, and if so a patent is first applied for.

ARCNL also practises data protection. Data is compartmentalised and shielded per individual research group. Access to data is also restricted. Finally, the building itself is protected: not all parts of the building are freely accessible and all offices can be locked. Employees are aware that not everyone has access to all areas, and are alert to any unusual situations.

# 3

# Three recommendations for a learning approach to knowledge security

**AWTI has three recommendations for improving the approach to knowledge security. They offer a layered and practical means of working towards the development of a learning approach, with permanent attention for nuance and awareness-raising. They are focused on the conceptualisation, differentiation, and realisation of an approach to knowledge security.**

A learning approach to knowledge security will enable Dutch knowledge institutes deal more effectively, now and in the future, with the complex challenges of international collaboration in knowledge development and higher education. A focus on learning is important, because it is an illusion to imagine that the Netherlands will get its policy on knowledge security right first time in a constantly changing world. That need not be a problem, as long as the approach is designed in such a way that it can incorporate lessons learned about what works and what does not. An approach such as this addresses the issue of growing complexity without unnecessarily undermining the value of international collaboration. By definition, such an approach requires continual attention.

AWTI believes that promoting knowledge security is primarily a responsibility of the government, in partnership with knowledge institutes; the different national interests and perspectives regarding knowledge security and related themes come together at government level and are weighed against each other. This report is accordingly focused mainly on the government. However, it is also directed towards knowledge institutes, which is where a learning process in relation to knowledge security will have to be implemented. It is vital that expertise and measures are developed in the context of the actual research and researchers. This needs to happen close to researchers, because familiarity and trust are important for a discussion of this topic, as is familiarity with of research practice. This demands leadership from within the sector itself. If a bottom-up approach makes insufficient progress, this will ultimately lead to a less nuanced, more restrictive top-down response from the government.

In developing the recommendations, AWTI drew on the results of the LeidenAsiaCentre (LAC) study on the approach to knowledge security taken in other countries.[104] The study's main conclusion is that an effective approach benefits from a coherent and pragmatic set of measures, good coordination between stakeholders, and government

104 (d'Hooghe & Lammertink, 2022)

support for bottom-up activities by knowledge institutes. These lessons are built into our recommendations.

The three parallel recommendations refer to different ‘levels’ where action is needed, resulting in a layered approach. Recommendation 1 is focused on gaining a better understanding of knowledge security in relation to other important themes and developments in other countries. This recommendation is aimed mainly at the government, working in partnership with knowledge institutes, but is intended to generate a broad debate to foster the conceptualisation of knowledge security among public authorities, knowledge institutes, security services, diplomatic posts and think tanks.

Recommendation 2 is about developing a professional, differentiated approach for the Netherlands. Here, too, the government needs to take the lead, but knowledge institutes, security services and other experts (for example on integrated security) also need to be aligned and involved. The approach specifies and operationalises the concept of knowledge security and defines a number of measures. This fits in with the need for a coherent set of measures and coordination between stakeholders.

Recommendation 3 targets knowledge institutes and stresses the need for changes in the thinking and actions of researchers, administrators, support workers, policy staff and managers. This aligns with the need for a pragmatic set of measures. Government plays a supporting role here, in line with the observation in the LAC study that government support for bottom-up initiatives from the sector contributes to effective policy.

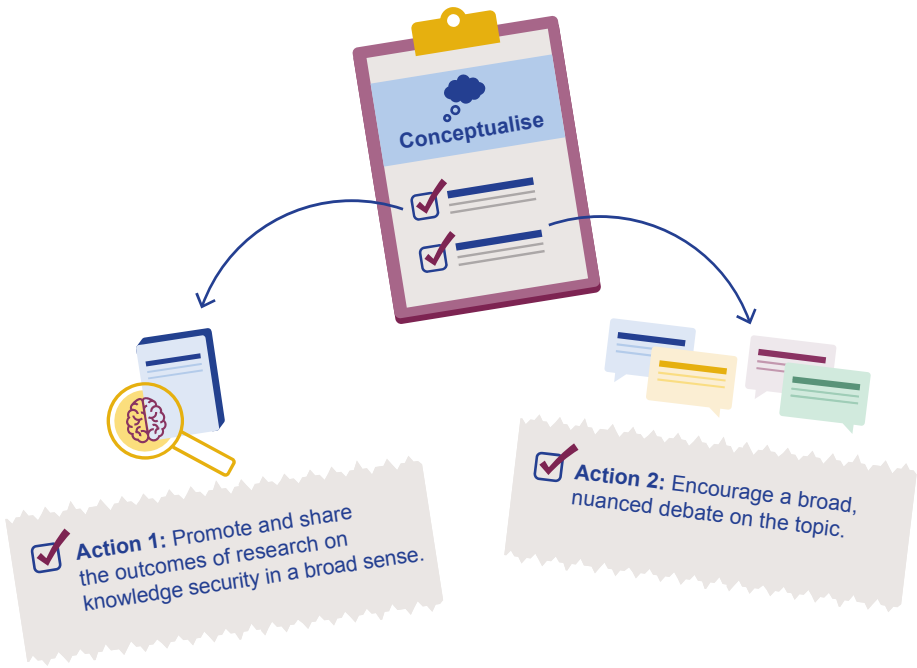
The recommendations to develop a learning approach are layered and also interact with each other, but if the maximum learning outcomes are to be realised it is however essential that they be implemented simultaneously and interactively, and not sequentially.

**Advice.** Simultaneous implementation of the three recommendations by government and knowledge institutes will lead to a shared learning approach.

## Recommendation 1. Conceptualise: improve the understanding of knowledge security

The theory and practice around knowledge security is still in its infancy and is therefore susceptible to unilateral criticism from specific perspectives (see section 2.1). The government, in collaboration with knowledge institutes, therefore has a leading role to play in the further development of the concept of knowledge security in all its facets and in striking a balance between different values and interests. The debate about themes and values is never over, but still needs to take place. Conceptualisation is crucial for the approach to knowledge security and forms the basis for awareness-raising, recognising and mitigating risks and identifying opportunities for collaboration.

**Recommendation 1.** Conceptualise: improve the understanding of knowledge security.




To ensure a broadly supported and fuller understanding of what knowledge security is, two specific actions are needed from the government:

### Action 1. Promote and share the outcomes of research on knowledge security in a broad sense

Research on knowledge security is gradually getting off the ground in the Netherlands and elsewhere.[105] It enriches and underpins the conceptualisation of knowledge security and illustrates how it relates to other themes such as open science, internationalisation, strategic autonomy[106] and scientific integrity. At present, the relationships and mutual dependencies between these concepts are insufficiently clear. The international study by the LeidenAsiaCentre (LAC) shows that other countries take different views on the conceptual fundamentals of an approach to knowledge security; some countries start from a security perspective, others from a perspective of scientific integrity.[107] In addition, the intuitive differences between disciplines in terms of risks (e.g. drone technology versus research on human rights) have barely been mapped at all in terms of knowledge security. It is advisable to intensify innovative conceptual and empirical research on knowledge security, given the challenging and dynamic nature of the topic.[108] Evaluation research on knowledge security policy and measures is also sorely needed. Measures and practices that have proved effective can then be incorporated in the professionalising of the approach at knowledge institutes and public authorities (see Recommendation 2).

### Action 2. Encourage a broad, nuanced debate on the topic

Knowledge security policy is not just an intellectual question, but also most definitely involves a normative judgement. Making that judgement requires that different values are brought together. There is a heated debate across the media and politics, but there are also signs of a nuanced discussion. In other countries, too, there are warnings against forcing the debate to the extremes, primarily to avoid researchers withdrawing from the debate. In France, a Parliamentary report on scientific heritage and academic freedom played an important role in encouraging the public debate (see Box below).[109] There are also those who argue for a clearer formulation of the risks in order to raise awareness.[110] AWTI argues for a nuanced debate because this fits in with the phase of development of the policy.

---

105 (Van der Wende & Kirby, 2020; d'Hooghe, 2021; Wellerstein, 2021; Clark, 2022; De Bruijn *et al.*, 2022; OECD, 2022; Shih, 2022; Snetselaar, 2022)
106 Strategic autonomy is in fact itself a concept which has not yet been fully defined.
107 (d'Hooghe & Lammertink, 2022, p. 51).
108 This topic is an ideal subject for interdisciplinary research (AWTI, 2022). Examples might include research on research practices, research on publication patterns, research on risks and threats. See also (Hudson *et al.*, 2022, p. 3).
109 (d'Hooghe & Lammertink, 2022, p. 21)
110 (d'Hooghe & Lammertink, 2022, p. 48).

### Report by French Parliament on better protection for scientific heritage and academic freedoms

The report by André Gattolin entitled *Mieux protéger notre patrimoine scientifique et nos liberte's académiques* ('Better protection for our scientific heritage and academic freedoms')[111] was written as a result of a 2021 initiative by the *Rassemblement des démocrates, progressistes et indépendants* ('Rally of Democrats, Progressive and Independent Group', RDPI). The report describes non-European state influences and their impact on French knowledge institutes, and draws attention to the reality of this threat. The aim of the report's authors is to prepare knowledge institutes for what they describe as one of the greatest challenges of the 21st century: maintaining and safeguarding the French scientific heritage, academic freedom and scientific integrity. The report describes the threat and the weaknesses in the French system and offers a framework for assessing external influences, the impact of foreign powers on the university sector and the associated government policy.

The report shows that every measure taken to protect the French academic sector requires a complex weighing of interests. On the one hand there is an academic tradition in which knowledge and ideas circulate freely, while on the other there are new strategies, designed for the long term and implemented with substantial funding by governments which can sometimes be regarded as 'hostile'. The report calls for differentiation, arguing that the response to foreign interference must be 'multi-variable' and scalable to reflect the fact that the strategies of foreign actors can change and are focused precisely on exploiting weak spots. The report lists five goals, together with a total of 26 (more) specific proposals. The overarching goals are as follows:

- Making the problem of foreign intervention a political priority;
- Protecting academic freedoms whilst respecting academic autonomy;
- Making transparency and reciprocity in international scientific collaboration a matter of national interest;
- Strengthening the administrative procedures used to oversee partnerships with higher education establishments and research institutes;
- Promoting a reference document of norms and guidelines nationally, internationally and in Europe.

