RAND EUROPE



Identiteits- en documentfraude in de context van kennisveiligheid

Internationale casestudies en lessen voor Nederland

Judith Huismans, Scott Warnier, Conlan Ellis, Fook Nederveen

Dit onderzoek werd gefinancierd door het Wetenschappelijk Onderzoek- en Datacentrum (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.

© 2026 RAND Europe. Auteursrechten voorbehouden. Niets uit dit rapport mag worden verveelvoudigd en/of openbaar gemaakt door middel van druk, fotokopie, microfilm, digitale verwerking of anderszins, zonder voorafgaande schriftelijke toestemming van RAND Europe.

Voorwoord

De overheid maakt zich zorgen over de internationale positie van Nederlandse kennisinstellingen en wetenschappelijke samenwerking, die onder druk staan door groeiende geopolitieke dreigingen. In een brief aan de Tweede Kamer geeft zij aan dat kennis en technologie steeds vaker worden ingezet als geopolitieke machtsmiddelen, waarmee landen hun eigen politieke, economische en militaire positie kunnen versterken. Omdat de Nederlandse wetenschapssector wereldwijd toonaangevend is, vormt deze een belangrijk doelwit voor statelijke actoren om strategische kennis te verwerven en zo hun machtspositie te versterken (Tweede Kamer der Staten-Generaal 2026). In reactie hierop ontwikkelt de Nederlandse overheid nieuw beleid en wetgeving. Voorliggend onderzoek, uitgevoerd in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) en aangevraagd door het ministerie van Onderwijs, Cultuur en Wetenschap (OCW), probeert hieraan bij te dragen. Het doel is achterhalen hoe screening op identiteits- en documentfraude in Nederland en andere landen is georganiseerd, de aard en frequentie van fraudepraktijken in kaart brengen, en identificeren welke waarborgen ontworpen zijn om risico's te beperken. De uitkomsten van dit onderzoek bieden handvatten voor het ontwikkelen van proportioneel, uitvoerbaar beleid ter bescherming van de Nederlandse kennisveiligheid.

RAND Europe is een onafhankelijk not-for-profit onderzoeksbureau voor beleidsanalyse, met als missie besluitvorming te verbeteren en het publieke debat te informeren. RAND Europe is onderdeel van RAND, een wereldwijd opererende onderzoeksinstelling, en heeft kantoren in Cambridge (Verenigd Koninkrijk), Brussel (België) en Den Haag (Nederland). De auteurs willen allereerst hun dank uitspreken aan de wetenschappelijke begeleidingscommissie van dit onderzoek voor hun begeleiding en waardevolle commentaar op conceptversies van het rapport. Deze commissie bestond uit voorzitter prof. dr. Bert Niemeijer (Vrije Universiteit Amsterdam), dr. Karin Wittebrood (zelfstandig adviseur), dr. Bart van der Sloot (Tilburg University), een medewerker van OCW en dr. mr. Simon Zebregs (WODC). Daarnaast is dit rapport getoetst volgens de kwaliteitsstandaarden van RAND Europe voor onafhankelijk en hoogwaardig onderzoek door onze collega's Stijn Hoorens en dr. Christian van Stolk. Wij danken hen voor hun commentaar op een eerdere versie van dit rapport en suggesties ter verbetering. Tevens willen we graag alle geïnterviewde experts bedanken voor hun bijdrage. De auteurs zijn verantwoordelijk voor de inhoud van dit rapport. Voor meer informatie over RAND Europe of dit document kunt u contact opnemen met Judith Huismans (jhuismans@randeurope.org).

RAND Europe	RAND Europe	RAND Europe
Gardens Business Centre New Babylon	Rue de la Loi 82	Eastbrook House
Anna van Buerenplein 41	Bus 3	Shaftesbury Rd
2595 DA Den Haag	1040 Brussel	Cambridge CB2 8BF
Nederland	België	Verenigd Koninkrijk
Tel. +31 10 899 5916	Tel. +32 2669 2400	Tel. +44 1223 353 329

Samenvatting

Internationale samenwerking en het aantrekken van talent zijn cruciaal voor de wetenschappelijke en economische vooruitgang van Nederland. Tegelijkertijd uit de overheid zorgen over toenemende veiligheidsdreigingen vanuit landen die gericht proberen waardevolle kennis en technologie uit Nederland te verkrijgen.[1] China wordt in recente dreigingsanalyses steevast genoemd als de voornaamste bedreiging vanwege het verweven beleid van kennis- en innovatieverwerving in dienst van de nationale veiligheid en defensie.[2] Dit uit zich onder meer in grootschalige spionageprogramma's en het financieren van studenten en onderzoekers om toegang te krijgen tot geavanceerde technologieën. Dergelijke activiteiten bedreigen niet alleen de kennisveiligheid van onderwijs- en onderzoeksinstellingen, maar ook de innovatiekracht van bedrijven, de effectiviteit van de krijgsmacht en de strategische autonomie van Nederland.[3]

Het tegengaan van ongewenste kennisoverdracht en strategische afhankelijkheden vraagt om een sterk kennisveiligheidsbeleid.

Doelstellingen en onderzoeksopzet

Tegen deze achtergrond is er behoefte aan verdiepend onderzoek naar het beleid en de praktijk rond kennisveiligheid, specifiek gericht op de risico's van identiteits- en documentfraude binnen de Nederlandse kennissector. Gedocumenteerde casuïstiek is schaars, wat het lastig maakt om effectief en proportioneel beleid te ontwikkelen. Lessen uit de praktijk over de inzet van identiteits- en documentatiefraude om toegang te krijgen tot sensitieve technologie en kennis kunnen niettemin belangrijke inzichten opleveren voor het ontwikkelen van een uitvoerbaar en efficiënt screeningsproces. Op aanvraag van het ministerie van Onderwijs, Cultuur en Wetenschap (OCW) heeft het Wetenschappelijk Onderzoek- en Datacentrum (WODC) daarom aan RAND Europe gevraagd om te analyseren hoe screening op identiteits- en documentfraude in Nederland en een selectie van andere landen is georganiseerd, welke vormen van fraude voorkomen, hoe frequent deze zich voordoen en welke waarborgen effectief zijn om deze risico's tegen te gaan.

Het onderzoek omvat een literatuurstudie naar de wijze waarop en de frequentie waarmee identiteits- en documentatiefraude worden gepleegd, en vier casestudies: Nederland, Australië, Duitsland en Zweden. De casestudies zijn gebaseerd op bureauonderzoek en interviews met experts die beschikken over specialistische kennis rond kennisveiligheid, identiteitscontrole en documentverificatie. Door de ervaringen, werkwijzen

[1] Tweede Kamer der Staten-Generaal (2026).

[2] NCTV (2025).

[3] NCTV (2025).

en uitdagingen in deze landen te vergelijken, zijn relevante lessen geïdentificeerd voor Nederland. Interviews zijn ingezet om ontbrekende informatie aan te vullen en inzicht te geven in de praktijk.

Bevindingen

Wat is bekend over de wijze waarop identiteits- en documentatiefraude wordt gepleegd om toegang te krijgen tot kennisinstellingen in Nederland en daarbuiten?

Informatie over fraude met betrekking tot kennisveiligheid in Nederland wordt niet centraal geregistreerd of geanalyseerd. De verschillende actoren zijn door deze gefaseerde aanpak slechts in staat om een deel van het fraudebeeld te schetsen. In de interviews komen verschillende modus operandi van fraude aan bod. Het Loket Kennisveiligheid hoort regelmatig van kennisinstellingen dat informatie over bijvoorbeeld defensiegerelateerde banden bewust wordt weggelaten uit cv's. Dit gebeurt mede door de toegenomen aandacht voor kennisveiligheid en het groeiende bewustzijn bij kennisinstellingen van de risico's die bepaalde connecties met zich meebrengen. Waar dergelijke banden voorheen als prestigieus werden gezien, zijn instellingen zich nu meer bewust van de mogelijke risico's en de rol van statelijke actoren. Nuffic, de organisatie voor internationalisering in het onderwijs, adviseert Nederlandse kennisinstellingen over de waardering van buitenlandse diploma's en verstrekt jaarlijks circa 30.000 niet-bindende adviezen. Daarbij controleert Nuffic de authenticiteit en erkenning van diploma's door de bevoegde autoriteit en beoordeelt ze bijbehorende documenten zoals cijferlijsten. Door te toetsen of het gehele opleidingstraject logisch en consistent is verlopen, kan Nuffic mogelijke fraude opsporen. Omdat gebruik wordt gemaakt van kopieën kan het echter lastiger zijn om fraude vast te stellen, zeker als er statelijke actoren bij betrokken zijn. Nuffic signaleert dat fraude met diploma's vaker voorkomt uit bepaalde landen, maar onderzoekt niet expliciet of er een link is met kennisveiligheid. Daarnaast bestaan er bekende *diploma mills* – of diplomafabrieken – waar valse diploma's kunnen worden besteld.

In Australië zijn regelgevingsmechanismen zoals de PACT-voorschriften (*Protecting Australia's Critical Technology*) en het ARC-kader (Australian Research Council) ontworpen om grondige controles van documenten en bewijsstukken uit te voeren. Echter ligt de primaire focus daarbij niet op het opsporen van fraude en het verifiëren van de authenticiteit van documenten zoals identiteitsbewijzen en diploma's, maar veeleer op het identificeren van potentiële risico's. Uit interviews met Australische experts komt naar voren dat het geven van onjuiste informatie de belangrijkste vorm van fraude is die in Australië wordt aangetroffen, met name in cv's en subsidieaanvragen. Een van de meest zorgwekkende trends die zich de afgelopen twaalf tot achttien maanden heeft afgetekend, is het opzettelijk achterhouden van de herkomst van studiebeurzen. Er is sprake van een toenemende, systematische verkeerde voorstelling van financiering en van gevallen waarin personen opzettelijk aangeven banden te hebben met instellingen met een lager risico en hun banden met de daadwerkelijke (en mogelijk risicovollere) organisaties verzwijgen. Op cv's laten personen vaak bepaalde banen of stages weg in de officiële versies die zij indienen, en bewaren zij de volledige details voor cv's die privé worden gedeeld. Hetzelfde patroon is waarneembaar bij onderzoeksresultaten: onderzoek zonder *dual use* wordt openbaar gemaakt, terwijl militair gerelateerd onderzoek wordt verborgen. Bovendien worden affiliaties met organisaties vaak niet vertaald, waardoor hun werkelijke betekenis nog verder wordt achtergehouden. Een andere vastgestelde vorm van fraude betrof zijn valse uitnodigingsbrieven voor visumdoeleinden. Vaak worden gevallen gesignaleerd door andere instellingen voor hoger onderwijs die

contact opnemen om te bevestigen dat een uitnodiging authentiek is. Deze informatie-uitwisseling wordt mogelijk gemaakt door het Australische Informal Foreign Interference Network (INFIN), een niet-gouvernementele organisatie van 39 Australische instellingen voor hoger onderwijs die gezamenlijk de inspanningen tegen ongewenste inmenging en de naleving van overheidsvoorschriften bespreken.

In Duitsland ligt de verantwoordelijkheid voor screening bij de onderzoekers en universiteiten zelf. De wettelijke verplichtingen beperken zich tot exportcontroles op militaire en dual-use-technologieën. Instellingen moeten zelf informatie verzamelen over veiligheidsrelevante aspecten, vaak met behulp van externe bronnen zoals de ASPI-tracker, een tracker van het Australian Strategic Policy Institute (ASPI) die defensielinks van Chinese universiteiten in kaart brengt, maar die bieden beperkte en soms onduidelijke informatie. De Duitse binnenlandse veiligheidsdienst (Bundesamt für Verfassungsschutz – BfV) geeft wel een overzicht van methoden die risicovolle landen inzetten om gevoelige technologieën en kennis te vergaren, waarvan het ontwijken van export- en kenniscontrole door misleidende informatie in aanvragen te gebruiken direct relevant is voor kennisveiligheid. Dit komt overeen met trends in andere landen.[4]

Zweden hanteert een gecentraliseerd aanmeldingssysteem voor het hoger onderwijs dat beheerd wordt door de Zweedse Raad voor Hoger Onderwijs (UHR). UHR adviseert en biedt referenties, maar universiteiten en hogescholen beslissen zelf over toelating en zijn verantwoordelijk voor het controleren van kwalificaties en het opsporen van fraude. Bij PhD-aanmeldingen ligt deze verantwoordelijkheid volledig bij de instellingen zelf. Er is geen centrale rapportageplicht, waardoor de UHR geen inzicht heeft in het aantal fraudegevallen bij de instellingen. In een interview werd benoemd dat kandidaten met vervalste diploma's van diploma mills – instanties en personen die zich bezighouden met de verkoop van diploma's en academische graden zonder dat er een studieprogramma is gevolgd – zijn toegelaten tot PhD-programma's, wat de ernst van de kwestie onderstreept. Diploma mills vormen een groeiende uitdaging.

In het Verenigd Koninkrijk is er ook aandacht voor het achterhouden van informatie. Binnen ATAS (Academic Technology Approval Scheme) wordt niet alleen gekeken naar de inhoud van een aanvraag, maar ook naar mogelijke omissies, zoals hiaten in cv's. De aangeleverde documenten worden vergeleken met open-source-informatie en als bepaalde zaken niet worden genoemd, kan dit aanleiding zijn voor verder onderzoek.

Samenvattend lijken de belangrijkste modus operandi wat betreft identiteits- en documentatiefraude in de context van kennisveiligheid:

- Het gebruik van onvolledige documenten en het bewust achterhouden van informatie, bijvoorbeeld over affiliaties of herkomst van financiering;
- Het verdraaien of geven van onjuiste informatie, door bijvoorbeeld minder risicovolle affiliaties te vermelden. Het niet vertalen van dergelijke affiliaties kan het moeilijker maken om de werkelijke betekenis te achterhalen;
- Valse diploma's, bijvoorbeeld gefabriceerd door diploma mills;
- Valse uitnodigingsbrieven voor visumdoeleinden.

[4] Bundesamt für Verfassungsschutz (2026).

In hoeverre is er een beeld van de frequentie waarin deze fraude plaatsvindt in Nederland en daarbuiten?

Uit het literatuuronderzoek en de interviews is gebleken dat het zeer lastig is om een goed beeld te krijgen van de frequentie waarin deze fraude plaatsvindt in Nederland. Dit komt met name doordat sprake is van een gedecentraliseerd systeem, waarbij de verantwoordelijkheid voor de screening grotendeels bij de kennisinstellingen zelf ligt. Verschillende instanties controleren onderdelen van het proces, zoals de authenticiteit van diploma's, en hebben daardoor soms zicht op fraude binnen hun eigen domein. Zij geven echter aan geen volledig overzicht te hebben. Zo heeft Nuffic een adviserende rol, maar zijn universiteiten niet verplicht diploma's door Nuffic te laten controleren.

Volgens geïnterviewde experts in Australië zijn er tot op heden geen gevallen ontdekt van personen die onder een valse identiteit reisden. Zij voegen hieraan toe dat – aangezien buitenlandse staatsactoren de grootste bedreiging vormen – het wellicht onmogelijk is om frauduleuze referenties op te sporen wanneer deze door overheidsinstanties zijn uitgegeven. Zoals eerder aangegeven is de belangrijkste vorm van fraude in Australië het geven van onjuiste informatie, met name in cv's en subsidieaanvragen. Ook van de omvang van dit fenomeen bestaat geen compleet beeld. Dat het gebeurt is echter duidelijk: de China Scholarship Council rapporteerde in 2024 1.000 ontvangers van financiering in Australië en toch gaven slechts 350 studenten openlijk toe deze steun te ontvangen. Deze aanzienlijke discrepantie onderstreept hoe vaak personen niet transparant zijn over de aard of de bron van hun onderzoeksfinanciering. Omdat het hierbij gaat om een enkele bron van financiering, is dit mogelijk slechts het topje van de ijsberg van een groter probleem waarbij ook andere informatie wordt achtergehouden. Wat betreft valse uitnodigingsbrieven voor visumdoeleinden registreerde de Australische universiteit van New South Wales in de afgelopen twee tot drie jaar 6 tot 12 gevallen. Dit komt voornamelijk voor op faculteitsniveau, bij gastwetenschappers. Opvallend is dat er geen relevante casestudies zijn met betrekking tot de PACT-voorschriften. Hoewel het PACT-mechanisme is toegepast om visumaanvragen te beperken, blijven beslissingen hierover buiten het publieke domein. Tijdens een interview wordt opgemerkt dat deze alleen openbaar worden gemaakt als een aanvrager in de toekomst besluit een beslissing aan te vechten.

