SUMMARY

RAND EUROPE



Identity and document fraud in the context of research security

International case studies and lessons for the Netherlands

Judith Huismans, Scott Warnier, Conlan Ellis, Fook Nederveen

This research was sponsored by the
Dutch Research and Data Centre (WODC).

For more information on this publication, visit www.rand.org/t/RRA5003-1

About RAND Europe
RAND Europe is a not-for-profit research organisation that helps improve policy and decision making through research and analysis. To learn more about RAND Europe, visit www.randeurope.org.

Research Integrity
Our mission to help improve policy and decision making through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behaviour. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

Published by the RAND Corporation, Santa Monica, Calif., and Cambridge, UK

© 2026 RAND Corporation

RAND® is a registered trademark.

Cover image: Adobe Stock

Limited Print and Electronic Distribution Rights
This publication and trademark(s) contained herein are protected by law. This representation of RAND intellectual property is provided for noncommercial use only. Unauthorised posting of this publication online is prohibited; linking directly to its webpage on rand.org is encouraged. Permission is required from RAND to reproduce, or reuse in another form, any of its research products for commercial purposes. For information on reprint and reuse permissions, please visit www.rand.org/pubs/permissions.

Summary

International cooperation and attracting researcher talent are crucial to the Netherlands' scientific and economic progress. At the same time, the government has expressed concerns about growing security threats from countries that are deliberately attempting to obtain valuable knowledge and technology from the Netherlands.[1] In recent threat analyses, China is consistently cited as the primary threat due to its intertwined policy of knowledge and innovation acquisition in the service of national security and defence.[2] This manifests itself, amongst other things, in large-scale espionage programmes and the funding of students and researchers to gain access to advanced technologies. Such activities threaten not only the knowledge security of educational and research institutions, but also the innovative capacity of businesses, the effectiveness of the armed forces and the strategic autonomy of the Netherlands.[3]

Combating undesirable knowledge transfer and strategic dependencies requires a robust knowledge security policy.

Objectives and research design

Against this backdrop, there is a need for in-depth research into the policy and practice surrounding knowledge security, specifically focusing on the risks of identity and document fraud within the Dutch knowledge sector. Documented case studies are scarce, which makes it difficult to develop effective and proportionate policy. Nevertheless, lessons from practice regarding the use of identity and document fraud to gain access to sensitive technology and knowledge can provide important insights for developing a workable and efficient screening process. At the request of the Ministry of Education, Culture and Science (OCW), the Scientific Research and Data Centre (WODC) has therefore asked RAND Europe to analyse how screening for identity and document fraud is organised in the Netherlands and a selection of other countries, what forms of fraud occur, how frequently they occur, and which safeguards are effective in countering these risks.

The study comprises a literature review examining the methods and frequency of identity and document fraud in four state case studies: the Netherlands, Australia, Germany and Sweden. The case studies are based on desk research and interviews with experts possessing specialist knowledge of information security, identity checks and document verification. By comparing the experiences, working methods sand challenges

[1] House of Representatives of the States General (2026).

[2] NCTV (2025).

[3] NCTV (2025).

in these countries, relevant lessons have been identified for the Netherlands. Interviews were used to supplement missing information and provide insight into practice.

Findings

What is known about the ways in which identity and document fraud is committed to gain access to knowledge institutions in the Netherlands and abroad?

Information on fraud relating to knowledge security in the Netherlands is not centrally recorded or analysed. Due to this piecemeal approach, the various stakeholders are only able to paint a partial picture of the fraud landscape. The interviews highlight various modus operandi of fraud. The Knowledge Security Desk regularly hears from knowledge institutions that relevant information, such as defence-related connections for example, is often deliberately omitted from CVs. This is partly due to the increased focus on knowledge security and the growing awareness amongst knowledge institutions of the risks associated with certain connections. Whereas such links were previously regarded as prestigious, institutions are now more aware of the potential risks and the role of state actors. Nuffic, the organisation for internationalisation in education, advises Dutch higher education institutions on the recognition of foreign qualifications and issues approximately 30,000 non-binding recommendations each year. In doing so, Nuffic verifies the authenticity and recognition of qualifications by the competent authority and assesses accompanying documents such as academic transcripts. By checking whether the entire course of study has proceeded in a logical and consistent manner, Nuffic can detect potential fraud. However, as copies are used, it can be more difficult to establish fraud, particularly when state actors are involved. Nuffic notes that diploma fraud is more common from certain countries, but does not explicitly investigate whether there is a link to knowledge security. In addition, there are known 'diploma mills' – or diploma factories – where fake diplomas can be ordered.