The report, with its specific proposals, played a key role in stimulating the public debate.[112]

111 (Gattolin, 2021)
112 (d'Hooghe & Lammertink, 2022, p. 21)

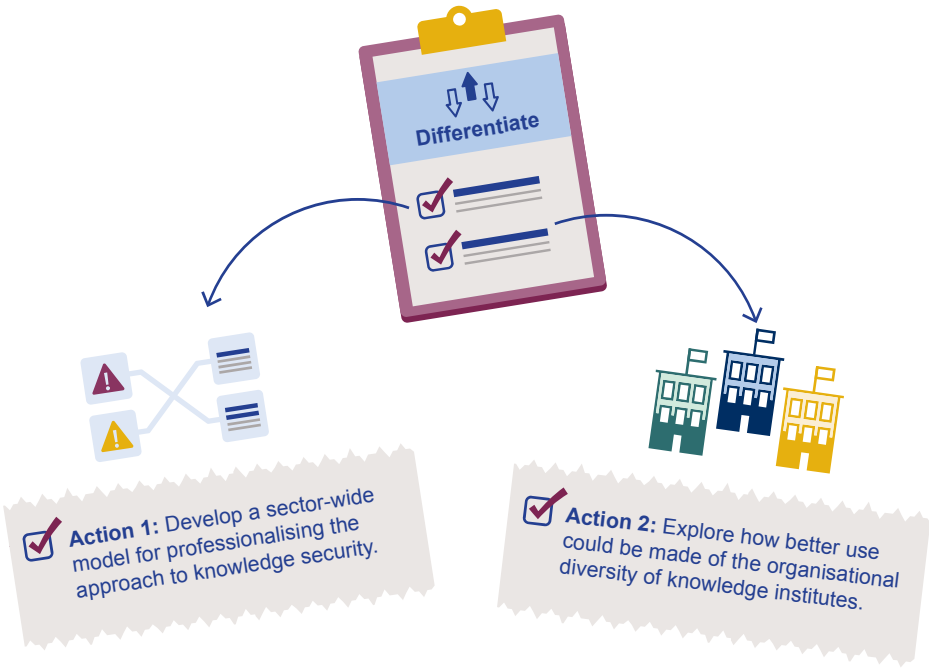
The actions proposed in this first recommendation have an international dimension, because the conceptualisation of knowledge security is also insufficiently developed in Europe. Tensions are increasingly arising between promoting global collaboration on research and innovation, in which alignment is sought with other countries,[113] and activities to foster open strategic autonomy,[114] whereby one-sided or undesirable dependencies are minimised. The concept of (open) strategic autonomy also needs to be fleshed out more fully: there is currently no consensus on what it means precisely.

## Recommendation 2. Differentiate: in risks, measures and organisations

The Netherlands needs an approach to knowledge security which both clarifies and differentiates. Clarity is needed in the sector so that researchers know what they can and cannot do. Differentiation means that mitigating measures are deployed proportionately, whereby opportunities and risks will depend on the type of research, the data used, social context and collaboration partners, and on influencing conscious and unconscious behaviour (see section 2.2). Top-down, binary, binding rules generally provide too little scope for this differentiation and nuance. An approach is therefore needed which incorporates a wide array of knowledge, internalises the weighing of different national interests and offers practical tools for knowledge institutes to professionalise knowledge security. Our second recommendation accordingly directly aligns with the conclusion of the LAC background study calling for a coherent and pragmatic set of measures. This differentiation will be made easier if better use is made of the organisational diversity of the knowledge institute landscape. Creating a structure for the knowledge and skills relating to knowledge security will help in professionalising the approach and maintaining cool heads.

113 (European Commission, 2021b)
114 (Molthof, Zandee & Cretti, 2021)

**Recommendation 2.** Differentieer: in risico's, maatregelen en organisaties.




Two actions are required from the government in order to achieve a differentiated approach:

### Action 1. Develop a sector-wide model for professionalising the approach to knowledge security

A sector-wide model distinguishes between different domains of knowledge security and defines which type of measures, agreements and systems are appropriate for mitigating the risks in each domain. Our proposal is based on the Capability Maturity Models that are used in cybersecurity (see Box below). Domain-specific goals for knowledge security include preventing undesirable knowledge transfer, collaboration based on reciprocity, combating self-censorship or preventing financial dependencies. These highly diverse aspects of knowledge security require specific measures. Improving the conceptualisation of knowledge security (Recommendation 1) will help in identifying the domains. This is not a one-off action, but requires continual attention and adaptation.

Involvement of different stakeholders is important in developing such a model. These stakeholders are both within and outside the knowledge sector, for example the security services and the Ministry of Foreign Affairs. They possess crucial knowledge and expertise to make the model effective and legitimate.[115] Publicly available information (such as the Threat Assessment for State Actors) and non-public information can form input for the model. The model brings together the available knowledge and expertise on the topic and makes the responsibilities explicit.

The model can be used by different functional entities within knowledge institutes, such as a department or a research group. It is crucial to recognise that not every risk within a domain is present to the same degree for each functional entity; that will depend on factors such as the particular research field, the potential applications for the knowledge, the research group's collaborations and the data used (see the discussion of differentiation in section 2.2). Everyone can therefore use the same model, but adapts it to their specific context. The model implies a layered approach (at research group level, institute level, in interaction with relevant actors outside the institute), thus enabling escalation to different levels within and outside the institutes.

The model then defines different levels indicating how well developed the approach to a given risk is. The maxim of less is more applies here: the aim is to mitigate the risks adequately with minimal intervention. Where there are no risks, therefore, no measures are taken. Where risks are present, a number of different levels are distinguished: the Maturity Indicator Levels. The specific context of a department or research group determines which level is needed. The aim is thus to achieve a situational balance of risks, opportunities and measures.

### Capability Maturity Model[116]

A Capability Maturity Model is a set of indicators to measure the capability and maturity of a specific sector. It is a descriptive rather than prescriptive model. It is used among other things to improve cybersecurity in crucial sectors. The model generally consists of best practices and practical standards.

To measure capability, the model uses a scale that defines the 'Maturity Indicator Level' or MIL. This describes how mature an organisation or organisational unit is in different security domains. Organisations can use the scale to measure their current

115 Experiences in the United Kingdom are interesting in this context. Good consultation has ensured that the guidelines for security services, universities and research funders are closely aligned (d'Hooghe & Lammertink, 2022, p. 49).
116 (Muneer, 2022)

capability, possibly in comparison with others, and may be able to identify scope for moving to the next level.

The goal is not necessarily to strive for the highest MIL; the key is to achieve the right level, given the attendant risks. This requires continual judgements and weighing of relevant factors.

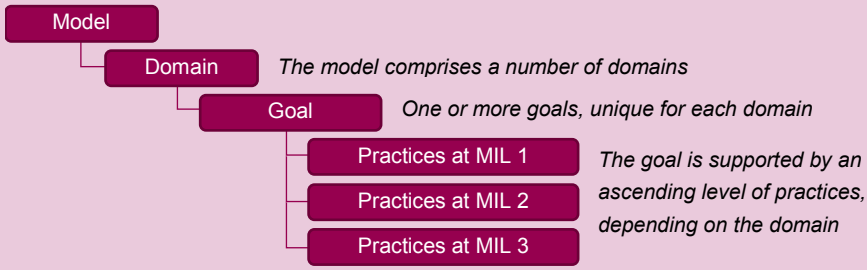



Figure 1. Model, domain, goals and practices in a Capability Maturity Model[117]

***Model structure*** The model comprises several domains. The practices within a domain are grouped based on goals which support the domain. Practices represent the activities carried out by an organisation to establish a certain capability in the domain. The model explains the goals for each domain, in a summary of the primary intention of the domain. The goal for the domain 'risk management', for example, could be 'establishing and maintaining plans and procedures to identify, analyse and manage risks in line with the goals of the organisation.'

The Capability Maturity Model is thus a coherent and generally usable model which makes possible differentiation in measures to monitor knowledge security. The model helps prevent malign actors from exploiting the 'weakest link' in the Dutch or even European research ecosystem. It also gives knowledge institutes and their component entities a way of comparing themselves with other organisations. And it contributes to collaboration, knowledge-sharing and the avoidance of competition for lucrative but potentially undesirable contracts.[118] Unlike binding and generally applicable lists of countries or disciplines, this approach allows scope for differentiation and contributes to a learning attitude (reflexivity) on the part of knowledge institutes (e.g. using benchmarks). The lists of high-risk disciplines, countries or organisations can however provide input for the model. Moreover, the model does not have to be built from scratch; it can get off to a

117 Figure taken in simplified form from (Muneer, 2022)
118 This form of competition between knowledge institutes is the Achilles heel of an approach to knowledge security. See also the best practices in (d'Hooghe & Lammertink, 2022, p. 49).

flying start by drawing on the national knowledge security guideline, as well as existing risk analyses and tools.