Net als in Duitsland, ligt ook in Zweden de verantwoordelijkheid bij de kennisinstellingen zelf, waardoor het eveneens in dit land lastig is om een beeld te krijgen van de frequentie. Wel worden toelatingen van bachelor- en masterstudenten gecentraliseerd bij de UHR behandeld. Uit een interview kwam naar voren dat voor academische toelatingen via het UHR-portaal het aantal gemelde fraudegevallen is gestegen, van 30 in 2024 tot 130 in 2025. Dit wordt grotendeels toegeschreven aan het gebruik van AI-agenten waardoor de aanmeldingsprocedure toegankelijker zou zijn geworden. Hier is echter geen directe link met kennisveiligheid te maken, want het kan bijvoorbeeld ook gaan om fraude om economische migratiedoeleinden. De aantallen geven echter wel een beeld van de schaal en de mogelijk groeiende rol van AI.

Welke waarborgen kunnen worden gecreëerd om de verschillende vormen van fraude tegen te gaan?

Uit het literatuuronderzoek en de interviews komen meerdere lessen voor Nederland naar voren, dan wel waarborgen die kunnen worden gecreëerd om de verschillende vormen van fraude tegen te gaan.

Screening op individueel en institutioneel-/landenniveau beter samenbrengen

Interviews en praktijkervaringen laten zien dat het opsporen van inconsistenties essentieel is voor het signaleren van fraude, vooral bij het gebruik van kopieën of de betrokkenheid van statelijke actoren.[5] Uit een interview voor de casestudie over Zweden bleek bijvoorbeeld dat het verifiëren van publicaties een van de voornaamste manieren is waarop ze controleren op mogelijke defensielinks.[6] Ook kunnen publicaties worden vergeleken met informatie op een cv waardoor inconsistenties aan het licht kunnen komen.[7] In Nederland ontvangt het Loket Kennisveiligheid, het centraal adviespunt voor kennisinstellingen, geen persoonsgegevens. Individuele screening ligt bij de kennisinstellingen, die hiervoor vaak beperkte middelen en landenkennis hebben. Een volledig beeld is daarom afhankelijk van vrijwillige coördinatie en kennisdeling tussen instanties. In bijvoorbeeld Frankrijk komt kennis over risico's op individueel en institutioneel-/landenniveau meer samen, doordat de kennisveiligheidscoördinator binnen kennisinstellingen een vertrouwelijke functie heeft en wordt aangesteld door de overheid.

Verken informatievoorziening voor kennisinstellingen over kennisdeling

Controles ten behoeve van kennisveiligheid zijn in alle onderzochte landen versnipperd over meerdere instanties. Dit wordt verder gecompliceerd doordat de benodigde informatie doorgaans persoonsgegevens omvat, en het delen ervan secuur en in overeenstemming met privacywetgeving moet gebeuren. In Zweden wordt dit bijvoorbeeld als heikel punt ervaren. Zelfs als fraude wordt vastgesteld tijdens een toelatingsprocedure kan deze informatie vaak niet extern, of zelfs niet intern, gedeeld worden.[8] In Zweden geeft de UHR zowel erkenning met het oog op de arbeidsmarkt als met het oog op vervolgstudies. Vanwege de regels rond gegevensbescherming is het delen van informatie tussen de twee procedures verboden, zelfs wanneer een persoon voor beide doeleinden een aanvraag heeft ingediend.[9] In Nederland geven betrokken instanties zoals Nuffic adviezen, maar zijn kennisinstellingen niet verplicht om advies in te winnen en behouden ze altijd de bevoegdheid om zelf te beslissen over toelating. Hierdoor kan het voorkomen dat een student, voor wie Nuffic zich heeft onthouden van advies vanwege twijfels over de authenticiteit of erkenning van documenten, bij de ene instelling niet wordt toegelaten, maar elders wel. In de praktijk vragen kennisinstellingen voor bepaalde herkomstlanden vrijwel altijd advies aan, maar ligt de interpretatie en uiteindelijke beslissing bij de instelling zelf.[10] Uit eerder onderzoek bleek al dat kennisinstellingen het zonder duidelijke wettelijke kaders lastig vinden om in te schatten wat ze AVG-technisch mogen opvragen en wie ze wel en niet moeten toetsen.[11] Kennisinstellingen hebben behoefte aan heldere richtlijnen en praktische ondersteuning over wat zij op grond van privacywetgeving mogen opvragen, wie zij wel of niet moeten screenen en hoe persoonsgegevens gedeeld mogen worden. Ook is er behoefte aan duidelijke richtlijnen over wanneer en op welke wijze fraudegevallen moeten worden opgeschaald of doorgezet naar andere instanties, zoals de inlichtingendiensten.

---

[5] RAND Europe Interview – 8.

[6] RAND Europe Interview – 9.

[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).

Organiseer herhaalde en gelaagde screening

In veel landen, zoals Australië, zijn formele controles ingebouwd in het visum- of financieringsproces, waardoor meerdere instanties betrokken zijn bij de screening. In Zweden en Duitsland zijn overheidsinstanties verantwoordelijk voor visumcontroles. In Nederland is het systeem gebaseerd op de Wet modern migratiebeleid (wet MoMi), waarbij kennisinstellingen als erkende referenten optreden en een belangrijke verantwoordelijkheid dragen voor het indienen en onderbouwen van aanvragen. De formele beoordeling van en beslissing op aanvragen blijft bij de IND. Het systeem gaat daarbij uit van een vertrouwensrelatie tussen de overheid en de erkende referent, waarbij controles mede op basis van signalen en achteraf steekproefsgewijs plaatsvinden.[12] Hierdoor speelt de kennisinstelling een belangrijke rol in het toelatingsproces, terwijl in andere landen de overheid een grotere rol speelt bij het visumproces. Effectieve kennisveiligheid vraagt om gelaagde screening, waarbij zowel overheidsinstanties als kennisinstellingen een actieve rol spelen gedurende het hele traject.

Zet technische expertise in bij screening

Het Britse systeem legt een sterke nadruk op technische expertise en duiding. Dit is essentieel, omdat ambtenaren vaak niet over de benodigde kennis van sensitieve vakgebieden beschikken. Het is belangrijk om experts te hebben die inzicht hebben in de risico's en die hun kennis voortdurend op peil houden, gezien de snelle veranderingen binnen de wetenschap.[13] Het belang van technische expertise en duiding komt ook in Frankrijk naar voren.[14] Daar krijgen onderzoekers een ambtelijke aanstelling, waardoor het makkelijker is om zowel ambtenaar als onderzoeker te zijn of tussen de functies te wisselen. Zo worden wetenschappers direct onderdeel van het screeningsproces.[15] De belangrijkste les is dat effectieve kennisveiligheid vraagt om structurele samenwerking tussen ambtenaren, kennisveiligheidscoördinatoren en wetenschappelijke experts, zodat technische en strategische duiding altijd beschikbaar is bij de beoordeling van risico's. Het opzetten van vaste overlegstructuren of expertgroepen, kan hierbij als *best practice* dienen.

Coördineer informatieverstrekking en landenkennis om fraude te herkennen

Een van de belangrijkste lessen uit dit onderzoek is het belang van het verkrijgen van de juiste informatie en het hebben van (landen)kennis en data om deze juist te interpreteren. Wat duidelijk werd uit meerdere casestudies is dat een van de meest gesignaleerde vormen van fraude het achterhouden of verdraaien van informatie is, waardoor bijvoorbeeld defensielinks niet zichtbaar worden. Het Loket Kennisveiligheid krijgt regelmatig vragen van kennisinstellingen over buitenlandse entiteiten die van naam veranderen of fuseren met andere instituten, wat het lastiger maakt om ze te volgen.[16] Ook het achterhouden van bepaalde financiering is gangbaar, zoals bleek uit de Australische casestudie. De China Scholarship Council rapporteerde in 2024 1.000 ontvangers van financiering in Australië, maar bij hun aanmelding gaven slechts 350 studenten openlijk toe deze steun te ontvangen.[17]

---

[12] Lodder (2019).

[13] RAND Europe Interview – 2.

[14] RAND Europe Interview – 2.

[15] RAND Europe Interview – 2.

[16] RAND Europe Interview – 4.

[17] RAND Europe Interview – 7.

Landenkennis

Een belangrijke waarborg voor een effectieve kennisveiligheidsscreening is het beschikken over specifieke landenkennis, zodat aangeleverde documenten en informatie correct kunnen worden geïnterpreteerd. Het Loket Kennisveiligheid heeft bijvoorbeeld medewerkers met kennis van relevante talen en culturele context die risico's beter kunnen inschatten. Inzicht in financieringsbronnen uit risicolanden maakt het mogelijk om te beoordelen of er sprake is van financiering met mogelijke defensielinks. Daarnaast maakt deze expertise het eenvoudiger om ontwikkelingen bij buitenlandse entiteiten, zoals naamswijzigingen, te volgen. Landenspecialisatie draagt bovendien bij aan het herkennen van terugkerende fraudepatronen, zoals ook uit interviews met Nuffic en hun Zweedse tegenhanger blijkt. Daar werken landenspecialisten die door hun ervaring snel patronen in fraude kunnen identificeren.

Goed begrip van en data over risicoindicatoren

In meerdere interviews komt naar voren dat tijdens het screeningsproces veelvuldig gebruik wordt gemaakt van de ASPI-tracker. Dergelijke instrumenten kunnen helpen om de informatie die wordt aangeleverd tijdens een aanmelding juist te interpreteren en zo bepaalde risico's tegen te gaan, zoals het gebruik van historische institutionele namen of acroniemen. Advies vanuit de overheid, afstemming tussen risicoindicatoren en tools om hierop te checken zouden welkom zijn, zodat kennisinstellingen dezelfde afwegingen maken.[18] De Europese Commissie werkt aan de ontwikkeling van een beveiligd IT-platform dat betrouwbare informatie over buitenlandse onderzoeksinstellingen zal verzamelen om onderzoekers te helpen inzicht te krijgen in de mogelijke risico's die gepaard gaan met het aannemen van buitenlandse onderzoekers.[19] Het is wenselijk dat kennisinstellingen actief participeren in de ontwikkeling en het gebruik van het Europese due-diligence-platform. Door ervaringen en best practices te delen, kan het platform optimaal aansluiten bij de behoeften van de praktijk.

Disclosure-voorwaarden

In Australië gelden in het ARC-proces bijvoorbeeld zogenoemde disclosure-voorwaarden voor risicoindicatoren, waarbij onderzoekers met niet-Australische affiliaties hun financiering en deelname aan talentprogramma's verplicht moeten melden.[20] Het ARC Research Security Framework bepaalt welke informatie verstrekt moet worden en legt de controle bij de universiteiten. Deze centrale disclosure-eisen geven kennisinstellingen helderheid over welke informatie zij moeten opvragen en zorgen voor een systematische aanpak. Hierdoor kan fraude, zoals het achterhouden van financiering door de China Scholarship Council, beter worden vastgesteld en zijn de consequenties van het niet melden vooraf duidelijk. Het invoeren van vergelijkbare, centraal vastgelegde disclosure-voorwaarden kan bijdragen aan meer transparantie en een eerlijk speelveld.

Zorg voor Europese coördinatie om weglekken te voorkomen

Het Loket Kennisveiligheid hoort regelmatig van kennisinstellingen dat er behoefte is aan een gelijker speelveld binnen Europa. Er bestaat concurrentie tussen Europese universiteiten, waardoor het

[18] Bokdam et al. (2023).

[19] European Union (2026).

[20] Australian Research Council (2026a)

problematisch is als in Nederland bepaald onderzoek wordt gehinderd vanwege veiligheidsrisico's rond buitenlandse onderzoekers, terwijl universiteiten in andere landen dergelijke onderzoekers ongehinderd toelaten. Dit kan Nederlandse instellingen op achterstand zetten.[21] Ook werken Nederlandse kennisinstellingen nauw samen met omliggende landen, waardoor sensitieve kennis en technologie alsnog kunnen weglekken.[22]

[21] RAND Europe Interview – 4.

[22] European Union (2026).

Inhoudsopgave

Voorwoord i
Samenvatting iii
1. Inleiding 1
1.1. Achtergrond en aanleiding 1
1.2. Reikwijdte 4
1.3. Doelstelling en onderzoeksvragen 9
1.4. Methodologie 9
1.5. Beperkingen 14
1.6. Leeswijzer 15
2. Nederland 15
2.1. Kennisveiligheid: algemene context 16
2.2. Beleid en wetgeving 17
2.3. Screeningsprocedures 21
2.4. Document- en identiteitsfraude 24
2.5. Bevindingen en conclusies 27
3. Australië 30
3.1. Kennisveiligheid: algemene context 30
3.2. Beleid, wetgeving en screeningsprocedures 32
3.3. Document- en identiteitsfraude 37
3.4. Bevindingen en conclusie 38
4. Duitsland 40
4.1. Kennisveiligheid: algemene context 40
4.2. Beleid en wetgeving 42
4.3. Screeningsprocedures 47
4.4. Document- en identiteitsfraude 48
4.5. Bevindingen en conclusies 48
5. Zweden 51
5.1. Kennisveiligheid: algemene context 51

5.2. Beleid 53
5.3. Document- en identiteitsfraude 56
5.4. Bevindingen en conclusies 58
6. Het Verenigd Koninkrijk en Frankrijk 59
6.1. Het Verenigd Koninkrijk 60
6.2. Frankrijk 61
7. Conclusies en lessen voor Nederland 64
Bronnen 76

1. Inleiding

In dit hoofdstuk bespreken we achtereenvolgens de achtergrond en aanleiding van dit onderzoek (paragraaf 1.1), de doelstelling en de onderzoeksvragen (paragraaf 1.3), de onderzoeksopzet (paragraaf 1.3), de reikwijdte (paragraaf 1.4) en de beperkingen van dit onderzoek (paragraaf 1.5).

1.1. Achtergrond en aanleiding

Geopolitieke dreigingen voor de Nederlandse kennissector zet internationale samenwerking onder druk

Wetenschap is gebaat bij internationale samenwerking en het aantrekken van talentvolle studenten en wetenschappers. De overheid maakt zich echter zorgen om de dreiging richting de wetenschappelijk sector veroorzaakt door geopolitieke ontwikkelingen. In de Kamerbrief *Aanpak Kennisveiligheid – voortbouwen op een solide basis*, uitgestuurd in juni 2026, wordt gesteld dat kennis en technologie een steeds belangrijkere rol spelen in de geopolitieke verhoudingen, waarbij landen deze inzetten om hun eigen positie op politiek, economisch en militair vlak te versterken. Zijn wereldwijde koppositie maakt van de Nederlandse wetenschapssector een aantrekkelijk doelwit voor statelijke actoren die strategische kennis willen verwerven om hun machtspositie te vergroten.[23] Uit dreigingsanalyses van onder andere de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) komt naar voren dat landen of organisaties Nederlandse wetenschappelijke kennis kunnen inzetten op een manier die de nationale veiligheid kan raken. De verwerving van Nederlandse kennis en technologie vormt een bedreiging voor de kennisveiligheid van Nederlandse onderwijs- en onderzoeksinstellingen, het innovatievermogen van bedrijven en hun winstgevendheid, evenals de effectiviteit van de krijgsmacht. Ze kan ook leiden tot een grotere, ongewenste strategische afhankelijkheid, met name op het gebied van vitale infrastructuur.[24] Daarnaast lopen Nederlandse kennisinstellingen volgens de NCTV het risico hun strategische leidende positie op de middellange termijn te verliezen.[25]

Uit het *Dreigingsbeeld Statelijke Actoren (DBSA) 2025* van NCTV, Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) komt duidelijk naar voren dat China, Rusland, Iran en Noord-Korea de grootste dreiging vormen voor de Nederlandse kennisveiligheid.[26] Deze landen proberen, onder andere via heimelijke verwervingsnetwerken, kennisinstellingen, studenten en onderzoekers, kennis en technologie te verwerven in Nederland. Rusland

[23] Tweede Kamer der Staten-Generaal (2026).

[24] NCTV (2025).

[25] NCTV (2025).

[26] NCTV (2025).

richt zich daarbij vooral op de ontwikkeling van militaire toepassingen van verschillende technologieën en Iran vooral op het gebied van ballistische raketten. Het overdragen van dergelijke kennis of technologieën door kennisinstellingen naar gesanctioneerde landen zoals deze drie, is verboden op grond van verordeningen en besluiten in het kader van het Gemeenschappelijk Buitenlands en Veiligheidsbeleid (GBVB) van de Europese Unie (EU).[27] Het DBSA laat verder zien dat ook in Nederland Chinese wetenschappers met militaire banden kennis hebben opgedaan bij kennisinstellingen.[28]

Dreigingen voor de kennisveiligheid in Nederland kunnen echter vanuit vrijwel alle delen van de wereld komen, en de dreigingsanalyses kunnen in de toekomst dusdanig veranderen dat andere landen een risico vormen. Dit kan ook in Nederland tot politieke vraagstukken leiden.