In Australia, regulatory mechanisms such as the PACT (*Protecting Australia's Critical Technology*) regulations and the ARC (Australian Research Council) framework have been designed to carry out thorough checks on documents and supporting evidence. However, the primary focus here is not on detecting fraud and verifying the authenticity of documents such as identity documents and diplomas, but rather on identifying potential risks. Interviews with Australian experts reveal that providing false information is the most common form of fraud encountered in Australia, particularly in CVs and grant applications. One of the most worrying trends to have emerged over the past twelve to eighteen months is the deliberate concealment of the source of scholarships. There is a growing, systematic misrepresentation of funding sources and instances where individuals deliberately claim to have links to lower-risk institutions whilst concealing their ties to the actual (and potentially higher-risk) organisations. On CVs, individuals often omit certain jobs or work placements from the official versions they submit, whilst retaining the full details for CVs shared privately. The same pattern can be observed with regard to research results: *non-dual-use* research is made public, whilst military-related research is concealed. Furthermore, affiliations with organisations are often not translated, thereby concealing their true significance even further. Another form of fraud identified involved false invitation letters for visa purposes. Cases are often flagged by other higher education institutions which contact to confirm that an invitation is genuine. This exchange of information is facilitated by the Australian Informal Foreign Interference Network (INFIN), a non-governmental

organisation comprising 39 Australian higher education institutions that jointly discuss efforts to combat undesirable interference and ensure compliance with government regulations.

In Germany, responsibility for screening lies with the researchers and universities themselves. Legal obligations are limited to export controls on military and dual-use technologies. Institutions must gather information on security-relevant aspects themselves, often using external sources such as the ASPI Tracker – a tool developed by the Australian Strategic Policy Institute (ASPI) that maps defence links of Chinese universities – but these sources provide limited and sometimes unclear information. The German domestic security service (Bundesamt für Verfassungsschutz – BfV) does, however, provide an overview of methods used by high-risk countries to acquire sensitive technologies and knowledge, of which circumventing export and knowledge controls by using misleading information in applications is directly relevant to knowledge security. This is consistent with trends in other countries.[4]

Sweden operates a centralised application system for higher education administered by the Swedish Council for Higher Education (UHR). UHR provides advice and references, but universities and universities of applied sciences decide independently on admissions and are responsible for verifying qualifications and detecting fraud. In the case of PhD applications, this responsibility lies entirely with the institutions themselves. There is no central reporting obligation, which means that the UHR has no insight into the number of fraud cases at the institutions. In an interview, it was mentioned that candidates with forged degrees from diploma mills – organisations and individuals involved in selling diplomas and academic degrees without any study programme having been completed – have been admitted to PhD programmes, which underlines the seriousness of the issue. Diploma mills represent a growing challenge.

In the United Kingdom, attention is also being paid to the withholding of information. Under the ATAS (Academic Technology Approval Scheme), the focus is not only on the content of an application but also on possible omissions, such as gaps in CVs. The documents submitted are compared with open-source information, and if certain details are not mentioned, this may prompt further investigation.

In summary, the main modus operandi regarding identity and document fraud in the context of knowledge security appear to be:

- The use of incomplete documents and the deliberate withholding of information, for example regarding affiliations or the source of funding.
- Distorting or providing incorrect information, for example by listing less high-risk affiliations. Failure to translate such affiliations can make it more difficult to ascertain their true significance.
- Fake qualifications, for example those produced by diploma mills.
- Fake invitation letters for visa purposes.

To what extent is there an understanding of the frequency with which this fraud occurs in the Netherlands and elsewhere?

The literature review and interviews have shown that it is very difficult to gain a clear picture of the frequency with which this fraud occurs in the Netherlands. This is mainly because the system is decentralised, with responsibility for screening largely resting with the higher education institutions

[4] Federal Office for the Protection of the Constitution (2026).

themselves. Various bodies monitor parts of the process, such as the authenticity of qualifications, and therefore sometimes have insight into fraud within their own domain. However, they indicate that they do not have a complete overview. For example, Nuffic has an advisory role, but universities are not obliged to have qualifications checked by Nuffic.