### Action 2. Explore how better use could be made of the organisational diversity of knowledge institutes in the Netherlands for the benefit of knowledge security

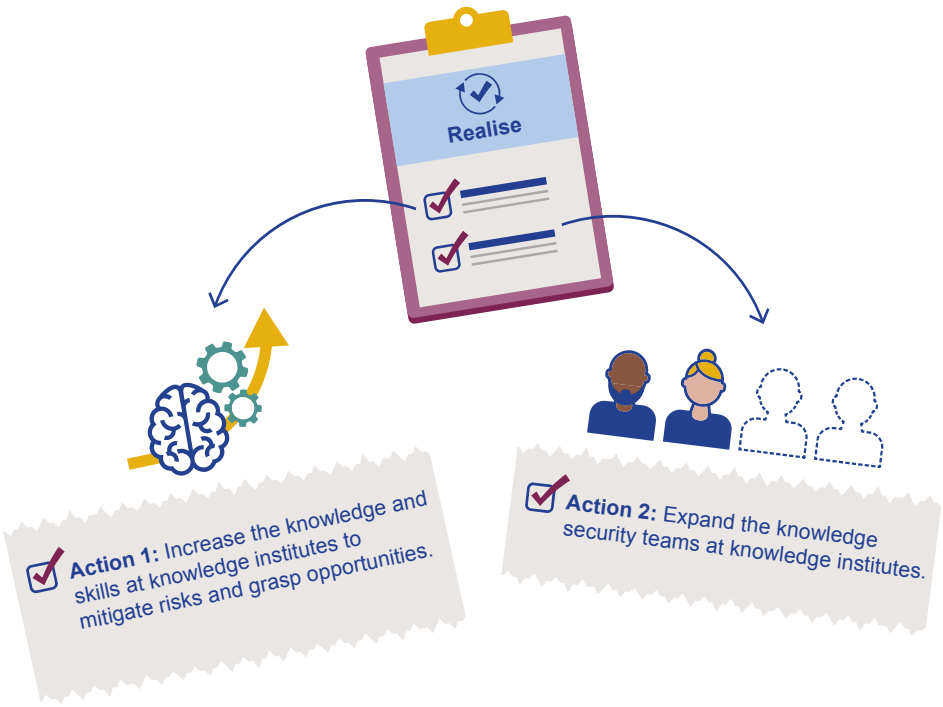
The Netherlands has a diverse landscape of knowledge institutes, focusing to a lesser or greater degree on practical application and built around different disciplines or thematic lines. AWTI has previously described this diversity as valuable.[119] Better use could be made of this diversity, including for knowledge security. An example can illustrate this: in the US, research that is designated as 'classified' is placed with national research institutes (National Laboratories), where security can be monitored more effectively. In the Netherlands, this kind of research could be transferred from one knowledge institute to another which is better equipped to mitigate knowledge security risks. The type of research and the associated risks would then be more closely aligned with the organisational features of the knowledge institute, for example because of a more rigorous approach to knowledge security. Separate legal entities – linked to but separate from the knowledge institute – could also take additional security measures which cannot readily be carried out by the knowledge institute.

## Recommendation 3. Realise: increase awareness and capacity

The awareness and capacity (knowledge and skills) in relation to knowledge security are currently underdeveloped (see section 2.3). AWTI therefore recommends that knowledge institutes devote a good deal of attention to this. The professionalisation model (Recommendation 2) provides key input for developing and implementing measures, agreements and security systems. Developing and implementing the model takes time, and we advise knowledge institutes not to wait for this; in fact, the experience being gained now at knowledge institutes can serve as input for the model.

119 (AWTI, 2017a)

**Recommendation 3.** Realise: increase awareness and capacity.




We recommend two actions to make knowledge institutes more competent as regards knowledge security:

### Action 1. Broaden and deepen the awareness, knowledge, and skills at knowledge institutes to mitigate risks and grasp opportunities

Individuals at various locations within knowledge institutes need to be aware of the new risks that are arising as a result of geopolitical changes. As well as greater awareness, knowledge security demands new skills and instruments, such as enhanced due diligence, screening procedures, checklists and data protection. We recommend that knowledge institutes gather expertise and disseminate it internally and externally, drawing on knowledge and external information.[120] Internal and external training on knowledge

120 In our interviews we heard that some knowledge institutes are already well advanced in this regard, see e.g. (De Bruijn, 2021), while others are not.

security should figure more frequently in the training of researchers. The international comparative study carried out by the LeidenAsiaCentre (LAC) makes clear the importance of material and non-material support from the government.[121] We accordingly recommend that the government support knowledge institutes with information, advice and resources, in order to create genuine scope to invest in prevention, detection and action in the event of problems around knowledge security. This support will prevent the extra attention needed for knowledge security from needlessly increasing the pressure of work on researchers. An awareness-raising campaign would be a good practical step here. The (national) Trusted Research Campaign in the UK could serve as a model for Dutch knowledge institutes (see Box below).

**Trusted Research Campaign**

The Trusted Research Campaign was developed by the Centre for the Protection of National Infrastructure (CPNI) and the National Cyber Security Centre (NCSC) on behalf of the British government. The aim is 'to raise awareness of the risks associated with research collaborations that involve organisations or research partners with links to nations whose democratic and ethical values are different from our own'; 'our' obviously refers to the UK.[122]

Trusted Research entails an approach aimed at safeguarding the integrity of the system of international research collaboration, which is regarded as essential for the continued success of the British research and innovation sector. Trusted Research includes guidelines and guidance for both the academic and industrial sectors, both of which were involved in drawing up the advice.

The guidelines can be found on the CPNI website (https://www.cpni.gov.uk/trusted-research) as well as in various downloadable documents. The material is supported with infographics, checklists and references to existing measures intended to help readers assess sensitive research or make strategic judgements.

### Action 2. Expand the knowledge security teams at knowledge institutes

Knowledge security teams play an important role within knowledge institutes. The problems they encounter are complex, and increasing their expertise and capacity is important to enable them to provide good and authoritative (or even binding) advice

121 (d'Hooghe & Lammertink, 2022)
122 (UKRI, 2021; d'Hooghe & Lammertink, 2022, p. 36; Karásková, Šebok & Blablová, 2022; CPNI, undated).

within their institute. This expansion could take the form of a network or a committee,[123] whose task would be to advise researchers, deans and other decision-makers on collaboration, funding and recruitment. They would have a direct line of communication to the board of the institute. Expanding these teams would give researchers more 'cover' - not with a view to minimising the risks, but to enable balanced decisions to be taken.

It is crucial that expertise around knowledge security develops at knowledge institutes, in close proximity to researchers and their research, and with sufficient account taken of the academic perspective. Physical, social, and organisational proximity contributes to mutual trust and understanding, which are essential when dealing with sensitive topics such as knowledge security. A national centre for knowledge security would be too detached from the sensitivities or diversity of issues within individual knowledge institutes.

The expanded knowledge security teams would not operate in isolation, but would be in close contact with the government, for example via the Knowledge Security Resource Centre and ongoing dialogue on knowledge security. The networks or committees would also need to be in contact with each other. There is a task here for the organisations within the Knowledge Coalition.[124] Setting up a consultation platform would be a practical implementation of this action.

123 (Rathenau Instituut, 2021)
124 https://kenniscoalitie.nl

# Appendices

# Appendix 1 Creation of this advisory report

This report was created in three phases. AWTI first carried out an exploratory study in the spring of 2022 on themes relating to knowledge security. We examined a number of typical knowledge security incidents, mapped the policy approach and talked to policy advisers, including from the Dutch Ministry of Education, Culture and Science and the Ministry of Economic Affairs and Climate Policy. This culminated in a memorandum setting out the steps to be taken in compiling this report.

In the next phase, a number of analyses were performed, starting with a stakeholder analysis. This was followed by an analysis of the underlying values in relation to knowledge security from differing perspectives (see Appendix 4). Thirdly, we compiled an inventory of the risks and threats in relation to knowledge security, based on several interviews and documents. Finally, an overview was compiled of policy instruments which impinge on knowledge security (see Appendix 3).

In parallel with the above activities, AWTI commissioned the LeidenAsiaCentre (LAC) to carry out an international comparative study on the measures taken by governments and knowledge institutes to promote knowledge security in other countries. This resulted in a separate study, which can be found on the AWTI website at www.awti.nl.

In the final phase, all the insights gained from the analyses were brought together, interpreted and worked up into an advisory report. A number of interviews were also conducted in this phase with stakeholders and experts, and meetings were attended and organised to validate the results and discuss the direction and fine-tuning of the report.

# Appendix 2 Interviewees

In compiling this report, discussions were held with a large number of interviewees from a wide range of organisations. We are grateful for their openness, time and knowledge. Some of the interviews took place during a meeting between AWTI and the Dutch Advisory Council on International Affairs in The Hague in early November 2022. During a working visit to Austria we spoke to eight experts, policymakers and researchers (not included in the list below). The researchers in the international study spoke to around 20 other individuals.

| | |
|---|---|
| ► Sebastiaan den Bak | Dutch Research Council (NWO) |
| ► Bibi van den Berg | Cyber Security Council (CSR); Leiden University |
| ► Bart van der Berg | Utrecht University |
| ► Nora van Bracht | Ministry of Education, Culture and Science |
| ► Jan Broeks | Advisory Council on International Affairs |
| ► Nienke Buisman | European Commission |
| ► Mirta Cugini | Datenna |
| ► Aad van Dorp | Royal Netherlands Aerospace Centre (NLR) |
| ► Juul van Ewijk | Ministry of Education, Culture and Science |
| ► Marjan Fretz | Advanced Research Center for Nanolithography (ARCNL) |
| ► Sven Hamelink | National Police Corps |
| ► Jennifer Herek | University of Twente; European Association of Universities of Applied Sciences (CESAER) |
| ► Gareth Heywood | Datenna |
| ► Just van den Hoek | Netherlands house for Education and Research (Neth-ER) |
| ► Ingrid d'Hooghe | Clingendael Institute, LeidenAsiaCentre |
| ► Hans van der Jagt | Advisory Council on International Affairs |
| ► Marenne Jansen | Advisory Council on International Affairs |
| ► Katleen Janssen | KU Leuven |
| ► Luuk Klomp | Dutch Research Council (NWO) |
| ► Linda Krom | Netherlands Organisation for Applied Scientific Research (TNO) |
| ► Willemijn Lamet | Universities of The Netherlands |
| ► Floris Lantzendörffer | Ministry of Economic Affairs and Climate Policy |

| | |
|---|---|
| Nina van Lanschot | EclecticIQ |
| Erwin Mededorp | University of Twente |
| Max Bueno de Mesquita | Ministry of Education, Culture and Science |
| Irna van der Molen | University of Twente |
| Marc Moquette | Ministry of Foreign Affairs |
| Mirko van Muijen | Ministry of Education, Culture and Science<br>European Commission |
| Karen Passier | Ministry of Economic Affairs and Climate Policy |
| Jolanda Peters – van Nieuwenhoven | Tilburg University |
| Jet de Ranitz | SURF collaborative organisation for IT in Dutch education and research |
| Miriam Roelofs | Foundation for Dutch Scientific Research Institutes (NWO-I) |
| Joep Roet | Netherlands house for Education and Research (Neth-ER) |
| Amber Schilte | Ministry of Education, Culture and Science |
| Henne Schuwer | Advisory Council on International Affairs |
| Haroon Sheikh | Netherlands Scientific Council for Government Policy (WRR) |
| Joris Teer | The Hague Centre for Strategic Studies |
| Maarten Tossings | Netherlands Organisation for Applied Scientific Research (TNO) |
| Peter Weijland | TU Delft |
| Marijk van der Wende | Utrecht University |
| Hans de Wit | Boston College |
| Dick Zandee | Clingendael |
| - | General Intelligence and Security Service (AIVD) |
| - | Military Intelligence and Security Service (MIVD) |
| - | National Coordinator for Security and Counterterrorism (NCTV) |

# Appendix 3 Overview of measures related to knowledge security

This Appendix contains an overview of existing measures related to knowledge security. Although broad, it is not exhaustive. The measures are broken down according to the following themes:

- Measures to prevent knowledge dissemination that is harmful to national security;
- Measures to strengthen and protect knowledge development for the Dutch economy;
- Measures to protect against foreign interference;
- Measures to counter misuse or ethics dumping.