In de verschillende dreigingsbeelden die het NCTV en de inlichtingendiensten in de afgelopen jaren gepubliceerd hebben, komt China steevast naar voren als de grootste dreiging op het gebied van kennisveiligheid.[29] In het Chinese overheidsbeleid staan kennis en innovatie nadrukkelijk ten dienste van de nationale veiligheid. Zo verweeft het Military-Civil Fusion-beleid technologische doelen met militaire en andere veiligheidsdoelen.[30] In het *Dreigingsbeeld Statelijke Actoren 2025* wordt benoemd dat voor de Chinese president Xi Jinping kennis en innovatie nadrukkelijk in dienst staan van China's nationale veiligheid.[31] In zijn jaarverslag van 2024 geeft de MIVD (2025) aan dat China's whole-of-society-benadering ervoor zorgt dat het onderscheid tussen normale academische of economische uitwisseling en spionageactiviteiten vervaagt. De MIVD kijkt met name naar de overdracht van hoogwaardige Nederlandse kennis en technologie naar China. Technologisch onderzoek waarin Nederland een sterke positie heeft, zoals op het gebied van halfgeleiders, kunstmatige intelligentie (AI) en kwantumtechnologie, is hierbij essentieel (NCTV 2025). In zijn rapport over decentrale contacten met China geeft de NCTV (2023) aan dat de sectoren waarbinnen China op zoek is naar buitenlandse kennis en kunde om meer zelfvoorzienend te worden, grotendeels overeenkomen met wat de Nederlandse overheid heeft aangemerkt als topsectoren.

Volgens het *Dreigingsbeeld Statelijke Actoren* van de NCTV, AIVD en MIVD blijven individuen en organisaties die banden hebben met China's militair-industrieel complex dan ook toenadering zoeken tot Nederlandse kennisinstellingen. Zo zouden tussen 2012 en 2022 meer dan 90 Chinese (militaire) wetenschappers kennis opgedaan hebben bij Nederlandse kennisinstellingen. In zijn jaarverslag van 2024 stelt de AIVD (2025) dat China in 2024 via zeer uitgebreide spionageprogramma's aan hoogwaardige technologie en kennis probeerde te komen. Ook zou China studenten en wetenschappers financieren die bij westerse kennisinstellingen gevoelige kennis kunnen opdoen. In 2021 heeft de Europese Commissie (EC) een document gepubliceerd over de aanpak van onderzoek en innovatie, waarin ze schrijft: '..sommige landen streven in toenemende mate naar technologisch leiderschap door middel van discriminerende maatregelen en gebruiken onderzoek en innovatie vaak als middel om wereldwijde invloed te verwerven en

[27] Onder andere de Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (herschikking).

[28] NCTV (2025, 42).

[29] NCTV (2025).

[30] Bitzinger (2021).

[31] NCTV (2025).

maatschappelijke controle uit te oefenen' (Europese Commissie 2021). Hierin wordt aangegeven dat China's positie als economische concurrent en systemische rivaal van de EU het noodzakelijk maakt om de samenwerking op het gebied van onderzoek en innovatie opnieuw in evenwicht te brengen.

Europese Unie

De afgelopen jaren zijn er in verschillende Europese lidstaten en op het niveau van de Europese Unie discussies geweest over het versterken van de kennisveiligheid, als reactie op het feit dat het onderzoeks- en innovatielandschap steeds kwetsbaarder wordt voor risico's zoals kwaadwillige beïnvloeding en misbruik.[32] Kader 1 geeft een beknopt overzicht van verschillende initiatieven in de EU die nuttige context vormen voor de Europese casestudies.

Kader 1. EU-initiatieven op het gebied van kennisveiligheid

- In mei 2024 heeft de Raad van de Europese Unie (Raad van de EU) de aanbeveling inzake het versterken van de kennisveiligheid aangenomen. Deze is gericht op het aanpakken van risico's die verband houden met internationaal onderzoek en innovatie. Aanbevolen wordt dat nationale autoriteiten beleid inzake kennisveiligheid ontwikkelen, dat nationale financiers robuuste waarborgen inbouwen en dat onderzoekers (zoals universiteiten) risicobeheerprocessen invoeren. Overheidsinstanties moeten de sector hierbij ondersteunen en onderzoekers in staat stellen weloverwogen beslissingen te nemen over internationale samenwerking. Daartoe is kennisveiligheid opgenomen als prioritaire actie in de volgende agenda voor de European Research Area, of ERA-beleidsagenda 2025-2027, zoals aangenomen door de Raad van de EU in mei 2025.
- De Europese Commissie zal de voortgang van de uitvoering volgen via een research security monitor. Daarnaast wordt gewerkt aan de oprichting van een Europees expertisecentrum voor kennisveiligheid, om te investeren in een empirische basis voor beleidsvorming en om een praktijkgemeenschap in de hele EU te creëren. Dit centrum zal naar verwachting medio 2026 van start gaan.
- In oktober 2025 heeft de Europese Commissie toegezegd kennisveiligheid in wetgeving te verankeren door deze op te nemen in het voorstel voor de wet inzake de Europese Onderzoeksruimte. Andere voorgestelde EU-initiatieven zijn, naast het op te richten Europese expertisecentrum voor kennisveiligheid, de oprichting van een due-diligence-platform om onderzoekers te helpen bij het beoordelen van risico's en de ontwikkeling van een nieuwe gemeenschappelijke methodologie voor lidstaten om de veerkracht van hun onderzoeksinstellingen te testen.

Bron: Europese Commissie (2025).

Nieuwe wetgeving en screeningsbeleid om kennisveiligheid in Nederland te versterken

Om Nederland beter te beschermen tegen ongewenste kennisoverdracht en spionage, wordt er gewerkt aan nieuwe voorstellen voor het verbeteren van de kennisveiligheid in Nederland.[33] Tot voor kort was er een wetsvoorstel in voorbereiding voor een Wet screening kennisveiligheid (Internetconsultatie.nl 2025). Dit wetsvoorstel werd aangeboden voor internetconsultatie door voormalig minister van Onderwijs, Cultuur en Wetenschap (OCW) Eppo Bruins, mede namens de minister van Justitie en Veiligheid (JenV) en in overleg met de minister van Economische Zaken (EZ). In het voorstel werd gestreefd naar inwerkingtreding medio 2027 (Rijksoverheid 2025). De wet zou Nederlandse kennisinstellingen verplichten om (aspirant-)studenten, onderzoekers en technisch ondersteunend personeel te screenen die toegang zouden krijgen tot gevoelige technologieën, zoals AI, kwantum en biotechnologie.

[32] Europese Commissie (2025; 2026).

[33] Tweede Kamer der Staten-Generaal (2026).

Ongewenste kennis- en technologieoverdracht omvat twee categorieën risico's voor de nationale veiligheid: ongewenst eindgebruik van sensitieve technologie en het ontstaan van risicovolle strategische afhankelijkheden (Internetconsultatie.nl 2025). Van ongewenst eindgebruik is sprake als de kennis of technologie bijvoorbeeld wordt ingezet in militaire toepassingen. Strategische afhankelijkheden worden tegengegaan door de eigen kennispositie te beschermen en versterken, waardoor statelijke actoren zoveel mogelijk de kans wordt ontnomen om Nederland of de EU onder druk te zetten (Internetconsultatie.nl 2025).

Gezien de ernst van de dreigingen is er dus veel aan gelegen om een sterk beleid te hebben voor kennisveiligheid. Tegelijkertijd is het essentieel om de vrije uitwisseling van wetenschappelijke kennis te waarborgen, het aantrekkelijke vestigingsklimaat voor talentvolle onderzoekers te behouden, en internationale samenwerking te stimuleren. De open onderzoeksomgeving waarin Nederlandse kennisinstellingen uitblinken, draagt immers bij aan wetenschappelijke vooruitgang en innovatie. Kennisveiligheidsbeleid dient daarom oog te houden voor de gevolgen de proportionaliteit en de uitvoerbaarheid van de maatregelen.

Het ministerie van OCW voerde sinds het opstellen van het wetsvoorstel gesprekken met Justis, een onderdeel van het ministerie van JenV, als beoogd uitvoerder van de screening. In 2025, is namens het Wetenschappelijk Onderzoek- en Datacentrum (WODC) al onderzoek gedaan naar de bestaande praktijk op het gebied van screening en toelating van (master)studenten en onderzoekers aan Nederlandse kennisinstellingen (Blom et al. 2025). Er werd onder meer gekeken naar de wijze waarop identiteits- en documentcontrole in het screeningsproces zijn geïntegreerd. Het gaat hierbij om de controle van identiteit en authenticiteit van aangeleverde documenten zoals diploma's, visa, referenties, identiteitsdocumenten en cv's. De vraag bleef toen openstaan welke typen casuïstiek zich in de praktijk concreet voordoen rondom kennisveiligheid.

1.2. Reikwijdte

Om de focus van het onderzoek te onderbouwen, presenteren we hieronder een conceptuele kadering van kennisveiligheid en het bijbehorende dreigingslandschap. We gaan in op de definitie van kennisveiligheid, de strategische belangen die ermee gemoeid zijn, de belangrijkste dreigingsvectoren en de rol van identiteits- en documentfraude. Daarnaast besteden we aandacht aan de verschillende internationale benaderingen van kennisveiligheid en fraude, en de uitdagingen die deze verschillen met zich meebrengen voor het vormgeven van effectief beleid. Deze kadering biedt een fundament voor het verdere onderzoek en helpt om de relevantie van het onderwerp te duiden.

1.2.1. Definitie kennisveiligheid

In dit onderzoek volgen we de definitie van kennisveiligheid zoals geformuleerd in de Leidraad Kennisveiligheid, waarin onderscheid wordt gemaakt naar drie verschijningsvormen:

> 1. De ongewenste overdracht van sensitieve kennis en technologie die van invloed kan zijn op de nationale veiligheid en/of de wetenschappelijke positie van instellingen.

> 2. Kwaadwillige invloed op onderzoek en onderwijs, waarbij kennis door of vanuit andere landen en statelijke actoren kan worden ingezet om onder meer desinformatie te verspreiden of studenten en onderzoekers aan te zetten tot zelfcensuur, waardoor inbreuk wordt gemaakt op de academische vrijheid en de integriteit van onderzoek en onderwijs in Nederland.
>
> 3. Ethische of integriteitsschendingen, waarbij kennis en technologie door statelijke actoren worden gebruikt om Nederlandse en Europese waarden en geldende verdragen te schenden of te ondermijnen.[34]

Het is belangrijk te onderkennen dat landen en instellingen verschillende visies en definities hanteren rond kennisveiligheid. Hetzelfde geldt voor fraude. Deze verschillen komen niet alleen voort uit uiteenlopende administratieve tradities en institutionele structuren, maar ook uit het feit dat landen verschillende typen risico's en motieven willen beheersen. Waar in het ene land de nadruk ligt op onderzoeksintegriteit en transparantie, ligt in het andere land de focus op kennisveiligheid, in het Engels vaak aangeduid als *research security*, en het voorkomen van ongewenste kennisoverdracht.

1.2.2. Strategische belangen

Uit het *Dreigingsbeeld Statelijke Actoren 2025* komt naar voren welke belangen op het spel staan. Nederland en de EU dreigen op steeds meer technologische terreinen achterop te raken. Dit brengt risico's met zich mee voor zowel de nationale veiligheid als de economie. Economische machtsconcentraties ontstaan bij landen die succesvol nieuwe technologieën ontwikkelen, wat het verdienvermogen van Nederland kan schaden en tot strategische afhankelijkheden kan leiden. Wanneer landen zelf niet beschikken over de kennis en technologie die nodig zijn voor hun geopolitieke ambities, zoeken ze daar actief naar in het buitenland.[35]

In het dreigingsbeeld komt naar voren dat door sancties getroffen statelijke actoren naar andere manieren zoeken om technologische kennis te verkrijgen, waarbij zij vaker gebruikmaken van heimelijke methoden.[36] Als andere landen via dergelijke verwerving toegang krijgen tot dezelfde technologische kennis als Nederland, kan dit op termijn leiden tot een verlies van de Nederlandse voorsprong in bepaalde technologische sectoren en het structureel verzwakken van het concurrentievermogen van Nederlandse bedrijven. Daarnaast kan het ertoe leiden dat andere landen militair sterker worden, waardoor de effectiviteit van de Nederlandse krijgsmacht kan afnemen.[37] Kennis en technologie uit het Westen kan namelijk worden ingezet voor het ontwikkelen van wapensystemen. Daarnaast kan verworven kennis worden ingezet voor spionagecapaciteiten, of voor surveillanceapparatuur waarmee mensenrechten onder druk worden gezet. Door de groeiende rol van kennis en technologie als geopolitieke machtsmiddelen en door de wereldwijde technologische wedloop, is het waarschijnlijk dat deze dreiging de komende jaren aanhoudt of zelfs toeneemt. Op de middellange termijn bestaat het risico dat kennisinstellingen hun strategische voorsprong verliezen.[38]

---

[34] Rijksoverheid (2022, p 9).

[35] NCTV (2025).

[36] NCTV (2025).

[37] NCTV (2025).

[38] NCTV (2025).

De risico's en belangen die op het spel staan verschillen per land en context. Sommige landen richten zich vooral op het beschermen van hun wetenschappelijke positie, andere op het voorkomen van ongewenste militaire toepassingen door andere landen of het waarborgen van academische vrijheid. Dit beïnvloedt welke risico's prioriteit krijgen en hoe beleid wordt vormgegeven. De verschillen worden onder meer bepaald door factoren als geografische ligging, de omvang van de economie, de mate van integratie in de wereldeconomie en het geldende juridische systeem.

1.2.3. Belangrijkste dreigingsvectoren

In dreigingsanalyses worden diverse methodes genoemd die statelijke actoren gebruiken om toegang te krijgen tot hoogwaardige technologie en kennis, zowel in de academische als private sector. Zo wordt er gebruik gemaakt van geavanceerde cyberaanvallen.[39] Andere methodes zijn ondoorzichtige investeringen die staatsbemoeienis verhullen, of het omzeilen van exportrestricties.[40] Ook worden bijvoorbeeld Westerse wetenschappers en werknemers van hoogtechnologische bedrijven gerekruteerd, of kunnen gezamenlijke publicaties, talentrekrutering, beursverstrekkingen en internationale fora gebruikt worden om toegang te krijgen tot technologie en kennis.[41]

Ongewenste kennis- en technologieoverdracht via personen wordt ook wel *insider threat* genoemd. Hierbij gaat de dreiging uit van onderzoekers, andere medewerkers of studenten die werkzaam zijn (geweest) bij Nederlandse kennisinstellingen. Statelijke actoren kunnen op verschillende manieren gebruik maken van de insider threat. Zo zetten ze heimelijke middelen in, zoals digitale en fysieke spionage. Ook gebruiken ze legitieme activiteiten zoals internationale uitwisselingen waarbij ze wel heimelijke intenties hebben. Soms gaat het om academische samenwerking die in beginsel geen heimelijke intenties heeft, maar waarvan de opgedane kennis op een later moment door een statelijke actor wordt verworven voor ongewenste doeleinden wordt ingezet.[42] Het onderscheid tussen wanneer er wel of geen sprake is van heimelijke intenties is in de praktijk lastig te maken. Statelijke actoren kunnen onderzoekers en studenten aansturen of onder druk zetten om informatie te delen, bijvoorbeeld in ruil voor financiering of een stageplaats. Soms zijn zij zelfs wettelijk verplicht om mee te werken met een statelijke actor. Daarbij wordt niet altijd openheid gegeven over nevenactiviteiten of verplichtingen richting andere kennisinstellingen of statelijke actoren.[43]

Screening van inkomende onderzoekers en studenten richt zich op dergelijke kennis- en technologieoverdracht via personen. Dit onderzoek richt zich specifiek op hoe identiteits- en documentfraude in deze context worden gebruikt, maar erkent dat het bredere dreigingsbeeld complexer is.

1.2.4. Modus operandi

Verschillende vormen van identiteits- en documentfraude kunnen bijdrage aan deze dreigingen. Zo kan er sprake zijn van verborgen financieringsbronnen, niet-gemelde affiliaties, selectieve openbaarmaking van onderzoeksactiviteiten en een verkeerde voorstelling van institutionele banden.

---

[39] AIVD (2024).

[40] NCTV (2025).

[41] NCTV (2025).

[42] Internetconsultatie.nl (2025).

[43] Internetconsultatie.nl (2025).