According to experts interviewed in Australia, no cases have been detected to date of individuals travelling under a false identity. They add that – given that foreign state actors pose the greatest threat – it may be impossible to detect fraudulent credentials when these have been issued by government bodies. As indicated earlier, the main form of fraud in Australia is the provision of false information, particularly in CVs and grant applications. Nor is there a complete picture of the scale of this phenomenon. However, it is clear that it occurs: in 2024, the China Scholarship Council reported 1,000 recipients of funding in Australia, yet only 350 students openly admitted to receiving this support. This significant discrepancy highlights how often individuals are not transparent about the nature or source of their research funding. As this concerns a single source of funding, it may well be just the tip of the iceberg of a wider problem involving the withholding of other information as well. Regarding false letters of invitation for visa purposes, the University of New South Wales in Australia has recorded between 6 and 12 cases over the past two to three years. This occurs mainly at faculty level, involving visiting scholars. It is striking that there are no relevant case studies relating to the PACT regulations. Although the PACT mechanism has been applied to restrict visa applications, decisions on these matters remain outside the public domain. During an interview, it was noted that these are only made public if an applicant decides to challenge a decision in the future, which has not yet occured at the time of this research.

As in Germany, responsibility in Sweden also lies with the higher education institutions themselves, which makes it difficult to gain an insight into the frequency of such cases in this country as well. However, admissions of Bachelor's and Master's students are processed centrally by the UHR. An interview revealed that, for academic admissions via the UHR portal, the number of reported cases of fraud has risen from 30 in 2024 to 130 in 2025. This is largely attributed to the use of AI agents, which are said to have made the application procedure more accessible. However, no direct link can be made here to knowledge security, as the cases may, for example, also involve fraud for economic migration purposes. The figures do, however, provide an indication of the scale and the potentially growing role of AI.

What safeguards can be put in place to combat the various forms of fraud?

The literature review and interviews reveal several lessons for the Netherlands, or safeguards that can be put in place to combat the various forms of fraud.

Better integration of screening at individual and institutional/country level

Interviews and practical experience show that identifying inconsistencies is essential for detecting fraud, particularly when copies are used or state actors are involved.[5] For example, an interview conducted for the case study on Sweden revealed that verifying publications is one of the main ways in which they check for possible links to the defence sector.[6] Publications can also be compared with information on a CV, which

[5] RAND Europe Interview – 8.

[6] RAND Europe Interview – 9.

can reveal inconsistencies.[7] In the Netherlands, the Knowledge Security Desk, the central advisory point for research institutions, does not receive any personal data. Individual screening is the responsibility of the knowledge institutions, which often have limited resources and country-specific knowledge for this purpose. A complete picture therefore depends on voluntary coordination and knowledge-sharing between organisations. In France, for example, knowledge about risks at individual and institutional/country level is better consolidated, as the knowledge security coordinator within knowledge institutions holds a confidential position and is appointed by the government.

Explore the provision of information to research institutions regarding knowledge sharing

In all the countries studied, checks relating to knowledge security are fragmented across multiple agencies. This is further complicated by the fact that the necessary information usually comprises personal data, and its sharing must be carried out securely and in accordance with data protection legislation. In Sweden, for example, this is perceived as a sensitive issue. Even if fraud is detected during an admissions procedure, this information often cannot be shared externally, or even internally.[8] In Sweden, the UHR grants recognition both for the purposes of the labour market and for further studies. Due to data protection regulations, the sharing of information between the two procedures is prohibited, even when a person has submitted an application for both purposes.[9] In the Netherlands, relevant bodies such as Nuffic provide advice, but higher education institutions are not obliged to seek such advice and always retain the authority to decide on admission themselves. As a result, it may happen that a student, for whom Nuffic has refrained from giving advice due to doubts about the authenticity or recognition of documents, is not admitted to one institution but is admitted elsewhere. In practice, higher education institutions almost always seek advice for certain countries of origin, but the interpretation and final decision rest with the institution itself.[10] Previous research has already shown that, in the absence of clear legal frameworks, higher education institutions find it difficult to assess what information they are permitted to request under the GDPR and whom they should or should not screen.[11] Higher education institutions need clear guidelines and practical support on what information they are permitted to request under privacy legislation, whom they should or should not screen, and how personal data may be shared. There is also a need for clear guidelines on when and how cases of fraud should be escalated or referred to other authorities, such as the intelligence services.

Organise repeated and multi-layered screening

In many countries, such as Australia, formal checks are built into the visa or funding process, meaning that several authorities are involved in the screening. In Sweden and Germany, government agencies are also responsible for visa checks. In the Netherlands, the system is based on the Modern Migration Policy Act (MoMi Act), under which higher education institutions act as recognised referees and are responsible for assessing the applications. When processing a visa application, the institution only needs to attach a copy of the passport and a personal statement. The Immigration and Naturalisation Service (IND) carries out

[7] RAND Europe Interview – 4.