Some measures are covered by more than one theme and therefore occur several times.

### Measures to prevent knowledge dissemination that is harmful to national security

- Help is provided to companies and knowledge institutes in taking measures to counter cyber attacks. The National Cyber Security Centre (NCSC) is the national expertise centre in the Netherlands aiming to safeguard the digital resilience of Dutch society, and undertakes a range of activities to this end. For vital companies, there are special organisations to help, while for less vital businesses there is the Digital Trust Centre. For knowledge institutes, SURF is the recognised body for strengthening cyber security.
- Stealing knowledge is a criminal offence. Dutch legislation on espionage was modernised in 2022,[125] with the aim of improving the ability to tackle new forms of espionage. Infringements of state or commercial secrets were already criminal offences, but the new legislation adds jeopardising national security and personal safety.
- Companies and knowledge institutes that are involved in defence contracts must take security measures. They must adhere to the General Security Standards for Defence Contracts (ABDO) to protect sensitive information.[126] The Military Intelligence and Security Service (MIVD) oversees this.
- Companies and knowledge institutes must comply with export legislation in respect of dual use goods, i.e. goods with both civil and military applications (e.g. a product that can be used as a fire retardant in the construction industry but can also be used

125 (Ministerie van Justitie en Veiligheid, 2022)
126 (Ministerie van Defensie, 2019).

for the production of poison gas).[127] These 'goods' also include knowledge, with the exception of 'fundamental scientific research'. The policy is set at European level and regularly updated (most recently in December 2019). The long, detailed list of goods in the European Regulation is drawn up in accordance with international agreements with parties including Australia Group, the Missile Technology Control Regime (MTCR), the Nuclear Suppliers Group (NSG), the Wassenaar Arrangement and the Chemical Weapons Convention.

- A security test is being developed for investments, acquisitions and mergers pursuant to the Investment, Mergers and Acquisitions (Security Screening) Act ('Wet vifo').[128] This test applies for companies which are vital providers or which possess sensitive knowledge or technology. The Act was developed to prevent 'malign parties' gaining control of companies which possess technology that poses a military or strategic risk to national security. Both the investors and the companies themselves must report changes in the control structure to the Dutch Ministry of Economic Affairs and Climate Policy. A dedicated unit assesses whether the change poses a risk to national security.
- Knowledge institutes must comply with two knowledge embargoes.[129] To prevent knowledge on building missiles and nuclear weapons ending up in Iran or North Korea, everyone involved in studies or research in this field must apply for a dispensation. The supervision of this legislation was tightened up in 2018 through the Undesirable Knowledge Transfer Task Force.[130]
- The Code of Conduct for Research Integrity requires researchers to abide by a number of guiding principles: honesty, due care, transparency, independence and responsibility. As well as applying methodological standards for the quality of the research, there are also ethical standards, covering the (ethical or strategic) risks of placing data in the public domain.
- A number of additional measures have been taken in the past year as part of the knowledge security policy aimed at helping prevent undesirable knowledge transfer with regard to national security. The first of these is a national guideline intended to help raise awareness, and offering practical tips. The second is a Knowledge Security Resource Centre where researchers and knowledge institutes can go if they

127 (Ministerie van Buitenlandse Zaken, 2018)
128 (Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid, 2022b)
129 https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies
130 (Heerschop & Riedstra, 2021)

have specific questions.[131] Third, knowledge institutes are required to appoint an officer and policy team with responsibility for knowledge security. Fourth, all knowledge institutes must carry out a risk analysis on international collaboration. Fifth is the announcement of an external audit of the knowledge security policy at knowledge institutes. Finally, an assessment framework has been announced (expected in 2023) whereby individuals from 'third countries' must seek permission to study or work in sensitive knowledge domains in the Netherlands.

### Measures to strengthen and protect knowledge development for the Dutch economy

- In broad terms, Dutch research and innovation policy is aimed at keeping industry innovative and competitive enough to deal with economic competition from other countries. Research and innovation within and from Europe is also encouraged, for example via Horizon Europe.[132] One question that is currently in play is to what extent non-EU member states are permitted to participate in European industrial alliances. By way of illustration, China is excluded from this, and collaboration only takes place with 'like-minded countries'.
- Companies are encouraged to do business internationally, from the point of view of both economic development and development cooperation.
- To strengthen crucial areas of technology, the Netherlands and Europe encourage knowledge development in those areas, for example through the Key Technology Policy and the National Growth Fund. The EU has a policy on Key Enabling Technology,[133] and recently published the European Chips Act.[134]
- The European Commission has begun a programme of Important Projects of Common European Interest (IPCEIs).[135] These allow more generous public funding for certain ecosystems. To a certain extent, it marks a weakening of the state aid rules, provided certain conditions are met. It is related to the mission-driven innovation policy and European industry policy. The European Commission largely

131 https://www.loketkennisveiligheid.nl/
132 There is however an inherent tension in this policy, because on the one hand it encourages collaboration with other countries to foster knowledge development, competitiveness and for geopolitical reasons, with the attractiveness of Europe being used to tempt third countries to collaborate; on the other hand, Europe also takes a critical stance on which countries are eligible for that collaboration. See also (European Commission, 2021b; Molthof, Zandee & Cretti, 2021; Roet, 2022)
133 (Müller & Potters, 2019)
134 (European Commission, 2022)
135 https://www.rvo.nl/subsidies-financiering/ipcei

determines the topics of research. The Commission is also looking at the possibility of relaxing the merger policy to allow the emergence of 'European Champions'.[136]

- Another measure concerns the embedding of technological standards of European internal market rules.[137] These standards compete with other standards on the international market, and pushing through European standards therefore offers strategic advantages for European industry and could increase economic competitiveness.
- Dutch and foreign companies are encouraged (to continue) to establish in the Netherlands in order to strengthen the Dutch economy and knowledge position.[138]
- The knowledge position of companies and knowledge institutes is internationally protected by intellectual property laws.
- The European Commission is preparing an 'anti-coercion instrument',[139] which sets economic standards for companies in order to put governments under pressure. Reciprocity is the principal here (if European companies do not have access to a foreign market, that country is also barred from accessing the European market).
- Statutory, sector-specific investment tests apply in order to protect crucial and vital sectors. These already existed for the electricity, gas and telecommunications sectors and are being expanded through the new Investment, Mergers and Acquisitions (Security Screening) Act (Wet vifo).[140]
- The knowledge security policy referred to earlier also helps raise awareness about the risks of knowledge transfer. This also has an impact on economic competitiveness and stability.

### Measures to protect against foreign interference

Foreign actors try to influence organisations or persons in the Netherlands and thus to undermine the scientific, social, democratic and social processes of society. The rise of autocratic countries is exacerbating this problem for knowledge institutes in the Netherlands.

136 (AIV, 2022, pp. 27–28)
137 (Lippert & Perthes, 2020)
138 (Minister van EZK, 2022)
139 (European Commission, 2021a)
140 (Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid, 2022b)

- The Code of Conduct for Research Integrity requires researchers to abide by a number of guiding principles: honesty, due care, transparency, independence and responsibility. The Code is intended to protect against foreign intervention.[141]
- The cyber security policy referred to earlier seeks to counter covert interference via digital means.
- The General Data Protection Regulation (GDPR) protects the personal data of European citizens.[142]
- The government's knowledge security policy also includes measures to counter foreign interference. In particular, there is the 'knowledge security guideline[143], the Knowledge Security Resource Centre[144] and the mandatory risk analysis.[145] These measures are aimed among other things at preventing vulnerabilities to foreign interference.

### Measures relevant for countering ethics dumping or misuse

Although the vast majority of the research community works in accordance with high ethical standards, there are also places in the world where compliance with those standards is less rigorous. Ethics dumping is the use of low ethical standards in research, for example in the area of animal testing or medical ethics standards. Misuse involves exploiting knowledge for unethical purposes, where the knowledge is misused against people or animals anywhere in the world. It may involve military actions, but also other forms of unethical practices, such as surveillance, repression or torture.

- The legislation on exports of dual use goods and knowledge embargoes helps limit misuse, though here the main focus is on knowledge with (partly) military applications. Surveillance technology, for example, is not covered by this legislation.[146]
- The Code of Conduct for Research Integrity referred to earlier[147] helps counter ethics dumping or misuse. Research integrity is moreover the subject of international

141 (KNAW *et al.*, 2018)
142 https://gdpr-info.eu/
143 (Universiteiten van Nederland *et al.*, 2022)
144 https://www.loketkennisveiligheid.nl/
145 (Minister van OCW, 2022a)
146 (Gildea & D'Alessandra, 2022)
147 (KNAW *et al.*, 2018)

agreements through the Singapore Statement on Research Integrity, ALLEA[148] and the UNESCO statement on Science and Scientific Researchers.[149]

- The Nagoya Protocol promotes the careful use of genetic material. Lack of care in the use of such material can undermine human rights. In the Netherlands, the Food and Consumer Product Safety Authority (NVWA) supervises companies and knowledge institutes that work with genetic material to ensure that they do so with all due care.[150]
- The aforementioned knowledge security policy, including the guideline, the Knowledge Security Resource Centre and the risk analyses carried out in recent years aim to make researchers and knowledge institutes more aware of the risks of misuse or ethics dumping.