Hieraan gekoppeld gaat eerder RAND-onderzoek in op het belang van transparantie en informatieverstrekking. Mogelijke indicatoren van gebrekkige transparantie of achtergehouden informatie die we tegenkwamen zijn:[44]

- Onderzoekers of instellingen verstrekken onvolledige of inconsistente informatie over banden, waaronder onderzoekspartners, financieringsbronnen, verplichtingen en andere relevante relaties, of hebben een geschiedenis van dergelijke praktijken.
- Onderzoekers weigeren informatie te verstrekken over eindgebruikers of eindgebruik, of onderzoekers gebruiken vertragingstactieken om het beantwoorden van vragen te vermijden.
- Onderzoekers gebruiken historische institutionele namen, acroniemen of aliassen waarin defensiebanden worden weggelaten of verhuld om due-diligence-inspanningen te omzeilen.
- In openbare bronnen (zoals websites, publicaties en gepubliceerde cv's) staan inconsistente affiliaties of worden bekende partnerschappen weggelaten, waardoor het moeilijk is om de werkelijke institutionele banden of verplichtingen van een medewerker te verifiëren.
- Een medewerker wordt gevraagd een geheimhoudingsovereenkomst of een non-disclosure agreement te ondertekenen voordat affiliaties, rollen, onderzoeksdoelen en financieringsbronnen worden onthuld. Hoewel dit een maatregel ter bescherming van intellectueel eigendom lijkt, kan het soms worden gebruikt om de ware aard of intentie van het onderzoek te verbergen.
- Discrepanties tussen publieke en interne presentaties (bijvoorbeeld meerdere versies van websites), waaronder discrepanties tussen informatie in de moedertaal en verstrekte informatie.
- Overdreven gescripte of ontwijkende berichten over onderzoeksdoelen, met name wanneer alle medewerkers identieke praatpunten herhalen of vermijden om mogelijke toepassingen te bespreken.
- Het cv van een medewerker wijst op overkwalificatie of onderkwalificatie voor het project, of vaardigheden komen niet overeen met opgegeven kwalificaties.
- Een derde partij financiert het onderzoek om identificatie van de eindgebruiker te voorkomen.
- Er worden verzoeken gedaan om institutionele compliance-, ethische of exportcontrole-beoordelingen te omzeilen of te vermijden.
- De website van een partner is opzettelijk niet toegankelijk in het rechtsgebied, wat due-diligence-inspanningen bemoeilijkt.[45]

Het gebruik maken van een andere naam of het weglaten van bepaalde affiliaties is een bekend probleem bij aanmeldingen vanuit China, waar reeds in 2018 over gepubliceerd is door Joske (2018). Voorbeelden die Joske aanhaalt zijn onder andere aanmeldingen vanuit de National University of Defense Technology (NUDT) die de naam Changsha Institute of Technology gebruiken om te voorkomen dat een visumaanvraag wordt afgewezen. Het Changsha Institute of Technology was een instelling van het PLA die

[44] Pernin et al. (2026).

[45] Pernin et al. (2026).

in 1975 door de NUDT werd opgenomen. Ook het achterhouden van informatie wordt hierin aangehaald. De NUDT adviseert in een document voor studenten die in het buitenland willen studeren, dat bij het indienen van documentatie in hun aanmeldingen bij buitenlandse instellingen 'militaire en politieke vakken kunnen worden weggelaten' uit hun academische dossiers.[46]

Er zijn diverse hulpmiddelen en databronnen beschikbaar die inzicht bieden in mogelijke, tijdens een aanmelding verzwegen, affiliaties met statelijke actoren of het defensieapparaat. Zo is er de ASPI-tracker van het Australian Strategic Policy Institute die defensielinks van Chinese universiteiten in kaart brengt. Ook RAND Europe heeft een tracker uitgebracht van kennisinstellingen binnen de Chinese Academy of Sciences.[47] Hierin worden de volgende indicatoren gebruikt om defensielinks in kaart te brengen:

- Leden van het management van de entiteit hebben tevens een adviesfunctie op defensiegebied.
- Laboratoria, onderzoekers of projecten van de entiteit hebben onderscheidingen ontvangen voor werk dat de militaire capaciteiten van China of andere belangrijke nationale defensiebelangen bevordert.
- Het werk van onderzoekers van de entiteit wordt momenteel gefinancierd door Chinese defensieorganisaties.
- De entiteit huisvest laboratoria die deel uitmaken van het Chinese onderzoeksnetwerk voor defensielaboratoria.
- Onderzoekers van de entiteit hebben wettelijke rechten op een patent voor een uitvinding of innovatie die specifiek bedoeld is voor militaire of defensietoepassingen.
- Onderzoekers van de entiteit hebben samen met personen van Chinese defensieorganisaties publicaties op hun naam staan.[48]

1.2.5. Internationale verschillen in benadering van kennisveiligheid en fraude

Zoals hierboven beschreven, hanteren landen en instellingen uiteenlopende visies en definities rond kennisveiligheid, fraude en integriteit. Dit komt niet alleen door verschillen in administratieve tradities en structuren, maar ook doordat landen verschillende risico's en motieven willen beheersen. Waar het ene land vooral inzet op onderzoeksintegriteit en transparantie, ligt elders de nadruk op kennisveiligheid en het voorkomen van ongewenste kennisoverdracht. Dit resulteert in uiteenlopend beleid, verschillende interpretaties van wat als fraude of risicovol gedrag wordt gezien, en daarmee ook in een ander beeld van de frequentie en aard van incidenten. In de casestudies wordt hier verder op ingegaan.

Het begrip fraude is in deze context bovendien breed en kent veel grijstinten. Het spectrum loopt van opzettelijke misleiding en spionage tot situaties waarin onderzoekers of studenten, uit anticipatie op strenge screening of door onduidelijkheid over meldplichten, informatie achterhouden. Soms is het voor een onderzoeker zelfs onmogelijk om zich volledig te distantiëren van defensiegerelateerde instellingen, of zijn

[46] Joske (2018).

[47] Chinese Academy of Sciences Directory (2026).

[48] Chinese Academy of Sciences Directory (2026). Een uitgebreide onderbouwing van de risicoindicatoren is hier te vinden: https://www.rand.org/pubs/tools/TLA4687-1/tool/user-guide.html

er wettelijke verplichtingen, ook als de intenties van een individu goed zijn. Deze uiteenlopende beweegredenen en contexten vragen om een genuanceerde beoordeling en een passende beleidsreactie.

1.3. Doelstelling en onderzoeksvragen

Kennisveiligheid in zijn huidige hoedanigheid is een relatief jong beleidsveld. Verdiepend onderzoek wordt nodig geacht om tot een steviger onderbouwd beleid te komen. Lessen uit de praktijk over de inzet van identiteits- en documentatiefraude om toegang te krijgen tot sensitieve technologie en kennis, kunnen inzichten opleveren voor het ontwikkelen van een uitvoerbaar en efficiënt screeningsproces. Op aanvraag van het ministerie van OCW heeft het WODC daarom aan RAND Europe gevraagd om in kaart te brengen hoe de screening is georganiseerd in Nederland en andere landen, en in hoeverre hierbij in de praktijk identiteits- en documentfraude gesignaleerd worden. Het doel van dit onderzoek is om bij te dragen aan het terugdringen van de risico's op het gebied van kennisveiligheid. De volgende onderzoeksvragen staan centraal:

1. Wat is bekend over de wijze waarop identiteits- en documentatiefraude wordt gepleegd om toegang te krijgen tot kennisinstellingen in Nederland en daarbuiten?
2. In hoeverre is er een beeld van de frequentie waarin deze fraude plaatsvindt in Nederland en daarbuiten?
3. Welke waarborgen kunnen worden gecreëerd om de verschillende manieren waarop fraude wordt gepleegd tegen te gaan?

In lijn met de Nationale Leidraad Kennisveiligheid uit 2022 (hierna: Leidraad Kennisveiligheid of Leidraad), opgesteld door de Rijksoverheid in samenwerking met verschillende partijen uit het kennis- en onderwijsveld, richten we ons bij kennisveiligheid voornamelijk op de ongewenste overdracht van sensitieve kennis en technologie binnen het hoger onderwijs en de wetenschap.[49]

1.4. Methodologie

Dit onderzoek bestaat uit een literatuuronderzoek (paragraaf 1.4.1) en casestudies (paragraaf 1.4.2). Voor de casestudies werden data verzameld door middel van bureauonderzoek en interviews met experts die beschikken over relevante kennis op het gebied van kennisveiligheid, identiteitscontrole en documentverificatie in hun land. Ook is tijdens dit onderzoek verkend of open-source-intelligence-onderzoek gebruikt zou kunnen worden om tot geaggregeerde inzichten te komen over risicoindicatoren voor identiteits- en documentfraude en zo de waarborgen beter te kunnen toespitsen. Uiteindelijk is omwille van privacyoverwegingen besloten om hiervan af te zien, omdat de data ook informatie over individuen zouden bevatten.

[49] Rijksoverheid (2022).

1.4.1. Literatuuronderzoek

We zijn dit onderzoek begonnen met het verzamelen en inventariseren van beschikbare literatuur. Het doel hiervan was vast te stellen in hoeverre de onderzoeksvragen konden worden beantwoord op basis van bestaande literatuur over de wijze waarop en de frequentie waarmee identiteits- en documentatiefraude worden gepleegd.

Zoekstrategie

Het onderzoeksteam doorzocht meerdere (academische) zoekmachines en databases met behulp van diverse zoekopdrachten waaronder Google en Google Scholar. Gehanteerde zoektermen zijn:

- **Nederlands:** "kennisveiligheid" OR "verantwoorde internationalisering" OR "onderzoeksintegriteit" AND ("beleid" OR "screening" OR "fraude" OR "identiteitsfraude" OR "documentfraude" OR "diplomafraude" OR "toelatingsprocedure" OR "verificatie van documenten" OR "verificatie van identiteit" OR "achtergrondonderzoek" OR "toelatingsbeleid" OR "risicobeoordeling" OR "risico-indicatoren").
- **Engels:** "research security" OR "responsible internationalisation" OR "research integrity" AND ("policy" OR "screening" OR "fraud" OR "identity fraud" OR "document fraud" OR "diploma fraud" OR "admission procedure" OR "document verification" OR "identity verification" OR "background check" OR "admission policy" OR "risk assessment" OR "risk indicators").

Dit werd gedaan om de beperkte middelen gericht in te zetten en de belangrijkste bronnen te selecteren. Het onderzoek richtte zich op academische bronnen in het Nederlands en Engels. Bij de bronselectie werd gezocht naar *peer-reviewed* tijdschriftpublicaties (inclusief systematische en niet-systematische literatuuroverzichten), beleidsrapporten van overheden, ngo's of onafhankelijke onderzoeksorganisaties, proefschriften, beleidsdocumenten, wetgeving, redactionele artikelen en opiniestukken. Expliciet uitgesloten werden scripties, documenten zonder duidelijk individueel of organisatorisch auteurschap, video's en podcasts. Er werden geen beperkingen gesteld aan de publicatiedatum. Bronnen werden als relevant gezien als ze ingingen op beleid en procedures ten behoeve van kennisveiligheid, om van daaruit zoveel mogelijk informatie te vergaren over specifieke screeningsprocedures en het daaruit voortkomende beeld van fraude. Aanvullend is gebruikgemaakt van snowballing, waarbij relevante bronnen en referenties die in reeds geselecteerde literatuur werden genoemd, verder zijn gevolgd en beoordeeld op bruikbaarheid voor het onderzoek.

1.4.2. Casestudies

Om niet alleen inzichten op te doen over de Nederlandse situatie, zijn casestudies uitgevoerd voor drie andere landen. Door goed te kijken naar wat andere landen doen, kan de situatie in Nederland in perspectief geplaatst worden, zelfs als directe cijfers ontbreken. Daarnaast was het doel om lessen te trekken uit de manier waarop andere landen waarborgen hebben ingebouwd.

Inventarisatie en selectiecriteria

De selectie is gemaakt op basis van een lange lijst van landen:

- Waarvan bekend is dat zij vergelijkbare zorgen hebben rond kennisveiligheid;

- Waarmee Nederland reeds samenwerkt; en
- Die tezamen verschillende juridische, sociale, organisatorische en beleidscontexten rondom screening en fraudebestrijding vertegenwoordigen.

Daarbij zijn ook pragmatische overwegingen meegenomen als:

- De beschikbaarheid van relevante wet- en regelgeving, of documentatie over beleidsmaatregelen gericht op het screenen van studenten en medewerkers in relatie tot toegang tot sensitieve kennis en technologie;
- De beschikbaarheid van informatie over de frequentie en aard van fraudegevallen binnen kennisinstellingen; en
- De mogelijkheid tot het voeren van interviews met experts, met inachtneming van privacy- en veiligheidsbeperkingen.

Selectie

In overleg met de begeleidingscommissie voor dit onderzoek, werden naast Nederland, uiteindelijk Australië, Duitsland en Zweden geselecteerd als casestudies. Uit het in paragraaf 1.4.1 genoemde literatuuronderzoek bleek namelijk dat voor deze drie landen indicaties te vinden waren over de frequentie en aard van fraudegevallen. Voor alle drie zijn cijfers over het aantal incidenten helaas niet openbaar, maar dat gold voor alle landen die zijn overwogen. De drie geselecteerde landen scoorden relatief goed op de hierboven genoemde selectiecriteria en pragmatische overwegingen. Daarnaast kwamen uit het literatuuronderzoek de in Tabel 1 opgenomen inhoudelijke bevindingen naar voren die aanknopingspunten bieden voor mogelijke lessen.

Tabel 1. Eerste bevindingen die meespeelden in de selectie van casestudies

Casestudieland	Bevindingen
Australië	Australië wordt als interessante casus gezien vanwege de in 2024 aangescherpte kennisveiligheidsprocessen, de visa condition 8202 van 2022 en het bestaan van een Counter Foreign Interference Coordination Centre (CFICC).
Duitsland	Ook in Duitsland worden de regels momenteel aangescherpt. Sinds 2024 zet het Federaal Ministerie van Onderzoek, Technologie en Ruimtevaart (Bundesministeriums für Forschung, Technologie und Raumfahrt, BMFTR) expliciet in op een risicogestuurde, proportionele aanpak van kennisveiligheid.
Zweden	In Zweden publiceert de Inspectie van Strategische Producten (ISP) vanuit de overheid toegankelijke uitleg en hulpmiddelen voor kennisveiligheid die instellingen helpen om risico's in internationale samenwerking te beoordelen en te mitigeren. Daarnaast publiceert de veiligheidsdienst Säpo jaarlijks over trends op het gebied van kennisveiligheid en documentatiefraude. Ook heeft het land sinds 2023 een FDI-wet die voorschrijft dat investeringen met mogelijke implicaties voor kennisinstellingen gescreend moeten worden. Ten slotte heeft Zweden sinds 2024 richtlijnen over verantwoorde internationalisatie gepubliceerd.

Het Verenigd Koninkrijk (VK) en Frankrijk werden eveneens overwogen als casestudies, maar in samenspraak met de begeleidingscommissie is besloten deze landen niet te selecteren, omdat de aanvrager

van het onderzoek al had aangegeven een goed beeld te hebben van het beleid en de screeningsmechanismen in deze landen. Niettemin werden in de interviews enkele inzichten opgedaan over de gehanteerde aanpak in deze twee landen. Om die mee te nemen in deze analyse en rapportage, zijn ze opgenomen in een apart hoofdstuk na de casestudies (Hoofdstuk 6).

Bureauonderzoek

Voor elk van de vier casestudies zijn de beschikbare bronnen onderzocht, waaronder academische literatuur, grijze literatuur, mediaberichtgeving en, waar beschikbaar, dossiers van rechtszaken of aanklachten. De bronnen werden geselecteerd door middel van een combinatie van open zoekopdrachten, snowballing bij citaten en vragen die tijdens de interviews met deskundigen zijn gesteld. De zoektermen die hiervoor zijn gebruikt komen overeen met de zoektermen in de paragraaf Zoekstrategie (1.3.1), gecombineerd met de naam van het betreffende land. Hierbij is ook gezocht in de taal van het betreffende land. Deze aanpak maakte het mogelijk om snel de belangrijkste nationale beleidskaders en initiatieven te identificeren, die doorgaans prominent zichtbaar zijn in zoekresultaten. De relevantie van bronnen is vervolgens bepaald op basis van de mate waarin zij concrete informatie boden over beleid, procedures, actoren of instrumenten gerelateerd aan kennisveiligheid en (toelatings)screening. Zodra een eerste set kernbronnen was vastgesteld, werd veelvuldig gebruikgemaakt van sneeuwbalmethoden. Deze documenten verwezen vaak onderling naar elkaar en brachten zo aanvullende beleidsstukken, rapporten en sleutelactoren aan het licht. Dataverzameling werd als verzadigd beschouwd op het moment dat nieuwe zoekopdrachten en referentienetwerken voornamelijk reeds geïdentificeerde bronnen en initiatieven opleverden en nauwelijks nog nieuwe typen informatie toevoegden. Dit punt werd bereikt na het analyseren van een beperkte, maar inhoudelijk consistente set bronnen. Op basis van deze bronnen hebben we voor iedere casestudie zoveel mogelijk de informatie over de volgende aspecten uitgewerkt:

1. **Kennisveiligheid**: onder andere wat betekent kennisveiligheid in dit land en welke maatschappelijke of politieke zorgen (zoals spionage of buitenlandse inmenging) staan hierbij op de voorgrond?
2. **Beleid en wetgeving**: onder andere welke nationale of lokale regels en beleidsdoelen (bijvoorbeeld een screeningswet) reguleren toegang tot kennisinstellingen en wat wordt daarmee beoogd? Deze waren eenvoudig te achterhalen via online zoekopdrachten en dienden als een toegankelijk uitgangspunt voor het in kaart brengen van zowel procedures als verantwoordelijke autoriteiten.
3. **Toelatings- en screeningsprocedures**: onder andere wanneer en hoe worden personeel en studenten gescreend en gelden er strengere controles bij gevoelige vakgebieden? Deze informatie werd voornamelijk gevonden via openbare bronnen, maar interviews met deskundigen hielpen bij het verduidelijken van belangrijke details rond specifieke mechanismen
4. **Verantwoordelijke instanties**: onder andere welke overheidspartijen en instellingen zijn betrokken bij toezicht, uitvoering en handhaving van deze regels?
5. **Identiteits- en documentfraude**: onder andere welke methoden van fraude (zoals valse diploma's) komen voor en zijn deze anders per herkomstland of vakgebied?