[8] RAND Europe Interview – 14.

[9] RAND Europe Interview – 14.

[10] RAND Europe Interview – 8.

[11] Bokdam et al. (2023).

only randomised checks. As a result, the main responsibility lies heavily with the higher education institutions, whereas in other countries a multi-layered screening process is in place. Effective knowledge security requires multi-layered screening, in which both government agencies and higher education institutions play an active role throughout the entire process.

Utilise technical expertise in screening

The British system places a strong emphasis on technical expertise and interpretation. This is essential, as civil servants often lack the necessary knowledge of sensitive specialist fields. It is important to have experts who understand the risks and who continually update their knowledge, given the rapid changes within the scientific community.[12] The importance of technical expertise and interpretation is also evident in France.[13] There, researchers are given civil service appointments, making it easier to be both a civil servant and a researcher, or to switch between the roles. Scientists become a direct part of the screening process.[14] The key lesson is that effective knowledge security requires structural collaboration between civil servants, knowledge security coordinators and scientific experts, so that technical and strategic interpretation is always available when assessing risks. Establishing permanent consultation structures or expert groups can serve as best practice in this regard.

Coordinate information sharing and country-specific knowledge to identify fraud

One of the key lessons from this study is the importance of obtaining the correct information and having (country-specific) knowledge and data to interpret it accurately. What became clear from several case studies is that one of the most frequently identified forms of fraud is the withholding or misrepresentation of information, which, for example, obscures defence links. The Knowledge Security Desk regularly receives enquiries from knowledge institutions about foreign entities that change their names or merge with other institutions, making them more difficult to track.[15] Withholding certain funding is also common practice, as the Australian case study revealed.

Country-specific knowledge

A key safeguard for effective knowledge security screening is having specific country-specific knowledge, so that submitted documents and information can be interpreted correctly. For example, the Knowledge Security Desk has staff with knowledge of relevant languages and cultural contexts who are better able to assess risks. An understanding of funding sources from high-risk countries makes it possible to assess whether funding with potential defence links is involved. Furthermore, this expertise makes it easier to monitor developments at foreign entities, such as name changes. Country specialisation also helps in recognising recurring fraud patterns, as is evident from interviews with Nuffic and their Swedish counterpart. They employ country specialists who, thanks to their experience, can quickly identify patterns of fraud.

[12] RAND Europe Interview – 2.

[13] RAND Europe Interview – 2.

[14] RAND Europe Interview – 2.

[15] RAND Europe Interview – 4.

A good understanding of and data on risk indicators

Several interviews mentioned that the ASPI tracker is frequently used during the screening process. Such tools can help to correctly interpret the information provided during an application and thus mitigate certain risks, such as the use of historical institutional names or acronyms. Guidance from the government, along with coordination between risk indicators and the tools used to check them, would be welcome, to ensure that research institutions apply the same criteria.[16] The European Commission is working on the development of a secure IT platform that will collect reliable information on foreign research institutions to help researchers gain insight into the potential risks associated with recruiting foreign researchers.[17] It is desirable for research institutions to actively participate in the development and use of the European due diligence platform. By sharing experiences and best practices, the platform can be optimally tailored to the needs of the field.

Disclosure requirements

In Australia, for example, the ARC process includes so-called disclosure requirements for risk indicators, under which researchers with non-Australian affiliations are required to declare their funding and participation in talent programmes.[18] The ARC Research Security Framework specifies what information must be provided and places the responsibility for monitoring with the universities. These centralised disclosure requirements provide research institutions with clarity on what information they need to request and ensure a systematic approach. This makes it easier to detect fraud, such as the withholding of funding by the China Scholarship Council, and ensures that the consequences of failure to report are clear in advance. The introduction of comparable, centrally defined disclosure requirements can contribute to greater transparency and a level playing field.

Ensure European coordination to prevent leaks

The Knowledge Security Desk regularly hears from research institutions that there is a need for a more level playing field within Europe. There is competition between European universities, which makes it problematic when certain research in the Netherlands is hindered due to security risks associated with foreign researchers, whilst universities in other countries admit such researchers without hindrance. This can put Dutch institutions at a disadvantage.[19] Dutch research institutions also work closely with neighbouring countries, which means that sensitive knowledge and technology may still leak out.[20]

[16] Bokdam et al. (2023).

[17] European Union (2026).

[18] Australian Research Council (2026a)

[19] RAND Europe Interview – 4.

[20] European Union (2026).