148 (ALLEA, 2017)
149 https://en.unesco.org/themes/ethics-science-and-technology/recommendation_science
150 https://www.nvwa.nl/onderwerpen/nagoya-protocol

# Appendix 4 A reflection on underlying values from three perspectives

The debate about knowledge security regularly refers, either implicitly or explicitly, to values. Values are things that are assumed to contribute to the 'good'. For example, we assume that academic freedom contributes to good science.

Seen from this perspective, it is also possible to perform a value analysis, which examines from three perspectives which values are relevant for safe knowledge development in a changing geopolitical context. In other words, how do the present international (geo)political developments jeopardise those values and how might they be protected by policy? The three perspectives are security, economic and academic.

Our interviews showed that people approach knowledge security from different perspectives and disciplines. People also sometimes talk to each other, but have so far not come to a coherent view of the problem. Different underlying values sometimes appear to contradict each other. Those values are analysed from the three perspectives, the correspondences and differences mapped, and their background described.

The next three sections describe the relevant values in each perspective. Each section begins with the main conclusions and then provides further detail on the debate around values. The fourth and final section compares the three perspectives.

### Security perspective

A security perspective is concerned with protecting democracy and key interests of the state against national and international threats.[151] It seeks to maintain a degree of **stability and sovereignty** that is inherent in the character of Dutch society, in a political (protection of the constitutional democracy), economic (knowledge security, strategic dependencies) and material (physical territory, physical security) sense. The way this is framed as a 'race' is interesting; the idea is that other countries are engaged in a technological or economic race to catch up and therefore sometimes attempt to steal knowledge and technology from the Netherlands, or may be behind corporate takeovers, mergers and investments which do not benefit the Netherlands. This can undermine the prosperity, stability and openness of our Dutch society. [152] The notion of a 'race' is therefore used as an underlying assumption to help understand the international context

151 (AIVD, 2022)
152 (AIVD, MIVD, & NCTV, 2021)

and the national security of the Netherlands within it. The starting point appears to be a kind of zero-sum concept.

Expanding on this idea, it is argued that **continuity** of vital infrastructure, **integrity** and **exclusivity** of knowledge and confidential information and preventing (undesirable) strategic dependencies are essential for the Netherlands' economic security and maintaining its economic position. A link is therefore made between economic interests and the continuity and integrity of Dutch infrastructure and knowledge. The notion of maintaining and sustaining a certain status quo is part of this. Any interference which disrupts the existing configuration is seen as a threat.

The foregoing observations stem from an analysis of three perspectives, in line with the Threat Assessment for State Actors and the values encapsulated within it:[153]

**Territorial security** is about the 'undisrupted functioning of the Netherlands and its EU and NATO allies as independent states in either a broad or narrow sense'. Territorial security in a narrow sense relates to the integrity of the territory of the Netherlands, the EU and the NATO alliance, and the associated vital infrastructure (e.g. the national government with the associated vital processes and their suppliers). Territorial security in a broad sense encompasses the integrity of essential organisations, institutions and services, knowledge institutes, companies and top sectors as well as international ties that are necessary for the sovereign functioning of the Dutch state. This includes security in the digital domain.

Several aspects are linked to secure knowledge development. The **integrity of knowledge institutes** and their relationship with the sovereign functioning of the Dutch state touches on covert influence: a state or non-state actor who exerts influence on the functioning of a knowledge institute is therefore touching on the sovereignty of the Dutch state. The security of the digital domain also plays a part in secure knowledge development. Espionage and covert influence are increasingly being carried out digitally in order to serve political, military, economic and/or ideological aims.[154]

Espionage is a second aspect. **Espionage** occurs when information or objects are obtained covertly or illicitly by or on behalf of another country. If innovative knowledge and technology are lost due to espionage, this undermines Dutch security, for example through the development of weapons that could threaten the Netherlands' territorial integrity.[155] Transfer of high-grade knowledge and technology can moreover lead to

153 (AIVD, MIVD, & NCTV, 2021)
154 (AIVD, MIVD, & NCTV, 2021) N.B., no indication is given whether this also includes knowledge institutes.
155 (AIVD, MIVD, & NCTV, 2021, p. 18)

undesirable end use, for example the development of military or surveillance applications which affect Dutch national security.

A third aspect is the importance of **social and political stability** for the Dutch state, with a central element being the undisrupted continuation of a social climate in which individuals and groups can function and live together peacefully. Targets in this context can also include science, advisory bodies and educational and knowledge institutes. The relationship with secure knowledge development is characterised by diaspora politics; this can lead to self-censorship in the public debate or to collaboration with intelligence services, for example by sharing sensitive (scientific) knowledge. Conversely, self-censorship also plays a role for Dutch scientists who operate internationally: the pressure from influence and interference can make scientists afraid to be openly critical.[156]

A fourth aspect is **economic security**: the undisrupted functioning of the Netherlands as an effective and efficient economy. Central aspects then are continuity of vital processes, the integrity and exclusivity of information and knowledge and the avoidance of (undesirable) strategic dependencies. The relevance to knowledge security here is the high-grade knowledge, technology and infrastructure possessed by top Dutch knowledge and research institutes. These organisations may therefore be the target of espionage, but also of undesirable transfer by (legitimate) collaborations. The undesirable transfer of knowledge on things such as vital infrastructure can moreover jeopardise that infrastructure by making it easier to interfere with it. From a security perspective, therefore, economic security means the security of vital processes which form the basis for the country's economic functioning.

### Economic perspective

A transformation is currently taking place within the existing global economic order. Over the last few years, this has brought about a shift in economic thinking in Europe, which has seen governments playing an increasing role in the economy. This shift is currently also beginning to play a role at national level.[157] The renewed European economic thinking frequently serves as a model here.

A core concept in this new way of thinking in European economic policy is 'open strategic autonomy', a concept which refers to the capacity to trade autonomously when and where necessary with any other party. This is nothing new in the military and security fields, but due to economic shifts (with China as the biggest, followed by India), strategic autonomy has also become necessary for political survival.[158] The Covid-19 crisis and the

156 (AIVD, MIVD, & NCTV, 2021)
157 See e.g. (AIV, 2022)
158 (Borrell, 2020)

trade war between the US and China have moreover demonstrated that (asymmetrical) economic dependence leads to vulnerability. Science, technology, trade and data are increasingly used as tools in international power politics.[159]

The European Commission wishes to strengthen the European market, and has in the first place introduced supportive measures. To promote **economic sovereignty**, the European internal market needs to be protected and strategic dependencies limited. In addition, European values must be promoted and circumstances must be created for **a strong European economy** in which European companies can flourish and take on the competition from firms from America, China and elsewhere.[160] This approach thus has both a defensive and an offensive component: maintaining the sovereignty of Europe's own economy, whilst at the same time being able to compete with others.[161]

This begs the question of what the Netherlands' position is with regard to this European policy. In March 2021 the Netherlands and Spain published a joint document arguing that Europe should be open where possible but autonomous where necessary.[162] This document explicitly emphasises openness, rather than autonomy alone. It warns that strategic autonomy must not lead to isolationism or economic protectionism, and stresses the importance of **collaboration** and **international trade**, as well as of the **efficiency** and **competitiveness** of the European internal market. The underlying notion is thus that economic competitiveness and efficiency are dependent on the **openness** of the economy. That certainly applies for the Netherlands. This raises the question of where (economic) openness ends and where autonomy (sovereignty) begins. [163] The Netherlands and Spain call for **customisation** and **proportionality**. The central question then of course is what this means in practice.

### Academic perspective

The changing geopolitical context means that academic institutions are having to rethink their attitude towards a number of fundamental core values. On the other hand, academic institutions have always operated within a geopolitical context; most academic research is funded by national governments, making academic research itself an inherently political activity. Moreover, the idea of global scientific research collaboration arose during the Cold War and therefore has deep political roots; it was an attempt by Western

159 (Borrell, 2020; AIV, 2022, pp. 25–26)
160 (Korteweg, Ortega en Otero, 2022, p. 2)
161 (AIV, 2022, p. 26)
162 (Spain & Netherlands, 2021)
163 (Inspectie der Rijksfinanciën, 2020, p. 13)

governments to make science in the West more attractive for researchers than it was in closed, communist countries.[164]

Academic values (see Box below) mainly concern the way in which the academic world ought to function: **openly**, **equitably** and **independently** – partly because that is fair, and partly because it contributes to good research quality. To some extent these values also serve society: ultimately, academia has a **responsibility** to use research to take on the challenges posed by the world, and to do so in an international context. Academic values thus relate both to the academic institutions or researchers themselves (**institutional** and **moral autonomy**), and to the outside world (**openness, international collaboration and social responsibility**). The task of academic institutions and researchers is to consistently strike the right balance between these different values.[165]

Values can come under threat in several ways within the academic perspective. First, transferring high-grade knowledge with dual use applications (or dual use applications themselves) can lead to the development and dissemination of weapons that pose a threat to the home country's own national security. That is diametrically opposed to the integrity and ethical values as defined in numerous key documents (see Box below).

Secondly, institutional freedom and autonomy can be threatened by financial dependence.

A third way in which values can be endangered occurs when lecturers or researchers are covertly influenced, leading to (self-)censorship, influencing of the choice of research topics and erosion of research integrity.[166] This clearly impinges on the ethical component of research, as well as on the academic freedom scientists need in terms of moral and scientific autonomy.

However, academic values can also be threatened if too rigid an approach is taken to knowledge security. This may result from a lengthy bureaucratic process, for example, leading to important research being delayed. It can also happen as a result of rigid restrictions on collaboration choices, potentially threatening institutional autonomy, inclusivity, social contribution and the importance of collaboration (e.g. in the case of equal collaboration between academic institutions or equal access to the academic community).

Finally, safeguarding security in knowledge development is at odds with open academic collaboration and the sharing of knowledge. At the same time, openness should not be viewed from too narrow a perspective. Its underlying value lies in progress of science and

164 (Fischer, 2022a)
165 (KNAW, 2021, p. 36)
166 (VSNU, 2021, p. 14).

society, but openness can also impede that progress, for example if academic integrity is infringed by not sharing data or by holding back certain research results.[167] In a more fundamental sense, openness can lead to the undesirable transfer of knowledge that is then used for the development of things such as surveillance technology or chemical weapons, which violate human rights.