6. **Omvang en monitoring**: onder andere zijn er data over de frequentie van fraude, hoe wordt dit gemonitord, en zijn er aanwijzingen voor onderrapportage? Deze gegevens waren niet openbaar beschikbaar en zijn in dit onderzoek volledig gebaseerd op interviews met deskundigen.
7. **Maatregelen en samenwerking**: onder andere welke waarborgen worden ingezet tegen fraude, zijn er internationale samenwerkingen, en welke best practices en zwakke plekken zijn er bekend?

De geïdentificeerde literatuur bood met name informatie over algemene beleidskaders en institutionele inrichting (aspecten 1-4) en was veelal afkomstig van overheidswebsites en beleidsdocumenten. Gedetailleerde informatie over specifieke frauderisico's en operationele indicatoren (aspecten 5-7) bleef schaars. Academische publicaties richtten zich doorgaans op afgebakende deelonderwerpen en minder op fraudevraagstukken als zodanig, terwijl (internationale) overzichtsstudies relatief waardevol bleken vanwege hun vergelijkende perspectief.

Interviews

Interviews met vertegenwoordigers van organisaties die betrokken zijn bij of kennis hebben van het screenen van onderzoekers en studenten, werden vervolgens gebruikt om hiaten in de beschikbare documentatie aan te vullen. Het ging daarbij in alle vier de landen voornamelijk om de laatste drie aspecten in bovenstaande opsomming, waarbij de eerdere aspecten kort aan bod kwamen om het onderzoek in de juiste context te plaatsen. Het interviewprotocol ging in op de volgende topics, waarbij het protocol indien nodig werd aangepast naar aanleiding van de specifieke organisatie en rol:

1. **Rol en context:** De geïnterviewde beschrijft zijn/haar rol en verantwoordelijkheden bij de toelating of screening van buitenlandse studenten of onderzoekers.
2. **Huidige processen:** Er wordt gevraagd hoe de organisatie de identiteit en authenticiteit van documenten (zoals paspoorten, visa, diploma's) controleert.
3. **Samenwerking en databronnen:** De samenwerking met nationale/internationale partners en het gebruik van gedeelde databases of externe bronnen voor verificatie komt aan bod.

   Soorten en frequentie van fraude: Er wordt geïnventariseerd welke vormen van identiteits- of documentfraude voorkomen en hoe vaak deze worden gesignaleerd.
4. **Detectie, registratie en trends:** De systematische registratie en analyse van fraudegevallen, en eventuele trends of patronen worden besproken.
5. **Opvallende gevallen en methoden:** Concrete (anonieme) voorbeelden van ontdekte fraude en de gebruikte detectiemethoden worden gevraagd.
6. **Staatsactoren en veiligheidsrisico's:** Er wordt nagegaan of er gevallen zijn van georganiseerde of door staten gesteunde pogingen om via fraude toegang te krijgen tot gevoelige kennis.
7. **Uitdagingen en knelpunten:** De belangrijkste uitdagingen en beperkingen bij het voorkomen of opsporen van fraude worden besproken (technisch, juridisch, organisatorisch, internationaal).
8. **Internationale vergelijking en leren:** Er wordt gevraagd naar best practices of relevante tools uit andere landen.
9. **Verbeterbehoeften:** De geïnterviewde reflecteert op mogelijke aanvullende maatregelen, middelen of beleidswijzigingen om fraude beter te kunnen voorkomen en detecteren.

In totaal werden vijftien interviews gehouden, zoals te zien in Tabel 2.

Tabel 2. Lijst met geïnterviewden

Land	Organisatie
Nederland	Expertisecentrum Identiteitsfraude en Documenten (ECID), Koninklijke Marechaussee
	Loket Kennisveiligheid, Rijksdienst voor Ondernemend Nederland (RVO)
	TU Delft
	Justis
	Ministerie van Onderwijs, Cultuur en Wetenschap
	Nuffic
Australië	Southern Cross University
	University of New South Wales (UNSW)
	Anoniem
Duitsland	Anoniem
	Anoniem
Zweden	Inspectie van Strategische Producten (Inspektionen för Strategiska Produkter, ISP)
	Zweedse Onderzoeksraad (Vetenskapsrådet, VR)
	Zweedse Raad voor Hoger Onderwijs (Universitets- och Högskolerådet, UHR)
	Koninklijke Technische Hogeschool (Kungliga Tekniska Högskolan, KTH)

De aantekeningen die tijdens de interviews werden gemaakt, zijn verwerkt in de analyse. Waar de interviews gebruikt zijn als bronvermelding, zijn deze willekeurig genummerd.

Voor de Duitse casestudie heeft de persvoorlichtingsdienst van het Federaal Ministerie voor Onderzoek, Technologie en Ruimte (BMFTR) op onze vragen schriftelijke input geleverd die eveneens de casestudie verder heeft geïnformeerd.

Ten slotte merken we op dat het verkrijgen van toegang tot de juiste betrokkenen niet eenvoudig was. Kennisveiligheid is een gevoelig onderwerp, waarover overheden bewust niet alles prijs willen geven. In Nederland en Zweden werd niettemin over het algemeen positief gereageerd op onze verzoeken. In Australië en met name Duitsland was dat echter niet het geval. Daar werd ofwel terughoudender gereageerd, dan wel met de boodschap dat de beoogde interviewkandidaten geen expertise hadden op dit onderwerp. Vooral dat laatste baarde opzien, aangezien wij ons specifiek richtten op de instanties die ogenschijnlijk het meest bekend zijn met het beleid op het gebied van kennisveiligheid en relevante screeningsprocedures in dat land.

1.5. Beperkingen

Dit onderzoek kent een aantal beperkingen:

1. Kennisveiligheid, en met name de wijze waarop de kennissector beschermd wordt, is een gevoelig onderwerp. Overheden houden de kaarten dicht tegen de borst. Immers, een publiek rapport als dit kan ook gelezen worden door personen of statelijke actoren die screening proberen te

omzeilen of te misleiden. Het is dan niet gewenst dat zij exact weten wanneer, door wie, waarop gescreend wordt. In dit onderzoek is duidelijk geworden dat belanghebbenden om deze reden vaak niet bereid zijn om dieper op procedures in te gaan. In enkele gevallen is dergelijke informatie wel in vertrouwen gedeeld, maar werd daarbij gevraagd deze niet op te nemen in de rapportage.

2. De interviews zijn hoofdzakelijk ingezet om informatie op te halen bij vertegenwoordigers van organisaties die identiteit en relevante documenten valideren en personen uit andere landen screenen. Ondanks dat ook enkele experts zijn geconsulteerd die niet direct betrokken of verantwoordelijk zijn voor screeningsprocessen, is het waarschijnlijk dat kritische tegengeluiden ondervertegenwoordigd zijn in dit onderzoek. Dit is een belangrijke beperking, omdat de effectiviteit van processen niet altijd duidelijk is, en uitbreiding van screening vaak gepaard gaat met zorgen over inbreuk op privacy en discriminatie. Hoewel de opgehaalde data te beperkt zijn om harde conclusies te trekken over de gevolgen van oppervlakkige dan wel rigide screening, is het relevant dit punt te benoemen. In de internationale literatuur en in enkele interviews wordt namelijk gewezen op het risico dat te oppervlakkige screening leidt tot onvoldoende risicobeheersing, terwijl te rigide of generieke screening kan leiden tot uitsluiting van onschuldige kandidaten, aantasting van academische vrijheid en internationale samenwerking, of zelfs discriminatie. Het rapport onderstreept daarom het belang van een proportionele, contextgevoelige aanpak en van het investeren in kennis en expertise bij de uitvoerende partijen.

1.6. Leeswijzer

Dit rapport vervolgt met **Hoofdstuk 2** over Nederland: hierin beschrijven we het beleid, de wettelijke kaders en procedures rondom kennisveiligheid, inclusief toelatings- en screeningsprocessen, en de aanpak van document- en identiteitsfraude. Daarna volgen de internationale casestudies: achtereenvolgens Australië (**Hoofdstuk 3**), Duitsland (**Hoofdstuk 4**) en Zweden (**Hoofdstuk 5**). In Hoofdstuk 6 gaan we in op de situatie in het Verenigd Koninkrijk en Frankrijk. Het rapport eindigt met **Hoofdstuk 7** met daarin een conclusie en de belangrijkste lessen uit de casestudies voor het versterken van kennisveiligheid in Nederland.

2. Nederland

2.1. Kennisveiligheid: algemene context

De Leidraad Kennisveiligheid, opgesteld door de Rijksoverheid in samenwerking met verschillende partijen uit het kennis- en onderwijsveld, beschrijft de Nederlandse opvatting van kennisveiligheid als volgt:

> Bij kennisveiligheid gaat het allereerst om ongewenste overdracht van sensitieve kennis en technologie. Overdracht is ongewenst als deze de nationale veiligheid van ons land aantast. Daarnaast gaat kennisveiligheid om heimelijke beïnvloeding van onderwijs en onderzoek door statelijke actoren. Deze inmenging brengt de academische vrijheid en de sociale veiligheid in gevaar. Tot slot gaat het om ethische kwesties die kunnen spelen in de samenwerking met landen die de grondrechten niet respecteren.[50]

Er worden dus drie kwesties specifiek uitgelicht: **ongewenste kennisoverdracht**, **inmenging** en **ethiek en integriteit**, waarbij de nadruk duidelijk ligt op de eerste kwestie. Deze afbakening vormt het kader waarop het Nederlandse kennisveiligheidsbeleid is gebaseerd.

Kader 2. Belangrijkste actoren in het Nederlandse ecosysteem voor kennisveiligheid

Overheidsactoren

De Rijksoverheid (onder andere de ministeries van OCW, JenV en EZK) is verantwoordelijk voor het ontwikkelen van beleidskaders en wetgeving, zoals de Leidraad Kennisveiligheid en het wetsvoorstel Wet screening kennisveiligheid. De overheid waarborgt samenhang in beleid en voert de uiteindelijke screening (beoogd via Justis) uit voor toegang tot sensitieve technologie.

De Immigratie- en Naturalisatiedienst (IND) beoordeelt visumaanvragen en fungeert als extra controlelaag voor niet-EU-studenten en -onderzoekers. Universiteiten treden hierbij op als erkend referent.

Inlichtingen- en veiligheidsdiensten (AIVD, MIVD) en NCTV leveren dreigingsanalyses en ondersteunen beleidsvorming rond kennisveiligheid, met een focus op statelijke actoren en geopolitieke risico's.

Koninklijke Marechaussee (KMar) en dienst Expertisecentrum Identiteitsfraude en Documenten (ECID) controleren identiteitsdocumenten, met name aan de grens. Zij spelen momenteel een beperkte rol richting kennisinstellingen.

Het Loket Kennisveiligheid fungeert als centraal adviespunt voor kennisinstellingen bij vragen over risico's rondom internationale samenwerking. Het biedt risicobeoordelingen, maar heeft geen toegang tot persoonsgegevens en kan geen bindende besluiten nemen.

Justis is een screeningsautoriteit die de betrouwbaarheid van personen en organisaties beoordeelt ter bevordering van een veilige en rechtvaardige samenleving en is de beoogd uitvoerder van de screening onder de screeningswet om persoonsgebonden risicoanalyses uit te voeren.

Nuffic adviseert instellingen over buitenlandse diploma's en controleert deze op authenticiteit en consistentie.

[50] Rijksoverheid (2022).

Het advies is niet bindend en richt zich primair op onderwijsdocumenten, niet op identiteitsverificatie.

Kennisinstellingen en -organisaties

Kennisinstellingen, bekostigde en niet-bekostigde instellingen zoals bedoeld in de WHW (universiteiten, hogescholen, academische ziekenhuizen), instellingen voor toegepast onderzoek (TO2-instellingen[51]), Koninklijke Nederlandse Academie van Wetenschappen (KNAW), en NWO(-I)- en andere instituten waar zich sensitieve technologie bevindt.[52] Deze organisaties dragen de primaire verantwoordelijkheid voor de dagelijkse uitvoering van kennisveiligheid, waaronder toelating, screening en documentverificatie van studenten en onderzoekers. De uitvoering verschilt echter sterk per instelling, waardoor het systeem fragmentarisch is.

Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) speelt als belangrijkste nationale onderzoeksfinancier een rol in het borgen van kennisveiligheid binnen gefinancierd onderzoek. NWO was in 2022 betrokken bij de ontwikkeling van de Leidraad Kennisveiligheid en werkt aan de implementatie van kennisveiligheidsmaatregelen in haar beoordelingsprocessen en eigen instituten. Als financier kan NWO kennisveiligheid meewegen in subsidieprocessen en internationale samenwerking, zonder zelf als screeningsautoriteit op te treden.

2.2. Beleid en wetgeving

2.2.1. Leidraad Kennisveiligheid

De Leidraad Kennisveiligheid positioneert kennisveiligheid nadrukkelijk als een gedeelde verantwoordelijkheid van meerdere actoren binnen het Nederlandse kennis- en beleidslandschap. Kennisinstellingen, zoals universiteiten en onderzoeksinstituten, dragen een primaire verantwoordelijkheid voor het herkennen en beheersen van risico's binnen onderwijs, onderzoek en internationale samenwerking. Van hen wordt verwacht dat zij passende interne procedures inrichten voor partnerselectie, screening en toezicht op kennisdeling. Tegelijkertijd ligt bij de Rijksoverheid – en in het bijzonder bij ministeries met een portefeuille voor onderwijs, wetenschap, economie en veiligheid – de verantwoordelijkheid om kaders, bewustwording en beleidsmatige samenhang te bieden. Financieringsorganisaties en uitvoeringsinstanties, zoals onderzoeksfinanciers, spelen daarbij een aanvullende rol door kennisveiligheid mee te wegen in subsidieverstrekking en toezicht, zonder de academische autonomie volledig te ondergraven.

De Leidraad Kennisveiligheid wijst expliciet op kwetsbaarheden in besluitvormings- en controleprocessen, waaronder risico's van documentfraude en misrepresentatie. Bestuurders en beleidsverantwoordelijken binnen kennisinstellingen worden aangesproken op hun rol in het beoordelen van de betrouwbaarheid van aangeleverde documentatie, zoals academische kwalificaties, samenwerkingsvoorstellen en verklaringen van herkomst en financiering. De Leidraad benadrukt dat documentfraude niet louter een administratief probleem is, maar een potentiële katalysator voor bredere kennisveiligheidsrisico's, doordat zij toegang kan verschaffen tot gevoelige kennis, infrastructuur of netwerken. In beleidsanalyses fungeert de Leidraad daarmee als een analytisch raamwerk dat uitnodigt tot een proportionele, risicogebaseerde benadering, waarin verantwoordelijkheden helder zijn verdeeld tussen instellingen, financiers en overheid. Veiligheid

[51] TO2-instellingen zijn de vijf Nederlandse topinstituten voor toegepast onderzoek: Deltares, MARIN, NLR, TNO en Wageningen Research (WR). Onder toezicht van het ministerie van Economische Zaken zetten ze wetenschappelijke kennis om in innovatieve impact voor overheid en bedrijfsleven.