### Academic values

The European research system is coming under increasing pressure, both internally and externally. In response to this, Science Europe, the association of organisations that fund and perform scientific research in Europe, has developed a values framework, largely building on other documents such as the Magna Charta Universitatum and the Declaration of Lima. The values framework aligns with views expressed by the Royal Netherlands Academy of Arts and Sciences (KNAW).[168] It espouses the values **autonomy and freedom, care and collegiality, collaboration, equality, diversity and inclusion, integrity and ethics**, and **openness and transparency**. The social contribution is also important.

**Autonomy and freedom**[169] means freedom from political influence and economic interests. This independence must be acknowledged and protected by the government and society. Every member of the academic community has the right to fulfil their role without discrimination and without fear of repression and influence by a state or from any other source. Science is also open-ended, and it is therefore important to enable scientists to pursue their own curiosity without constraint. This autonomy and freedom is of course not absolute; it is constrained by statutory obligations imposed on higher education establishments, but also by other academic values such as integrity and transparency.[170]

**Care and collegiality** is defined as caring for the research ecosystem, including the responsible use of resources, as well as creating a respectful environment free from intimidation. Every member of the academic community enjoys freedom of conscience and freedom of thought, religion, expression, association and movement.[171]

---

167 (d'Hooghe & Lammertink, 2020, pp. 42–43)
168 (KNAW, 2021, p. 25; Magna Charta Universitatum Observatory, 2022; Science Europe, 2022)
169 N.B. A distinction is often drawn between academic freedom for the individual and for institutions, with the latter being described as institutional autonomy. Both aspects are included under autonomy and freedom here.
170 (KNAW, 2021, p. 26)
171 (World University Service, 1989)

**Collaboration** is about encouraging collaboration within specific disciplines as well as interdisciplinary and transdisciplinary collaboration, but also collaboration with relevant policy domains, sectors of industry and society as a whole. International academic collaboration should moreover be encouraged which goes beyond regional, political and other barriers. The replication and reproduction of research must also be safeguarded. To achieve this, universities must have a reliable social contract with society.[172]

**Equality, diversity and inclusion** involves making all roles within the scientific community accessible, regardless of sex, gender, orientation, religion or other factors. The importance of diversity of research inputs (data, methods) and outputs (forms of communication and dissemination) is also emphasised. All of this must moreover be accessible for everyone.

**Integrity and ethics** refer to safeguarding reliability, honesty and responsibility both in the performance and funding of research and in publishing the outcomes of research. It is also about preventing abuses of science and technology in a way that is detrimental to achieving the freedoms referred to above. Institutions should also take a critical view of violations of human rights in their own society and show solidarity with institutions that are subject to this.

**Openness and transparency** entail sharing and making accessible all aspects of research with a view to making research explainable.

**Social contribution** is the responsibility to respond to the ambitions and challenges of the world and the communities they serve, in order to benefit humankind and contribute to sustainability. All higher education institutions should work to realise the economic, social, cultural, civil and political rights of society. Each institution will also focus on contemporary social problems. Every institution must also strive to avoid scientific and technological dependence in order to achieve the most equal partnerships possible.[173]

### Comparison of the different perspectives

The discussion of the security perspective, the economic perspective and the academic perspective shows that there are considerable tensions within the changing geopolitical context in which knowledge development takes place. To date, these tensions have

172 (Magna Charta Universitatum Observatory, 2022)
173 (Magna Charta Universitatum Observatory, 2022)

always been approached from a single perspective. However, there are also a number of tensions between these perspectives.

**Autonomy and sovereignty**

First, autonomy or sovereignty occur in each of the three perspectives. This therefore appears to be a broadly shared value, although with a different interpretation within each perspective. From the security perspective, for example, autonomy means avoiding undesirable influence to preserve national stability. The relationship between sovereignty and stability therefore does not create a direct tension within the security context. The situation is different with the economic or academic perspective, where autonomy serves competitiveness or good research practice. Here a tension does arise, because competitiveness and research practice both operate within an international context and therefore require openness. There is thus a tension between core values in the economic and academic perspectives, which is not present within the security perspective.

In line with this tension between the security perspective on the one hand and the economic and academic perspectives on the other, we can also identify a set of differing attitudes. The security perspective appears to support an attitude that can be characterised by ‘maintaining’ or ‘protecting’ our way of life and work, whereas the economic and academic perspectives enshrine an attitude that can best be characterised as ‘improving’ or ‘disseminating’. In an economic sense, this manifests itself in the free movement of goods, services and people in order to improve economic strength. In academic terms, it is expressed in the free movement of persons, data, research collaborations and results with a view to boosting the social impact of science.

There is of course a national-international axis running through these tensions. The economic and academic perspectives are by definition international perspectives, both as regards the end goal (knowledge) and the process (doing science). Naturally, the security perspective also has an international component, but the focus then is on safeguarding the national interests.

**Who constrains or defends the values?**

A more general point emerges when we compare the different perspectives with each other. Values are not only threatened by ‘the other’ (espionage, covert influence), but possibly also by a country’s ‘own’ policy: an overly strict, risk-avoiding policy also puts pressure on certain core values such as openness and autonomy. On the economic front, Dutch policy is alert to this danger (with calls for open strategic autonomy), but on the academic front there currently appears to be a trend in the opposite direction: where the policy focus was originally on self-regulation by knowledge institutes, binding policy

instruments are now increasingly being deployed, such as the assessment framework and the administrative agreement incorporating an external audit.

**Academic/economic tensions**

Third, a number of tensions can be discerned between the economic perspective and the academic perspective. Universities of the Netherlands, the organisation which represents Dutch universities, highlights the tension between academic entrepreneurship, comprising the free dissemination of knowledge and maximising fruitful collaboration on the one hand, and on the other hand protecting the innovative strength of the Netherlands relative to other countries.[174] On this point, therefore, academic and economic values are at odds with each other.

The financial incentive structure also creates a tension for universities. Economic stability, academic autonomy and the security perspective come together here. Internationalisation in the scientific world has long been important in increasing the second and third flow of funds (indirect government funding and funding from contract research, respectively). This has also been encouraged by government. Placing too much emphasis on risk-avoiding measures can have a negative impact on the opportunities for academics. This could potentially lead academics to move abroad or into the commercial sector. There is thus a tension in the financial incentive structure for universities, the academic autonomy of individual academics and the security perspective.

174 (VSNU, 2021, pp. 14–15)

# Appendix 5 References


- AIV (2022) *Slimme industriepolitiek: een opdracht voor Nederland in de EU*. Advies 120. Den Haag, Adviesraad Internationale Vraagstukken.
- AIVD (2022) *Jaarverslag AIVD 2021*. Jaarverslag. Den Haag, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, Algemene Inlichtingen- en Veiligheidsdienst.
- AIVD, MIVD, & NCTV (2021) *Dreigingsbeeld statelijke actoren*. Den Haag, Algemene Inlichtingen- en Veiligheidsdienst, Militaire Inlichtingen- en Veiligheidsdienst, Nationaal Coordinator Terrorismebestrijding en Veiligheid.
- ALLEA (2017) *European Code of Conduct for Research Integrity. Revised Edition*. Berlin: ALLEA ALL European Academies.
- AWT (2012) *De Chinese handschoen: hoe Chinese en Nederlandse kennis elkaar kunnen versterken*. Den Haag: Adviesraad voor het Wetenschaps- en Technologiebeleid (AWT).
- AWTI (2017a) *Onmisbare schakels. De toekomst van het toepassingsgericht onderzoek*. Den Haag: Adviesraad voor wetenschap, technologie en innovatie.
- AWTI (2017b) *WTI Diplomatie. Offensief voor internationalisering van wetenschap technologie en innovatie*. Den Haag: Adviesraad voor wetenschap, technologie en innovatie.
- AWTI (2020a) *Krachtiger kiezen voor sleuteltechnologieën*. Den Haag: Adviesraad voor het Wetenschaps- en Technologiebeleid.
- AWTI (2020b) *Versterk de rol van wetenschap, technologie en innovatie in maatschappelijke transities*. Den Haag, Adviesraad voor wetenschap, technologie en innovatie.
- AWTI (2022) *Grenzeloos onderzoeken. Stimuleer interdisciplinariteit met twee onderscheidende overheidsrollen*. Den Haag: Adviesraad voor wetenschap, technologie en innovatie.
- Baker, S. (2022) 'Marginson: push back on "securitisation" to save global science', *Times Higher Education*, 21 June. Accessible at: https://www.timeshighereducation.com/news/marginson-push-back-securitisation-save-global-science (Accessed: 10 July 2022).
- Baurichter, R. & Pols, M. (2020) 'Accountants terughoudend over kritisch rapport', *Financieele Dagblad*, 16 January.
- Bertuzzi, L. (2022) 'Six EU countries call for ambitious cyber defence policy, document', *EURACTIV*, 30 September. Accessible at: https://www.euractiv.com/section/cybersecurity/news/six-eu-countries-call-for-ambitious-cyber-defence-policy-document/ (Accessed: 6 October 2022).

- Borrell, J. (2020) 'Why European strategic autonomy matters', *European Union External Action*, 3 December. Accessible at: https://www.eeas.europa.eu/eeas/why-european-strategic-autonomy-matters_en.
- Boulton, G.S. (2021) 'Science as a Global Public Good. International Science Council Position Paper', in. *LERU Anniversary Conference*, Brussels, p. 21. Accessible at: https://council.science/wp-content/ uploads/2020/06/Science-as-a-global-public-good_v041021.pdf (Accessed: 20 August 2022).
- Brainard, J. & Normile, D. (2022) 'China rises to first place in one key metric of research impact', *Science*, 377(6608), pp. 799–799. doi:10.1126/science.ade4423.
- Bruins, R. (2022) 'Tekort accountants vraagt om modernisering van het partnermodel - Executive Finance -', *Executive Finance*, 27 January. Accessible at: https://executivefinance.nl/2022/01/tekort-accountants-vraagt-om-modernisering-van-het-partnermodel/ (Accessed: 2 October 2022).
- Clark, R. (2022) *Inadvertently Arming China? One Year On. The Chinese military complex and its exploitation of scientific research at UK universities*. London, Civitas.
- Committee on Protecting Critical Technologies for National Security in an Era of Openness and Competition *et al.* (2022) *Protecting U.S. Technological Advantage*. Washington, D.C.: National Academies Press.
- CPNI (undated) *Trusted research*. Accessible at: https://www.cpni.gov.uk/trusted-research (Accessed: 24 October 2022).
- CSR (2021) *CSR Advies 'Nederlandse Digitale Autonomie en Cybersecurity'. Hoe verminderen we onze digitale afhankelijkheden met behoud van een open economie?* Den Haag, Cyber Security Raad.
- De Bruijn, A. (2021) 'TU-rector: "Wat wel en wat niet met China? Dat weten we niet altijd"', *Delta*, 5 July.
- De Bruijn, A. *et al.* (2022) 'Europese universiteiten helpen China om 's werelds modernste leger op te bouwen', *Follow the money*, 19 May.
- Diercks, G., Deuten, J. & Diederen, P. (2019) *Kennis in het vizier. De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur.* Den Haag, Rathenau Instituut.
- Ellis, L. & Gluckman, N. (2019) 'How University Research Landed on the Front Lines of the Fight With China', *The Chronicle of Higher Education*, 31 May. Accessible at: https://www.chronicle.com/article/how-university-research-landed-on-the-front-lines-of-the-fight-with-china (Accessed: 1 April 2022).
- European Commission (2021a) 'Strengthening the EU's autonomy – Commission seeks input on a new anti-coercion instrument', *European Commission - Press release*, 23 March.

- European Commission (2021b) *The Global Approach to Research and Innovation Europe's strategy for international cooperation in a changing world*. Brussel, European Commission.
- European Commission (2022) 'A Chips Act for Europe. Commission Staff Working Document'. European Commission. Accessible at: https://digital-strategy.ec.europa.eu/en/library/european-chips-act-staff-working-document (Accessed: 6 June 2022).
- European Commission. Directorate General for Research and Innovation. (2022) *Tackling R&I foreign interference: staff working document.* Luxemburg: Publications Office. Accessible at: https://data.europa.eu/doi/10.2777/513746 (Accessed: 6 July 2022).
- Evans, S.W. (2022) 'When All Research Is Dual Use', *Issues*, 38(3 spring).
- Fägersten, B. (2022) *Leveraging Science Diplomacy in an Era of Geo-Economic Rivalry. Towards a European strategy*. Stockholm, The Swedish Institute of International Affairs.
- Fischer, K. (2021) 'Chinese Scientists Feel a Chill Under U.S. Investigation of Higher Ed's China Ties, a New Survey Shows', *The Chronicle of Higher Education*, 28 October. Accessible at: https://www.chronicle.com/article/chinese-scientists-feel-a-chill-under-u-s-investigation-of-higher-eds-china-ties-a-new-survey-shows?cid2=gen_login_refresh&cid=gen_sign_in (Accessed: 3 April 2022).
- Fischer, K. (2022a) 'Is Geopolitics Closing the Door on Open Research?', *The Chronicle of Higher Education*, 19 April. Accessible at: https://www.chronicle.com/article/is-geopolitics-closing-the-door-on-open-research (Accessed: 1 June 2022).
- Fischer, K. (2022b) 'Latitudes: A New Visibility for International Scholars', *The Chronicle of Higher Education*, 18 May. Accessible at: https://www.chronicle.com/newsletter/latitudes/2022-05-18.
- Foy, H. (2022) 'EU ministers advised to take tougher line on China', *Financial Times*, 17 October.
- Fransman, J. *et al.* (2021) 'Beyond partnerships: embracing complexity to understand and improve research collaboration for global development', *Canadian Journal of Development Studies / Revue canadienne d'études du développement*, 42(3), pp. 326–346. doi:10.1080/02255189.2021.1872507.
- G7 (2022) 'Annex to the G7 Science Ministers` Communiqué 2022. Further Implementation and G7 Science Working Groups'. Accessible at: https://www.bmbf.de/SharedDocs/Downloads/de/2022/220613-g7-annex.pdf (Accessed: 1 September 2022).
- Gattolin, A. (2021) *Mieux protéger notre patrimoine scientifique et nos liberte's académiques. Rapport d'information*. Rapport d'information 873. Paris, Sénat.

Accessible at: https://www.senat.fr/rap/r20-873/r20-873_mono.html (Accessed:: 10 October 2022).
- Geurts, L. (2022) 'Raad van State: wetsvoorstel nieuwe spionagewet is "onvoldoende duidelijk"', *NRC*, 27 September.
- Ghodsvali, M., Krishnamurthy, S. & de Vries, B. (2019) 'Review of transdisciplinary approaches to food-water-energy nexus: A guide towards sustainable development', *Environmental Science & Policy*, 101, pp. 266–278. doi:10.1016/j.envsci.2019.09.003.
- Gildea, R.J. & D'Alessandra, F. (2022) 'We Need International Agreement on How to Handle These Dangerous Technologies', *Slate.com*, 7 March. Accessible at: https://slate.com/technology/2022/03/dual-use-surveillance-technology-export-controls.html (Accessed: 4 juni 2022).
- Gort, J. (2011) 'Veranderen voor veiligheid Hoe doe je dat eigenlijk?' *TNO*, 16 March.
- Graaf, de, B.A., Rinnooy Kan, A. & Molenaar, H. (eds.) (2017) *The Dutch National Research Agenda in Perspective. A Reflection on Research and Science Policy in Practice*. Amsterdam University Press. doi:10.5117/9789462982796.
- Heerschop, D. & Riedstra, S. (2021) *Evaluatie Taskforce ongewenste kennisoverdracht*. Den Haag, ABDTOPConsult.
- d'Hooghe, I. *et al.* (2018) *Assessing Europe-China Collaboration in Higher Education and Research*. Leiden, LeidenAsiaCentre.
- d'Hooghe, I. (2021) 'Wetenschappelijke samenwerking met onvrije landen: de casus China. Rondetafelgesprek Tweede Kamer'. Netherlands Institute of International Relations 'Clingendael', LeidenAsiaCentre.
- d'Hooghe, I. & Dekker, B. (2020) *China's invloed op onderwijs in Nederland: een verkenning*. Den Haag, Clingendael Netherlands Institute of International Relations.
- d'Hooghe, I. & Lammertink, J. (2020) *Towards Sustainable Europe-China Collaboration in Higher Education in Research*. Leiden, LeidenAsiaCentre.
- d'Hooghe, I. & Lammertink, J. (2022) *How National Governments and Research Institutions Safequard Knowledge Development in Science and Technology*. Leiden, LeidenAsiaCentre.
- Hudson, R.L. (2022) 'How to keep science open – but also secure G7 nations work on an answer', *Science Business*, 7 July. Accessible at: https://sciencebusiness.net/news/how-keep-science-open-also-secure-g7-nations-work-answer (Accessed: 1 August 2022).
- Hudson, R.L. *et al.* (2022) 'The conduct of science in times of war'. ScienceBusiness.
- Huotari, M. & Jean, S. (2022) 'Bolstering Europe's Economic Strategy vis-à-vis China', (72).

- Inspectie der Rijksfinanciën (2020) 'BMH Speelbal of spelverdeler? Concurrentiekracht en nationale veiligheid in een open economie'. Rijksoverheid.
- de Jager, D., Meier, I. & Koevoets, K. (zonder datum) 'Strategische autonomie, een veelzijdig debat', *pwc*. Accessible at: https://www.pwc.nl/nl/marktsectoren/publieke-sector/veiligheid/defensie/strategische-autonomie-een-veelzijdig-debat.html (Accessed: 9 September 2022).
- Johnson, J. *et al.* (2022) *Stumbling bear, soaring dragon. Russia, China and the geopolitics of global science*. London, The Policy Institute. King's College London, Clarivate, Harvard Kennedy School Mossavar-Rahmani Centre for Business and Government.
- Karásková, I., Šebok, F. & Blablová, V. (2022) *How to Do Trusted Research: China-Specific Guidelines for European Stakeholders*. Analysis. Prague, Czech Republic, Association for International Affairs (AMO), p. 62.
- Kempes, M. & Strijker, R. (2021) 'Nederland doet samen met China DNA-onderzoek "Fundamenteel fout"', *RTL nieuws*, 6 October. Accessible at: https://www.rtlnieuws.nl/nieuws/artikel/5258161/nederland-china-dna-oeigoeren-mensenrechten (Accessed: 20 August 2022).
- Kissinger, H. (1995) *Diplomacy*. 1. Touchstone ed. New York, NY: Simon & Schuster (A Touchstone book).
- KNAW *et al.* (2018) 'Nederlandse gedragscode wetenschappelijke integriteit'. Data Archiving and Networked Services (DANS). doi:10.17026/DANS-2CJ-NVWU.
- KNAW (2019) *Evenwicht in het wetenschapssysteem De verhouding tussen ongebonden en strategisch onderzoek*. Advies. Den Haag, Koninklijke Nederlandse Academie van Wetenschappen.
- KNAW (2021) *Academische vrijheid in Nederland – een begripsanalyse en richtsnoer*. Amsterdam: KNAW.
- Korteweg, R., Ortega, A. & Otero, M. (2022) *A Spanish-Dutch view on open European strategic autonomy in trade, industry and digital policy: seven pitfalls to avoid*. Madrid, Elcano Royal Institute.
- Lippert, B. & Perthes, V. (2020) *Strategic rivalry between United States and China: causes, tragectories, and implications for Europe*. 4. Berlin, Stiftung Wissenschaft und Politik. Accessible at: https://www.swp-berlin.org/10.18449/2020RP04/ (Accessed: 15 November 2022).
- Long, G. (2019) *Fundamental Research Security*. JSR-19-2I. McLean, JASON. The MITRE Corporation.
- Magna Charta Universitatum Observatory (2022) 'Magna Charta Universitatum 2020'. Magna Charta Universitatum Observatory.
- van der Meulen, B. & Rip, A. (1998) 'Mediation in the Dutch science system', *Research Policy*, 27(8), pp. 757–769. doi:10.1016/S0048-7333(98)00088-2.