[52] Blom et al. (2025, 6).

wordt zo structureel meegenomen in strategische besluitvorming op nationaal niveau. In juli 2026 is een nieuwe versie van de Nationale leidraad kennisveiligheid verschenen.[53]

2.2.2. Voorstel Wet screening kennisveiligheid

Een wetsvoorstel van het kabinet-Schoof voor een Wet screening kennisveiligheid werd in april 2025 ter consultatie gepubliceerd.[54] Met dit wetsvoorstel zou een screeningsprocedure worden geïntroduceerd voor personen die toegang willen tot delen van Nederlandse kennisinstellingen waar zij in aanraking kunnen komen met gevoelige technologie. Het doel was om te voorkomen dat ongewenste kennis en technologie via onderzoekers, studenten of technisch personeel werd overgedragen, en om zo de risico's voor de nationale veiligheid te verkleinen.[55] In het regeerakkoord van het kabinet-Jetten is vervolgens opgenomen dat er een screeningswet kennisveiligheid zou komen "die mogelijk maakt dat we waar nodig onderzoekers en PhD-studenten van buiten de Europese Unie die met onze kennis werken kunnen screenen".[56]

Tijdens de consultatiefase van het wetsvoorstel uitten meerdere partijen vanuit het kennis- en onderzoeksveld – waaronder de TO2-federatie van topinstellingen en de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW) – zorgen over de effectiviteit, uitvoerbaarheid en proportionaliteit van de wet zoals voorgesteld.[57] Zaken zoals het uitwijken van talent naar andere landen met een soepeler beleid en de administratieve lasten die de screening met zich mee zou brengen, worden als grote problemen voor de uitvoerbaarheid gezien.[58] Ook de lijst met sensitieve technologieën wordt als niet adequaat geacht, deze 'loopt namelijk altijd achter de feiten aan, waardoor schijnveiligheid ontstaat'.[59] In juni 2026 heeft het kabinet daarom besloten dat het wetsvoorstel uit 2025 niet haalbaar is en werd een haalbaarheidsanalyse naar een screening kennisveiligheid in aangepaste, meer beperkte en gerichtere vorm aangekondigd.[60] Aangezien nog niet duidelijk is een aangepaste screening haalbaar is en welke vorm deze dan zou krijgen, worden hieronder de doelen en werking van de screeningsprocedure zoals deze uiteengezet zijn in het oorspronkelijke wetsvoorstel kort besproken. Het voorstel uit 2025 vormt ten slotte de aanleiding voor dit onderzoek.

Beleidsdoelen wetsvoorstel screening kennisveiligheid

De beleidsdoelen van het wetsvoorstel screening kennisveiligheid moeten in de eerste plaats worden gezien tegen de achtergrond van een verscherpt dreigingsbeeld, waarin statelijke actoren actief proberen hoogwaardige kennis en technologie uit Nederland te verwerven. Uit dreigingsanalyses van onder meer AIVD, MIVD en NCTV blijkt dat Nederlandse kennisinstellingen hierbij een aantrekkelijk doelwit

[53] Loket Kennisveiligheid (2026).

[54] Internetconsultatie.nl (2025).

[55] Internetconsultatie.nl (2025).

[56] D66, VVD & CDA (2026).

[57] Internetconsultatie.nl (2025); Minister van Onderwijs, Cultuur en Wetenschap 2026 [31288-1260]; KNAW (2025); TO2-Federatie (2025).

[58] KNAW (2025); TO2-Federatie (2025).

[59] KNAW (2025).

[60] Minister van Onderwijs, Cultuur en Wetenschap 2026 [31288-1260].

vormen, mede vanwege hun sterke internationale positie.[61] In deze context is het primaire beleidsdoel het waarborgen van de nationale veiligheid door ongewenste kennis- en technologieoverdracht te voorkomen of te mitigeren.[62] Dit raakt direct aan bredere doelstellingen zoals het beschermen van de strategische autonomie en economische weerbaarheid van Nederland en de EU, evenals het voorkomen van afhankelijkheden die geopolitiek kunnen worden uitgebuit. Tegelijkertijd speelt de integriteit van het kennis- en innovatiesysteem een centrale rol: het gaat om het behouden van een veilige onderzoeksomgeving waarin wetenschappelijke samenwerking mogelijk blijft zonder dat ze wordt misbruikt voor bijvoorbeeld militaire toepassingen, spionage of digitale aanvallen.

Daarnaast omvatten de beleidsdoelen expliciet het realiseren van een evenwicht tussen veiligheid en openheid, wat nauw samenhangt met internationale reputatie en naleving van internationale verplichtingen. Nederland positioneert zich traditioneel als een open kennisland dat internationale samenwerking stimuleert; het beleid beoogt deze openheid te behouden, terwijl tegelijkertijd proportionele maatregelen worden genomen om risico's te beheersen. Dit vertaalt zich in doelstellingen zoals het beschermen van academische vrijheid, het faciliteren van veilige internationale samenwerking en het waarborgen van rechtstatelijke principes zoals non-discriminatie en een zorgvuldige belangenafweging bij screening. Tegelijk sluit het voorstel aan bij bestaande internationale kaders, waaronder EU-sanctieregelgeving en exportcontrole, en draagt het bij aan bredere EU-doelen rond economische veiligheid en kennisbescherming. Daarmee bestrijkt het beleid een geïntegreerd palet aan doelen: van veiligheidsbelangen zoals security en compliance tot andere cruciale dimensies zoals wetenschappelijke integriteit, internationale geloofwaardigheid en het toekomstige innovatievermogen van Nederland.

Werking wetsvoorstel screening kennisveiligheid

Het wetsvoorstel is nadrukkelijk ontworpen als een preventief instrument. De screening vindt plaats vóór toegang wordt verleend tot zogenoemde hoogrisico-onderdelen van kennisinstellingen waar gewerkt wordt met sensitieve technologie. Hieronder vallen onder meer kunstmatige intelligentie, kwantumtechnologie, halfgeleiders, biotechnologie en cyberbeveiliging, die door hun brede toepasbaarheid en mogelijke militaire of strategische inzet van groot belang zijn voor de nationale veiligheid.

De screeningsplicht geldt voor iedereen die onderzoek wil doen, onderwijs wil verzorgen of wil studeren in een omgeving waar toegang tot deze sensitieve technologie mogelijk is. Hiermee beoogt de wetgever een non-discriminatoire en risicogerichte aanpak, waarbij niet de herkomst van de persoon centraal staat, maar de potentiële risico's die samenhangen met toegang tot kritieke kennis en technologie.

De screening wordt uitgevoerd door de Rijksoverheid en bestaat uit een brede risicobeoordeling. Daarbij wordt onder meer gekeken naar mogelijke banden met statelijke actoren, relevante gedragingen en antecedenten en risico's die voortvloeien uit internationale sanctieregimes. Ook wordt beoordeeld of toegang kan leiden tot ongewenste kennisoverdracht of het ontstaan van strategische afhankelijkheden die de nationale veiligheid onder druk kunnen zetten. Het resultaat van de screening is een besluit waarin wordt vastgesteld of er wel of geen bezwaar bestaat tegen toegang tot de betreffende technologie. De

[61] NCTV (2025).

[62] Internetconsultatie.nl (2025).

screeningsautoriteit Justis is in het voorstel de beoogde uitvoerder van de screening en heeft een uitvoeringstoets op dit wetsvoorstel verricht.[63]

Een belangrijk uitgangspunt van het wetsvoorstel is het principe 'open waar mogelijk, beschermen waar nodig'. Het voorstel beoogt nadrukkelijk niet om internationale samenwerking of academische vrijheid onnodig te beperken, maar om deze juist duurzaam te beschermen door risico's gericht te mitigeren. Screening wordt daarom alleen toegepast in situaties waar de risico's voor de nationale veiligheid het grootst worden geacht.

Daarnaast speelt de kennissector zelf een actieve rol in de uitvoering. Kennisinstellingen zijn verantwoordelijk voor het identificeren en aanwijzen van de onderdelen waar sensitieve technologie aanwezig is en waar de screeningsplicht dus geldt. Hierdoor wordt aangesloten bij de expertise van instellingen zelf en kan de maatregel flexibel en toekomstbestendig worden toegepast, bijvoorbeeld wanneer nieuwe technologieën of dreigingen ontstaan.

Tot slot moet het wetsvoorstel worden gezien als het sluitstuk van een bredere beleidsaanpak rond kennisveiligheid, waarin ook instrumenten zoals het Loket Kennisveiligheid, exportcontrolemaatregelen en sanctieregelgeving een rol spelen. De screening richt zich specifiek op het adresseren van persoonsgebonden risico's die met bestaande instrumenten moeilijk effectief en uniform te beheersen zijn.

Deze beleidsontwikkeling laat zien dat kennisveiligheid in Nederland steeds explicieter als beleidskwestie aangekaart wordt en er gezocht wordt naar een institutioneel verankerde oplossing. Tegelijkertijd maakt ze zichtbaar hoe lastig het is om brede beleidsdoelen zoals nationale veiligheid, open wetenschap en non-discriminatie te vertalen naar een uitvoerbare en consistente screeningspraktijk.

2.2.3. Spanningsveld tussen kennisveiligheid en academische vrijheid

Een belangrijk knelpunt binnen het kennisveiligheidsbeleid is het spanningsveld tussen nationale veiligheid en academische vrijheid. Universiteiten hebben zich in dit debat kritisch opgesteld, onder meer in hun reactie op het voorstel voor de screeningswet, getiteld Zware lasten, schijn van veiligheid.[64] Hierin benadrukken zij dat vergaande screeningsmaatregelen een aanzienlijke administratieve druk met zich meebrengen, terwijl het effect van een daadwerkelijke risicoreductie volgens hen beperkt kan zijn. In interviews met betrokkenen komt ook naar voren dat academische vrijheid als kernwaarde van de academische wereld wordt gezien en niet onnodig mag worden ingeperkt.[65]

Tegelijkertijd wordt erkend dat er duidelijke gevallen zijn waarin screening noodzakelijk is, bijvoorbeeld bij samenwerking met gesanctioneerde instellingen of bij onderzoek binnen gevoelige domeinen zoals rakettechnologie of nucleaire kennis, waar dankzij sanctieregelingen internationale kennisembargo's gelden. In dergelijke situaties bestaat er weinig discussie over de noodzaak van strikte maatregelen. Het grootste vraagstuk bevindt zich echter in het grijze gebied daartussen: samenwerkingen die niet expliciet verboden zijn, maar wel risico's kunnen bevatten.[66] Dit geldt bijvoorbeeld voor samenwerking met instellingen in

[63] RAND Europe Interview – 10.

[64] Universiteiten van Nederland (2025).

[65] RAND Europe interviews – 2, 4 & 15.

[66] RAND Europe interview – 15.

landen als China, waar enerzijds strategische zorgen spelen en anderzijds vaak sprake is van wederzijds waardevolle kennisuitwisseling, soms zelfs op een niveau waarop buitenlandse partners al verder ontwikkeld zijn. Het beoordelen van deze grijze zone vraagt om zorgvuldige afwegingen, waarbij zowel veiligheidsrisico's als het belang van een open wetenschap serieus worden meegewogen.

2.3. Screeningsprocedures

Dit hoofdstuk beschrijft de huidige screeningsprocedures voor studenten en medewerkers (waaronder onderzoekers en wetenschappers) die toegang verkrijgen tot Nederlandse kennisinstellingen. De analyse is gebaseerd op vooronderzoek van Blom et al. (2025) dat ingaat op bestaand beleid en praktijk rond identificatie, authenticatie en documentcontrole, zoals dat wordt toegepast door kennisinstellingen en betrokken overheidsorganisaties in Nederland. Daarbij wordt ingegaan op de momenten waarop screening plaatsvindt, de mate van differentiatie voor sensitieve domeinen, de verdeling van verantwoordelijkheden tussen het nationale en institutionele niveau, en de gebruikte middelen en methoden. Deze screeningsprocedures hebben betrekking op screening van studenten en onderzoekers bij kennisinstellingen.

Formeel gemandateerde screeningsprocedures voor werknemers in kennisintensieve bedrijven bestaan momenteel niet. Een verkenning van het ministerie van Economische zaken kwam tot de conclusie dat screeningsplicht voor alle sensitieve technologiebedrijven 'niet opportuun' werd geacht omdat 'dit niet voldoende effectief, uitvoerbaar en proportioneel' zou zijn door de omvang van de doelgroep, kosten en eventuele neveneffecten.[67] Het kabinet heeft dan ook besloten af te zien van deze optie.[68] Voor vragen over veiligheid rondom onderwerpen als human resources-beleid, insider risk, exportcontrole en dual-use-goederen kunnen bedrijven met kennisintensieve producten of diensten wel gebruik maken van de expertise van het Ondernemersloket Economische Veiligheid (OLEV) van de Rijksdienst voor Ondernemend Nederland.[69]

2.3.1. Algemene opzet screening en toelatingsprocedures

De screening van personen binnen het hoger onderwijs en onderzoeksdomein is geen uniforme of centraal georganiseerde procedure, maar bestaat uit een keten van deels overlappende controles die op verschillende momenten in het toelatings- en aanstellingsproces plaatsvinden. Deze keten strekt zich uit van de eerste aanmelding of sollicitatie tot en met de start bij de kennisinstelling. Een deel van dit proces wordt uitgevoerd door kennisinstellingen zelf, terwijl een ander deel uitgevoerd wordt door centrale overheidsinstanties volgens een gestandaardiseerd proces.

Een belangrijk onderscheid bestaat tussen studenten en medewerkers. Studenten doorlopen in beginsel een formeel, gestandaardiseerd toelatingsproces, terwijl bij wetenschappers en onderzoekers meer sprake is van decentrale en informele werving en selectie. Daarnaast verschillen procedures aanzienlijk naar nationaliteit; met name voor derdelanders (niet-EU/EER) zijn extra juridische en administratieve stappen vereist. Deze

[67] Ministerie van Economische Zaken (2026).

[68] Delta (2026).

[69] Rijksdienst voor Ondernemend Nederland (2026).

verschillen zitten met name in de visum- en/of verblijfsvergunningprocedures die studenten of wetenschappers als beoogd werknemers doorlopen.

Deze gefaseerde inrichting creëert meerdere controlemomenten, maar betekent ook dat geen enkele actor een volledig beeld heeft van de kandidaat of van het totale risicoprofiel. De effectiviteit van het systeem hangt daardoor niet alleen af van afzonderlijke controles, maar ook van de mate waarin deze elkaar in de praktijk aanvullen.

2.3.2. Screening van studenten

Voor studenten start het proces met een aanmelding via Studielink. Hierbij worden persoonsgegevens vastgelegd en, afhankelijk van de herkomst van de student, digitale identificatiemiddelen gebruikt. Nederlandse en EU-studenten maken gebruik van DigiD of eIDAS, terwijl studenten van buiten de EU doorgaans een scan of foto van hun paspoort uploaden. De gebruikte software leest persoonsgegevens uit deze documenten, maar verricht in dit stadium geen diepgaande authenticatie of identiteitsverificatie.

Na aanmelding volgt het toelatingsproces bij de kennisinstelling zelf. Dit proces bestaat doorgaans uit drie fasen. In de eerste fase vindt de waardering van diploma's en vooropleidingen plaats, veelal met ondersteuning van Nuffic. In de tweede fase beoordelen faculteiten of opleidingscommissies de inhoudelijke geschiktheid van de kandidaat, op basis van kwalificaties, cijfers, motivatie en eventueel referenties. Deze beoordeling is primair gericht op academische kwaliteit en omvat doorgaans geen controle op de echtheid van documenten. In de laatste fase vindt, afhankelijk van de instelling, verificatie van documenten plaats. De mate en diepgang hiervan verschillen sterk: sommige instellingen verifiëren alle academische documenten, andere doen dit alleen steekproefsgewijs of bij studenten uit zogenoemde aandachtslanden.

Sommige universiteiten geven ook aan studenten te screenen in de fasen van hun studie waarbij zij in aanraking kunnen komen met onderzoek en kennis die als sensitief worden beschouwd.[70] Dit kan onderzoek zijn waarvan de innovatiewaarde zeer hoog ligt of dat betrekking heeft of bestaande sensitieve technologieën.

Voor niet-EU-studenten vormt de verblijfsvergunningprocedure een extra screeningsmoment. Kennisinstellingen treden hierbij op als erkend referent en dienen namens de student de aanvraag in bij de Immigratie- en Naturalisatiedienst (IND). In dit kader worden identiteitsdocumenten en aanvullende bewijsstukken gecontroleerd. Pas na verkrijging van de verblijfsvergunning kan de student definitief worden ingeschreven en naar Nederland reizen.

2.3.3. Screening van onderzoekers

De screening van wetenschappers en onderzoekers kent volgens Blom et al. (2025) een ander karakter. Werving en selectie vinden grotendeels decentraal plaats, vaak binnen bestaande academische netwerken. Sollicitatiegesprekken vormen het kerninstrument om de geschiktheid van kandidaten te beoordelen. De nadruk ligt hierbij op inhoudelijke expertise en reputatie, waarbij veel vertrouwen wordt gesteld in vakinhoudelijke beoordeling door *peers*.

[70] RAND Europe interview – 15.

Juist in deze informelere context ontstaat een belangrijke kwetsbaarheid: waar sterk wordt vertrouwd op reputatie, referenties en academische netwerken, blijft structurele verificatie van documenten en achtergrondinformatie vaak beperkt. Daardoor is het systeem mogelijk minder goed toegerust om misrepresentatie, weglatingen of contextuele risico's tijdig te signaleren.