- Minister van Buitenlandse Zaken (2021) *Recente ontwikkelingen in China en de situatie in Xinjiang*.
- Minister van EZK (2022) *Het belang van het Nederlandse vestigings- en ondernemingsklimaat*.
- Minister van OCW (2022a) *Afschrift brief aan kennisinstellingen inzake implementatie Nationale Leidraad Kennisveiligheid*.
- Minister van OCW (2022b) *Werken aan een sectorbeeld Kennisveiligheid*, *Officiele bekendmakingen*.
- Minister van OCW, Minister van EZK, & Minister van J&V (2022) *Voortgang en vooruitblik aanpak kennisveiligheid hoger onderwijs en wetenschap*.
- Minister van OCW, Minister van J&V, & Staatssecretaris van EZK (2020) *Kennisveiligheid hoger onderwijs en wetenschap*.
- Ministerie van Buitenlandse Zaken (2018) 'Handboek Strategische Goederen en Diensten'. Rijksoverheid. Accessible at: www.rijksoverheid.nl/exportcontrole (Accessed: 1 April 2022).
- Ministerie van Buitenlandse Zaken (2019) *Nederland-China: een nieuwe balans*.
- Ministerie van Defensie (2019) 'ABDO Algemene Beveiligingseisen voor Defensieopdrachten 2019'. Ministerie van Defensie.
- Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid (2022a) 'Besluit toepassingsbereik sensitieve technologie'. Rijksoverheid. Accessible at: https://www.internetconsultatie.nl/sensitievetechnologievifo/ (Accessed: 28 September 2022).
- Ministerie van Economische Zaken en Klimaat & Ministerie van Justitie en Veiligheid (2022b) *Wet van 18 mei 2022, houdende regels tot invoering van een toets betreffende verwervingsactiviteiten die een risico kunnen vormen voor de nationale veiligheid gezien het effect hiervan op vitale aanbieders, beheerders van bedrijfscampussen of ondernemingen die actief zijn op het gebied van sensitieve technologie (Wet veiligheidstoets investeringen, fusies en overnames)*, *Staatsblad*.
- Ministerie van Justitie en Veiligheid (2022) 'Strafbaarstelling spionage gemoderniseerd', *Rijksoverheid.nl*, 28 February. Accessible at: https://www.rijksoverheid.nl/actueel/nieuws/2022/02/28/strafbaarstelling-spionage-gemoderniseerd?msclkid=a33c7425bb3a11ec95caff439b37de90 (Accessed: 1 March 2022).
- MIVD (2022) *Openbaar Jaarverslag 2021*. Jaarverslag. Den Haag, Militaire Inlichtingen- en Veiligheidsdienst, Ministerie van Defensie.
- Molthof, L., Zandee, D. & Cretti, G. (2021) *Unpacking open strategic autonomy. From concept to practice*. Den Haag, Netherlands Institute of International Relations 'Clingendael'.

- Monitoring Commissie Accountancy (2020) 'Spiegel voor de accountancysector Veel problemen zijn helemaal niet nieuw, ze keren alleen telkens terug'.
- Müller, J. & Potters, L. (2019) *Future technology for prosperity: Horizon scanning by Europe's technology leaders*. Luxembourg: Publications Office of the European Union.
- Muneer, F. (2022) 'Cybersecurity Capability Maturity Model (C2M2)'. U.S. Department of Energy and Office of Cybersecurity, Energy Security and Emergency Response.
- Myklebust, J.P. (2022) 'Researcher arrested on suspicion of being a Russian spy', *University World News. The Global Window on Higher Education*, 28 October. Accessible at: https://www.universityworldnews.com/post.php?story=20221026105932263 (Accessed: 28 October 2022).
- National Security Commission on Artificial Intelligence (2021) *Final Report National Security Commission on Artificial Intelligence*. Accessible at: https://www.nscai.gov/2021-final-report/ (Accessed: 25 October 2022).
- Nouwens, M. & Legarda, H. (2018) *China's pursuit of advanced dual-use technologies*. Research paper. London, Internationaal Instituut for Strategische Studies, p. 43. Accessible at: https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance (Accessed: 20 August 2022).
- OECD (2022) *Integrity and security in the global research ecosystem*. Paris, OECD Science, Technology and Industry.
- Pheijffer, M. (2021) 'Waarom ik blijf schrijven over accountants en fraude', *Financieele Dagblad*, 1 December.
- Pols, M. (2020) 'Commissievoorzitter: "Accountants hebben niet goed genoeg in de spiegel gekeken"', *Financieele Dagblad*, 14 January.
- Pols, M. (2022) 'Het blijft wachten op de echte verbeteringen in accountancy', *Financieele Dagblad*, 21 July.
- Rathenau Instituut (2021) *Kennisveiligheid in hoger onderwijs en wetenschap. Een gedeelde verantwoordelijkheid*. Den Haag, Rathenau Instituut.
- Roet, J. (2022) 'Ministers zoeken derde landen, hervormen research assessment en bekritiseren uitvoering missies', *Neth-ER*, 16 June. Accessible at: https://www.neth-er.eu/onderzoek/ministers-zoeken-derde-landen-hervormen-research-assessment-en-bekritiseren-uitvoering-missies (Accessed: 16 April 2022).
- Science Europe (2022) *A Values Framework for the Organisation of Research*. Brussel, Science Europe AISBL. Accessible at: https://zenodo.org/record/6637847 (Accessed: 15 November 2022).
- ScienceGuide (2022a) '"Generieke maatregelen kennisveiligheid onnodige bureaucratie"', *ScienceGuide*, 9 September. Accessible at:

https://www.scienceguide.nl/2022/09/generieke-maatregelen-kennisveiligheid-onnodige-bureaucratie/ (Accessed: 10 September 2022).
- ScienceGuide (2022b) 'Regeringspartijen willen strenger toezicht op aanpak kennisveiligheid door universiteiten', *ScienceGuide*, 16 September. Accessible at: https://www.scienceguide.nl/2022/09/regeringspartijen-willen-strenger-toezicht-op-aanpak-kennisveiligheid-door-universiteiten/ (Accessed: 16 September 2022).
- Scientific integrity fast-track action committee (2022) *Protecting the integrity of government science*. Washington, DC, National Science and Technology Council.
- Shih, T. (2022) 'Recalibrated responses needed to a global research landscape in flux', *Accountability in Research*, pp. 1–7. doi:10.1080/08989621.2022.2103410.
- Snetselaar, D. (2022) 'DREAMS Lab: assembling knowledge security in Sino-Dutch research collaborations', *European Security*, pp. 1–19. doi:10.1080/09662839.2022.2127317.
- Spain & Netherlands (2021) 'Spain-Netherlands non-paper on strategic autonomy while preserving an open economy'. Permanent representation. Accessible at: https://www.permanentrepresentations.nl/documents/publications/2021/03/24/non-paper-on-strategic-autonomy (Accessed: 15 April 2022).
- Stone, G.R. *et al.* (2022) *Report of the Committee on Freedom of Expression*. Chicago, University of Chicago.
- Sue-Yen Tjong Tjin Tai *et al.* (2018) *Bedrijf zoekt universiteit. De opkomst van strategische publiek-private partnerships in onderzoek*. Den Haag, Rathenau Instituut.
- Teer, J. (2021) *Kennissamenwerking met onvrije landen in een tijd van harde competitie tussen grootmachten: de militaire dimensie*. Den Haag, The Hague Centre for Strategic Studies.
- Teer, J. (2022) *China's militaire opkomst en Europese technologie*. Den Haag, Hague Centre for Strategic Studies. Accessible at: https://www.jstor.org/stable/resrep40031 (Accessed: 1 August 2022).
- The University of Copenhagen *et al.* (2022) 'The EVALUATE framework and handbook. Harnessing the power of evaluation to build better international strategic partnerships between universities'. The University of Edinburgh.
- UKRI (2021) 'Trusted Research and Innovation Principles'. UK Research and Innovation.
- Universiteiten van Nederland *et al.* (2022) 'Nationale leidraad kennisveiligheid. Veilig internationaal samenwerken'. Rijksoverheid. Accessible at: https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid (Accessed: 4 March 2022).
- Van den Broek, J. (2022) 'Opinie | Deep tech moet de ruimte krijgen in Nederland - NRC', *NRC*, 15 September.

- Van der Dool, P. (2022) '"Het bagatelliseren van dreigingen is geen basis voor beleid"', *NRC*, 4 September.
- Van der Woude, H. & Van der Molen, H. (2022) *Motie van de leden Van der Woude en Van der Molen over de risicoanalyse kennisveiligheid op systematische wijze laten uitvoeren door de instellingen*.
- Versteegh, K. (2022) 'Juristen en oud-spionnen zijn het een keer eens: die nieuwe wet tegen spionage deugt niet', *NRC*, 24 July, p. 4.
- VSNU (2021) *Kader Kennisveiligheid Universiteiten*. Den Haag, Vereniging van Universiteiten.
- Wellerstein, A. (2021) *Restricted data: the history of nuclear secrecy in the United States*. Chicago: The University of Chicago Press.
- van der Wende, M. & Kirby, W.C. (2020) *China and Europe on the New Silk Road: Connecting Universities Across Eurasia*. Oxford university press.
- van Wijnen, J.F. (2022) 'Wetenschappers zijn bang voor hun toekomst door Googles superieure computer', *Financieele Dagblad*, 1 July, p. 5.
- World University Service (1989) 'The Lima Declaration on Academic Freedom and Autonomy of Institutions of Higher Education'. World University Service.
- Xie, Y. *et al.* (2022) 'Caught in the Crossfire: Fears of Chinese-American Scientists', *Physics and Society*, p. 16. doi:arXiv:2209.10642.

Awti Advisory council for science, technology and innovation

Prins Willem-Alexanderhof 20
2595 BE Den Haag
t. +31 (0)70 3110920
e. secretariaat@awti.nl
w. http://english.awti.nl