Formele verificatie van diploma's, cv's en referenties vindt tijdens de sollicitatiefase slechts sporadisch plaats, meestal alleen bij twijfel.[71] Identiteitsdocumenten worden doorgaans pas in een later stadium gecontroleerd, met name tijdens de onboarding. Sommige instellingen maken hierbij gebruik van commerciële pre-employment-screeningdiensten, afhankelijk van functie en senioriteit.[72] Deze screenings kunnen bestaan uit een controle van identiteitsbewijzen, diploma's, referenties en eventueel een Verklaring Omtrent Gedrag (VOG).

Universiteiten delen onderling kennis over gemanipuleerde cv's door informatie uit te wisselen over de karakteristieken van deze cv's.[73] Vanwege privacyredenen worden deze cv's of de kenmerken ervan volledig geanonimiseerd en vervolgens gedeeld binnen netwerken van universiteiten om zo een beter beeld te creëren van mogelijke frauduleuze kenmerken en kennisveiligheid in de sector te verbeteren.

Ook voor onderzoekers van buiten de EU geldt dat een verblijfsvergunning vereist is. De IND-procedure fungeert hiermee als een aanvullende nationale controlelaag. Instellingen geven aan in belangrijke mate te steunen op deze externe waarborg voor identiteitsverificatie. De kennisinstelling heeft als erkend referent naast een zorgplicht ook een administratie- en bewaarplicht, zoals voor de kopie van het paspoort van de student, de antecedentenverklaring en het bewijs van voldoende middelen om in Nederland te wonen en te studeren. Sommige instellingen maken voor dit verblijfsvergunningproces en -administratie ook wel gebruik van commerciële diensten.

2.3.4. Momenten van identiteits- en documentcontrole

Identiteits- en documentcontroles vinden verspreid plaats over het gehele traject. Belangrijke momenten zijn de aanmelding (aanleveren en uitlezen van identiteitsgegevens), de toelatings- of selectieprocedure (beperkte documentverificatie), de verblijfsvergunning- en visumprocedure (formele identiteits- en documentcontrole), de grenspassage (controle door de Koninklijke Marechaussee), de inschrijving in de Basisregistratie Personen (BRP) bij de gemeente, en tot slot de start bij de kennisinstelling waar de wettelijke identificatieplicht voor werkgevers geldt.

Deze gefaseerde aanpak betekent dat geen enkel moment op zichzelf als allesomvattende screening fungeert; in plaats daarvan is sprake van cumulatieve waarborgen, uitgevoerd door verschillende actoren.

2.3.5. Verdeling van verantwoordelijkheden

De huidige screeningsprocedures zijn deels nationaal vastgelegd en deels institutioneel ingericht. Nationale wet- en regelgeving bepaalt onder meer de verblijfsrechtelijke controle, grensbewaking, BRP-inschrijving en de identificatieplicht voor werkgevers. Kennisinstellingen zijn verantwoordelijk voor werving, toelating, selectie en een belangrijk deel van de documentverificatie. Dit leidt tot variatie in uitvoering en diepgang

[71] Blom et al. (2025).

[72] RAND Europe interview – 15.

[73] RAND Europe interview – 15.

tussen instellingen. De Nederlandse screeningspraktijk laat daarmee een bredere spanning zien tussen instellingsautonomie en uniforme risicobeheersing. De decentrale inrichting biedt ruimte voor maatwerk, maar leidt ook tot verschillen in capaciteit, prioritering en diepgang van controles tussen instellingen.

2.3.6. Gebruikte middelen en methoden

Voor screening en verificatie wordt gebruikgemaakt van een combinatie van digitale tools, commerciële diensten en handmatige controles. Voorbeelden zijn software voor het uitlezen van identiteitsdocumenten, diplomawaardering via Nuffic en internationale netwerken, commerciële pre-employment-screeningsplatforms, en specialistische expertise bij overheidsinstanties zoals Bureau Documenten en het Expertisecentrum Identiteitsfraude en Documenten (ECID). Fysieke identificatie, met name bij grenscontrole en indiensttreding, blijft een essentieel onderdeel van het systeem.

2.4. Document- en identiteitsfraude

Zoals eerder aangegeven, bestaat de screening van personen binnen het hoger onderwijs en onderzoeksdomein niet uit één uniforme of centraal georganiseerde procedure. In plaats daarvan is sprake van een reeks deels overlappende controles die op verschillende momenten tijdens het toelatings- en aanstellingsproces plaatsvinden. Door deze gefaseerde aanpak is er geen enkel moment waarop een volledige screening plaatsvindt; de waarborgen stapelen zich juist op en worden uitgevoerd door verschillende betrokken partijen. Kennisinstellingen zijn verantwoordelijk voor de werving, toelating, selectie en een groot deel van de documentverificatie. Deze fragmentatie zorgt voor verschillen in de uitvoering en grondigheid van de screening tussen de diverse instellingen.

Informatie over fraude wordt dan ook niet centraal geregistreerd of geanalyseerd, en verschillende actoren in deze gefaseerde aanpak zijn slechts in staat om een deel van het fraudebeeld te schetsen. Dit betekent dat het ontbreken van een centrale registratie niet alleen een informatieprobleem is, maar ook een analytische beperking vormt voor beleid en toezicht. Zonder een gedeeld inzicht in patronen, frequentie en terugkerende kwetsbaarheden blijft het lastig om gerichte waarborgen te ontwikkelen of de effectiviteit van bestaande maatregelen te beoordelen.

2.4.1. Loket Kennisveiligheid – algemene vragen en informatie

Het Loket Kennisveiligheid (ook: Loket) fungeert als centraal aanspreekpunt voor kennisinstellingen met vragen over kennisveiligheid. Het Loket beantwoordt de vragen en voert analyses uit met behulp van risicoprofielen om potentiële risico's te signaleren en instellingen te ondersteunen bij hun risicobeoordeling. In deze rol treedt het Loket op als frontoffice, terwijl de interdepartementale afstemming plaatsvindt in de backoffice. Het Loket heeft een adviserende functie en kan geen bindende besluiten nemen.[74]

De vragen die het Loket ontvangt, gaan bijvoorbeeld over het aannemen van gastonderzoekers of PhD-studenten. Daarbij ligt het risico vaak niet bij de persoon zelf, maar bij de organisatie waaraan de gastonderzoeker verbonden is. Zo kan het voorkomen dat een gastonderzoeker afkomstig is van een instelling met militaire connecties, waardoor de kennisinstelling hulp nodig heeft bij het inschatten van de

[74] RAND Europe Interview – 4.

risico's. Controle op identiteits- of documentfraude behoort echter niet tot het takenpakket van het Loket, en het beschikt hiervoor dan ook slechts over beperkte middelen. Daarnaast worden meldingen geanonimiseerd gedaan en ontvangt het Loket geen persoonsgegevens. De focus ligt daarom vooral op de achtergrond van de entiteit, niet op het individu. Vragen over fraude komen slechts sporadisch binnen.[75] Ook bij het ECID van de Koninklijke Marechaussee komen geen vragen over fraude binnen vanuit universiteiten of andere organisaties in de kennissector.[76]

Het Kennisloket hoort wel regelmatig van kennisinstellingen dat informatie over bijvoorbeeld defensiegerelateerde banden soms bewust wordt weggelaten uit cv's. Dit gebeurt mede door de toegenomen aandacht voor kennisveiligheid en het groeiende bewustzijn bij kennisinstellingen van de risico's die bepaalde connecties met zich meebrengen. Waar dergelijke banden voorheen als prestigieus werden gezien, zijn instellingen zich nu meer bewust van de mogelijke risico's en de rol van statelijke actoren. Het achterhouden van dergelijke informatie is een bekende werkwijze, maar het Loket is niet verantwoordelijk voor de controle hierop; wel geeft het hierover voorlichting.[77] Dit suggereert bovendien dat de voornaamste kwetsbaarheid niet noodzakelijk ligt in klassieke vervalsing van documenten, maar in strategische misrepresentatie en omissies. Dergelijke vormen van fraude zijn moeilijker te detecteren met traditionele documentcontrole en vragen om een bredere, contextuele risicobeoordeling.

Wanneer kennisinstellingen vragen hebben over fraude, of wanneer het Loket zelf een acuut risico signaleert, adviseert het de instelling contact op te nemen met de relevante veiligheidsdiensten. Het Loket verwijst in principe niet door naar Nuffic of de IND. Voor kennisinstellingen is het vaak lastig om fraude te herkennen op basis van een cv. Ook komt het voor dat de IND een positief signaal afgeeft over een verblijfsvergunning terwijl het Loket een negatief advies uitbrengt over de risico's die samenhangen met een samenwerking. Omdat het beoordelen van fraude niet tot het mandaat van het Loket behoort, kan het geen uitspraken doen over de omvang ervan.[78]

2.4.2. Nuffic – controle van diploma's en onderwijsdocumenten

Nuffic adviseert Nederlandse kennisinstellingen over de waardering van buitenlandse diploma's. Op verzoek van een instelling beoordeelt Nuffic of een buitenlands diploma gelijkwaardig is aan een Nederlands diploma en geeft hierover een advies. Dit advies is niet bindend; de uiteindelijke toelatingsbeslissing ligt bij de kennisinstelling zelf. Jaarlijks verstrekt Nuffic ongeveer 30.000 adviezen, waarvan 17.000 aan kennisinstellingen, de overige 13.000 vertrekt ze aan anders klanten zoals ministeries en bevoegde autoriteiten. Hoewel het aanvragen van een advies niet verplicht is, kiezen veel instellingen hier wel voor, bijvoorbeeld omdat dit in hun onderwijs- en examenreglementen is vastgelegd of bij twijfel over de toelaatbaarheid van een student.[79]

Bij de beoordeling controleert Nuffic of het diploma is erkend door de bevoegde autoriteit in het land van herkomst. Daarnaast worden bijbehorende documenten zoals cijferlijsten beoordeeld. Door te kijken of het

[75] RAND Europe Interview – 4.

[76] RAND Europe Interview – 13.

[77] RAND Europe Interview – 4.

[78] RAND Europe Interview – 4.

[79] RAND Europe Interview – 8.

gehele opleidingstraject logisch en consistent is verlopen, kan Nuffic mogelijke fraude opsporen. De controle vindt doorgaans plaats op basis van kopieën, omdat buitenlandse studenten zich vaak nog niet in Nederland bevinden en geen originele documenten kunnen overleggen. Nuffic beschikt echter wel over de expertise om originele documenten te beoordelen wanneer deze beschikbaar zijn.[80]

Nuffic richt zich primair op onderwijsdocumenten en niet op identiteitsbewijzen. Indien identiteitsdocumenten toch worden meegestuurd, wordt slechts globaal gecontroleerd op bijvoorbeeld leeftijd en naam en altijd in relatie tot de onderwijsloopbaan. De persoonsidentificatie behoort tot de verantwoordelijkheid van de kennisinstelling.[81]

Nuffic signaleert dat fraude met diploma's vaker voorkomt uit bepaalde landen, maar onderzoekt niet expliciet of er een link is met kennisveiligheid. Fraude wordt opgespoord door te letten op inconsistenties in documenten of onlogische onderwijsloopbanen. Daarnaast zijn er de bekende diploma mills waar valse diploma's kunnen worden gekocht. Informatie hierover wordt gedeeld binnen het internationale netwerk van Nuffic, waardoor deze gevallen snel kunnen worden herkend en aangepakt.[82]

Indien Nuffic twijfels heeft over de echtheid van documenten, wordt dit teruggekoppeld aan de kennisinstelling. Nuffic doet zelf geen aangifte van fraude en neemt geen formele besluiten. Wanneer Nuffic een trend signaleert, bijvoorbeeld als meerdere aanvragers dezelfde (onlogische) onderwijsroute hebben gevolgd en gebruik maken van dezelfde tussenpersonen, kan hiervan melding worden gemaakt bij relevante instanties, zoals de veiligheidsdiensten. Hierbij wordt steeds een afweging gemaakt tussen privacy en veiligheid.[83]

Voor onderzoekers, zoals promovendi van buiten de Europese Unie, verloopt de procedure anders. In deze gevallen is het niet verplicht om diploma's door Nuffic te laten waarderen. De kennisinstelling beoordeelt zelf of het niveau van de kandidaat voldoende is voor toelating. Er vindt doorgaans geen controle op de authenticiteit van diploma's plaats; de academische wereld vertrouwt hierbij op referenties en netwerken.[84]

2.4.3. IND – visa en immigratiedocumenten

Bij de aanvraag van een visum via de IND hoeft de kennisinstelling als erkende referent alleen een kopie van het paspoort en een eigen verklaring toe te voegen aan het dossier.[85] De formele beoordeling van en beslissing op aanvragen blijft bij de IND. Het systeem gaat daarbij uit van een vertrouwensrelatie tussen de overheid en de kennisinstelling als erkende referent, waarbij controles door de IND mede op basis van signalen en achteraf steekproefsgewijs plaatsvinden. Dit systeem is gebaseerd op het moderne migratiebeleid (wet MoMi), waarbij universiteiten en hogescholen als erkende referenten optreden en een belangrijke verantwoordelijkheid dragen voor het indienen en onderbouwen van aanvragen.[86] In de praktijk hebben medewerkers die het immigratieproces begeleiden, vaak nauw contact met de kennisveiligheidscoördinator

[80] RAND Europe Interview – 8.

[81] RAND Europe Interview – 8.

[82] RAND Europe Interview – 8.

[83] RAND Europe Interview – 8.

[84] RAND Europe Interview – 8.

[85] RAND Europe Interview – 8.

[86] Lodder (2019).

binnen de instelling. Technische universiteiten beschikken doorgaans over meer expertise op dit gebied dan andere instellingen. Ook vinden er onderling overleg en kennisdeling plaats tussen kennisveiligheidscoördinatoren van verschillende universiteiten.[87]

2.4.4. Koninklijke Marechaussee – controle aan de grens

De Koninklijke Marechaussee (KMar) heeft een gespecialiseerde afdeling voor de controle van reis- en identiteitsdocumenten: het Expertisecentrum Identiteitsfraude en Documenten (ECID). Hier zijn specialisten aanwezig die de echtheid van documenten kunnen controleren. Het expertisecentrum heeft naast documentenexperts op de luchthaven Schiphol ook experts werken op diverse locaties in Nederland (de zogenaamde ID-desks). Andere instellingen kunnen het expertisecentrum benaderen voor de controle op echtheid van eerdergenoemde documenten als zij deze zelf niet kunnen beoordelen. Diverse overheidsorganisaties, bijvoorbeeld politie en gemeentes, maar ook financiële instellingen zoals banken, laten bij twijfel over echtheid de identiteitsdocumenten van klanten controleren door de experts van het expertisecentrum. Ze leggen volgens de KMar regelmatig documenten voor aan het expertisecentrum ter controle. Van kennisinstellingen heeft het ECID tot op heden nog geen vragen of documenten ter controle ontvangen.[88]

2.5. Bevindingen en conclusies

In de Nederlandse context wordt kennisveiligheid opgevat als het voorkomen van ongewenste overdracht van sensitieve kennis en technologie die de nationale veiligheid kan schaden, het tegengaan van heimelijke beïnvloeding van onderwijs en onderzoek door statelijke actoren en het adresseren van ethische vraagstukken in internationale samenwerking. Deze brede benadering vormt het kader waarbinnen beleid, wetgeving en uitvoeringspraktijk zijn vormgegeven. Enerzijds is sprake van een doordacht systeem, waarin verschillende actoren en instrumenten gezamenlijk bijdragen aan de bescherming van kennis en technologie. Anderzijds laat de praktische uitvoering ook duidelijke beperkingen en kwetsbaarheden zien, met name op het gebied van informatievoorziening en verificatieprocessen.

De Nederlandse aanpak kan worden gekarakteriseerd als een gelaagd, maar gefragmenteerd systeem: er bestaan verschillende relevante controles en gespecialiseerde organisaties, maar deze zijn niet ingebed in één integraal screenings- en registratiekader. Daardoor hangt de effectiviteit van het systeem sterk af van afstemming tussen actoren, institutionele capaciteit en het vermogen om signalen uit verschillende processtappen samen te brengen.

Beleid en procedures

Breed begrip en zelfregulatie: De Nederlandse kennisorganisaties zijn voor een groot deel zelf verantwoordelijk voor kennisveiligheid in hun organisaties. Het meest recente sectorbeeld laat zien dat de meerderheid van de Nederlandse instellingen op alle thema's van de Leidraad Kennisveiligheid beleid

[87] RAND Europe Interview – 8.

[88] RAND Europe Interview – 13.

hebben geïmplementeerd.[89] Daarnaast laat het sectorbeeld zien dat de sector brede vooruitgang heeft geboekt ten opzichte van vorige sectorbeelden. Dit geeft aan dat het belang van kennisveiligheid begrepen wordt door kennisinstellingen en dat hiernaar gehandeld wordt.

Bestaande specialisaties: Het centraal georganiseerde Loket Kennisveiligheid heeft veel expertise weten op te bouwen, bijvoorbeeld over het inschatten van risico's bij partnerkennisinstellingen. Nuffic is van oudsher gespecialiseerd in het controleren van documenten en het controleren op fraude hiermee. Kennisinstellingen weten deze organisaties goed te vinden en schakelen hen regelmatig in wanneer zij hulp nodig denken te hebben.

Gelaagde controleketen: Controles vinden op meerdere momenten in het toelatings- en aanstellingsproces plaatsvinden. Studenten en onderzoekers kunnen in verschillende fasen te maken krijgen met documentcontrole, diplomawaardering, visum- en verblijfsprocedures, grenscontrole en identificatie bij inschrijving of indiensttreding. Hoewel deze controles niet als één geïntegreerd systeem zijn ontworpen, creëren zij gezamenlijk wel een reeks waarborgen die bepaalde vormen van identiteits- en documentfraude kunnen helpen signaleren.

Bestaande beperkingen

Beperkte en gefragmenteerde verificatie van documenten: Een belangrijke beperking van de Nederlandse aanpak ligt in de beperkte en gefragmenteerde verificatie van documenten. De kennisinstellingen zijn grotendeels zelf verantwoordelijk. Instanties zoals Nuffic en het Loket Kennisveiligheid hebben slechts een adviserende rol, waardoor zij niet structureel betrokken zijn. Indien Nuffic betrokken wordt voor diplomaverificatie worden haar beoordelingen regelmatig gebaseerd op kopieën van documenten in plaats van originelen, wat de betrouwbaarheid van verificatie verkleint. Onder de Wet modern migratiebeleid zijn kennisinstellingen erkende referenten, waardoor controle bij visa-aanvragen door de overheid grotendeels ontbreekt. Deze variatie in diepgang en aanpak leidt ertoe dat het systeem kwetsbaar blijft voor documentfraude en misrepresentatie. Daarmee ontstaat een risico dat personen op basis van onjuiste of onvolledige informatie toegang krijgen tot kennis, infrastructuur of netwerken, wat de effectiviteit van het bredere kennisveiligheidsbeleid ondermijnt.

Beperkte kennisdeling: Het huidige systeem is versnipperd en er vindt geen structurele kennisdeling plaats. Instanties zoals Nuffic en Bureau Documenten van de KMar zijn gericht op formele onjuistheden in documenten van individuen, waarbij de link naar kennisveiligheid vaak niet expliciet gelegd wordt. Vertegenwoordigers van instanties zijn in dit onderzoek in staat geweest om een breder beeld te geven van fraude, maar dit beeld koppelen aan kennisveiligheid is lastig, omdat dit niet systematisch wordt geanalyseerd. Het Loket Kennisveiligheid richt zich op risicoindicatoren van de partnerinstelling. Vanuit kennisinstellingen horen zij dat strategische misrepresentatie, zoals het weglaten van relevante affiliaties, regelmatig voorkomt. Kennisinstellingen delen onderling ook geanonimiseerde kenmerken van verdachte documenten. De verantwoordelijkheid voor een integrale screening van zowel individuele als institutionele risicofactoren ligt echter bij de kennisinstellingen zelf.

Beperkte capaciteit kennisinstellingen: Om een integrale screening goed te kunnen uitvoeren zijn contextuele duiding, landenkennis en inhoudelijke expertise van belang. Juist op dit punt ontstaan

[89] De Boer et al. (2026).

kwetsbaarheden, omdat deze expertise niet overal in gelijke mate beschikbaar is. Binnen sommige kennisinstellingen ontbreekt het aan de gespecialiseerde expertise om grondige verificaties uit te voeren, zeker gezien de internationale en vaak complexe aard van documenten en loopbanen. Hierdoor blijft controle op cv's, nevenfuncties en institutionele affiliaties vaak oppervlakkig en afhankelijk van individuele inschattingen. Het creëert een kwetsbaarheid, waarbij persoonsgebonden risico's onvoldoende systematisch worden geïdentificeerd en beheerst.

3. Australië

3.1. Kennisveiligheid: algemene context

In plaats van de term kennisveiligheid te gebruiken, hanteerde Australië aanvankelijk het bredere concept van 'het tegengaan van buitenlandse inmenging' (*countering foreign influence* ofwel CFI).[90] Deze term heeft betrekking op een breder spectrum van kwetsbaarheden. Naast het hoger onderwijs en onderzoek benadrukt het Australische ministerie van Binnenlandse Zaken (DHA) de toepasbaarheid van CFI ook op gemeenschappen in de samenleving, democratische instellingen, het bedrijfsleven en de media.[91] Ondanks de bredere reikwijdte van de term CFI kent Australië een reeks aan betrokken actoren en heeft het meerdere beleidsmaatregelen geïmplementeerd die zich richten op wat kan worden omschreven als de dimensie kennisveiligheid binnen CFI. Bovendien wordt de term kennisveiligheid (*research security*) in sommige contexten in Australië wel gebruikt (met name in handleidingen en andere documenten van universiteiten).

De kwetsbaarheden van het Australische hoger onderwijs zijn de afgelopen tien jaar geleidelijk naar het middelpunt van de beleidsdiscussies verschoven. In 2019 richtte de regering de University Foreign Interference Taskforce (UFIT) op en begon zij te investeren in CFI-capaciteit binnen het DHA.[92] Op dat moment waren de publieke en politieke aandacht echter voornamelijk gericht op de Chinese invloed op politiek gebied. Een reeks incidenten waarbij Australische politici betrokken waren, zoals niet-openbaar gemaakte lobbyactiviteiten, contante betalingen en lidmaatschap van aan de Chinese Communistische Partij (CCP) gelieerde organisaties, zorgde ervoor dat kennisveiligheid een ondergeschikte rol bleef spelen binnen de CFI-inspanningen.[93]

In de daaropvolgende jaren, toen Australië zijn relatie met China heroverwoog tegen de achtergrond van bredere economische en nationale veiligheidsbelangen, kwam kennisveiligheid steeds meer op de voorgrond. Dat gebeurde onder meer nadat de toenmalige schaduwminister voor cyberveiligheid en bestrijding van buitenlandse inmenging James Paterson in 2023 live op Sky News Australia aankondigde dat Chinese instellingen samenwerkten met Australische universiteiten en Chinese studenten actief opleidden in offensieve cybercapaciteiten.[94] Deze studenten keerden na hun afstuderen terug naar China om voor Chinese cyberagentschappen te gaan werken. Hoewel de kwestie op dat moment meer in de publieke belangstelling kwam te staan, was de regering al eerder begonnen met onderzoeken naar buitenlandse

[90] RAND Europe Interview – 7.

[91] Australian Department of Home Affairs (2024).

[92] University Foreign Interference Taskforce (2021).

[93] Clarke & Sussex (2022).

[94] RAND Europe Interview - 7; Sharma (2023).

inmenging in het hoger onderwijs, waaronder een onderzoek uit 2022 naar nationale veiligheidsrisico's die van invloed waren op de sector.

In het onderstaande kader worden de belangrijkste actoren in het Australische ecosysteem voor kennisveiligheid beschreven, waarnaar in deze casestudie wordt verwezen.

Kader 3. Belangrijkste actoren in het Australische ecosysteem voor kennisveiligheid

Overheidsactoren

De Australian Research Council (ARC) draagt, zoals vastgelegd in de Australian Research Council Act 2001, een reeks verantwoordelijkheden met betrekking tot het Australische ecosysteem voor onderzoek in het hoger onderwijs. Naast het beheer van het National Competitive Grants Program is de ARC nauw betrokken bij een reeks activiteiten op het gebied van kennisveiligheid. De ARC heeft het ARC Countering Foreign Interference (CFI)-kader gepubliceerd en beheert dit, waarbij zij toezicht houdt op, en screening uitvoert naar, aanvragen voor overheidssubsidies. De organisatie opereert met een hoge mate van onafhankelijkheid, maar staat als orgaan van het Australische Gemenebest niet los van de overheid. Dit kader is in mei 2026 ge-update en omgedoopt naar ARC Research Security Framework.

Het ministerie van Onderwijs (DOE – Department of Education) speelt een sleutelrol als lid van UFIT en bij de algemene coördinatie met de hogeronderwijssector. Het is betrokken geweest bij een reeks beleidsmaatregelen en evaluaties, waaronder de evaluatie van de UFIT-richtlijnen in 2023 en de follow-up in 2024.

Het ministerie van Binnenlandse Zaken (Department of Home Affairs - DHA) speelt een sleutelrol als lid van UFIT en huisvest een reeks belangrijke instanties die verantwoordelijk zijn voor de uitvoering van richtlijnen inzake kennisveiligheid. Het interne Critical and Emerging Technology Security Policy Team blijft verantwoordelijk voor de PACT-regelgeving (Protecting Australia's Critical Technologies).

Nationale veiligheidsdiensten bieden ondersteuning bij de uitvoering van het beleid. Zoals uiteengezet in het ARC-kader voor het tegengaan van buitenlandse inmenging (CFI), beoordelen deze diensten op verzoek van de ARC de nationale veiligheidsrisico's van subsidieaanvragen.

Overheidsactoren gericht op buitenlandse inmenging

The University Foreign Interference Taskforce (UFIT) is een samenwerkingsplatform voor actoren uit de universitaire en overheidssector ter bestrijding van buitenlandse inmenging. De taskforce is in 2019 opgericht.[95] Deze groep was verantwoordelijk voor het opstellen van de Guidelines to Counter Foreign Interference in the Australian University Sector. Zowel het Australische ministerie van Binnenlandse Zaken als het ministerie van Onderwijs zijn bij de taskforce betrokken.

De National Counter Foreign Interference Coordinator (NCFIC) is een door de Australische regering ingestelde functie die tot doel heeft de inspanningen van de overheid en de particuliere sector ter bestrijding van buitenlandse inmenging te versterken. Zijn bevoegdheden reiken verder dan de veiligheid van het hoger onderwijs en onderzoek en strekken zich uit tot de domeinen van de Australische industrie, de media, lokale gemeenschappen, democratische instellingen en lokale overheden.[96]

Het Coördinatiecentrum voor de bestrijding van buitenlandse inmenging (Counter Foreign Interference Coordination Centre, CFICC) is een overheidsinitiatief dat is opgezet om buitenlandse invloed in de Australische samenleving tegen te gaan. Het ondersteunt de NCFIC in zijn rol door de uitvoering van de Australische inspanningen op het gebied van buitenlandse inmenging te beheren en advies te geven aan sectoren die kwetsbaar zijn voor buitenlandse invloed.[97] Hierbij wordt opgemerkt dat het CFICC, net als de NCFIC, een aanzienlijk breder takenpakket heeft dan alleen onderzoek en hoger onderwijs.

[95] Australian Department of Education (2025).

[96] Australian Department of Home Affairs (2025).

[97] Australian Department of Home Affairs (2025).

Het Informal Foreign Interference Network (INFIN) is een informeel (niet door de overheid geleid) orgaan van 39 Australische instellingen voor hoger onderwijs. Het heeft tot doel best practices uit te wisselen en te zorgen voor naleving van overheidsvoorschriften op het gebied van kennisveiligheid.

Kennisinstellingen en -organisaties

Instellingen voor hoger onderwijs, zoals uiteengezet in het beleidsgedeelte, dragen de primaire verantwoordelijkheid voor het dagelijks beheer van de kennisveiligheid, met name in de context van subsidiefraude. Bepaalde universiteiten hebben geformaliseerde interne systemen opgezet die verantwoordelijk zijn voor deze taak. De University of Western Australia (UWA) heeft bijvoorbeeld een **Foreign Interference Advisory Committee** opgericht om de inspanningen te coördineren.[98] Deze commissie bestaat uit een aantal leden op het niveau van vice-rector. Het beleid van de universiteiten verplicht medewerkers om jaarlijks een verklaring in te vullen en voorziet in meldingskanalen voor studenten. Andere, kleinere universiteiten beschikken vaak niet over de benodigde middelen om fulltime personeel voor CFI aan te nemen, of kiezen ervoor dit niet te doen vanwege de financiële voordelen die internationale studenten opleveren.

3.2. Beleid, wetgeving en screeningsprocedures

3.2.1. Wettelijke basis

De belangrijkste wetgeving voor de kennisveiligheid in Australië is de Australian Research Council Act 2001. Hiermee werd een nationaal orgaan opgericht, de Australian Research Council (ARC), met een breed takenpakket dat onder meer bestaat uit het ondersteunen van Australische instellingen voor hoger onderwijs bij het faciliteren van academische loopbaantrajecten, het ondersteunen van de werving van onderzoekers door instellingen voor hoger onderwijs, het bevorderen van onderzoeksintegriteit en het beheren van financiering voor fundamenteel onderzoek.

De raad van bestuur van de ARC is verantwoordelijk voor het goedkeuren van onderzoekssubsidies, maar is verplicht deze af te wijzen als ministers van mening zijn dat de aanvragen in strijd zijn met 'de veiligheid, defensie of internationale betrekkingen van Australië' (artikel 47, leden 8 en 9). Specifieke omstandigheden die aanleiding kunnen geven tot toepassing van deze clausule zijn onder meer banden met buitenlandse onderzoeks-, overheids-, militaire of inlichtingeninstanties, evenals met entiteiten waarop sancties van toepassing zijn.[99]

In 2024 werd de Australian Research Council Act 2001 gewijzigd en heeft de ARC het onderzoeksscreeningsproces aangescherpt. Hiermee werd een reeks mechanismen ingevoerd, waaronder:

- Het vervroegen van veiligheidscontroles naar een eerder stadium in de aanvraagprocedure;
- Het verzamelen van open-source-inlichtingen (OSINT) om de affiliatie van onderzoekers vast te stellen;
- Verduidelijking van de regels inzake informatieverstrekking;
- Intensievere samenwerking met administratieve organisaties op het gebied van risicobeperking; en
- Versterking van de nalevingsmaatregelen.[100]

[98] The University of Western Australia (2026).

[99] Australian Government (2001).

[100] Australian Research Council (2026a).

3.2.2. Onderzoek naar nationale veiligheidsrisico's

Zoals beschreven in paragraaf 4.1 heeft de Parlementaire Commissie voor Inlichtingen en Veiligheid (PJCIS) in maart 2022 het rapport *Inquiry into national security risks affecting the Australian higher education and research sector* gepubliceerd.[101] Hierin worden de nationale veiligheidsrisico's voor de sector onderzocht, evenals het bewustzijn en de mogelijkheden van de sector om deze risico's aan te pakken, en de effectiviteit van het bestaande beleid om deze bedreigingen het hoofd te bieden.

Het onderzoek deelt de belangrijkste risico's voor de hogeronderwijssector in verschillende brede categorieën in, met name cyberdreigingen, spionage en buitenlandse beïnvloeding. Opvallend is dat fraude niet als aparte categorie wordt genoemd, maar in bepaalde gevallen wel wordt besproken als een faciliterende factor. Het rapport belicht voorbeelden, zoals een mogelijke subsidiefraude van 280 miljoen AUD in de afgelopen 20 jaar als gevolg van talentprogramma's van de CCP. De ARC merkt op dat subsidiefraude wijdverbreid was en dat dit een uitdaging vormde, omdat universiteiten verantwoordelijk zijn voor subsidies en dus ook voor het beperken van frauderisico's. Een voorbeeld van het laatste was Monash University in Melbourne die verplichte trainingen voor medewerkers en studenten heeft geïmplementeerd op het gebied van kennisveiligheid, waaronder fraudebestrijding.[102]

Op basis van de bevindingen bevat het rapport een lijst met 27 aanbevelingen die de regering moet uitvoeren. Relevant voor dit onderzoek is aanbeveling 26, waarin staat [103]:

> De commissie beveelt de Australian Research Council aan om via de University Foreign Interference Taskforce duidelijk aan de sector te communiceren wat de ernstige gevolgen zijn van subsidiefraude, teneinde het bewustzijn van de openbaarmakingsvereisten te vergroten. Alle financieringsorganisaties van het Gemenebest dienen na te gaan of het bestaande beleid inzake naleving en verantwoording met betrekking tot de toekenning van subsidiegelden toereikend is.
>
> Daarnaast beveelt de commissie de Australian Research Council aan de sancties tegen subsidiefraude en ontoereikende of onvolledige openbaarmaking aan te scherpen en prioriteit te geven aan het onderzoek naar en de handhaving van deze zaken.
>
> Aanbestedingen die worden uitgeschreven door alle overheidsinstanties die subsidies verstrekken aan onderzoeksinstellingen, moeten een standaardclausule bevatten waarin naleving van het bestaande beleid ter bestrijding van buitenlandse inmenging wordt vereist.

In februari 2023 maakte de Australische regering haar reactie op dit parlementaire rapport bekend.[104] Ze stelde daarin ten aanzien van aanbeveling 26 dat de voorstellen 'in principe worden gesteund'. ARC kreeg daarbij de opdracht om samen te werken met het ministerie van Onderwijs en de Taskforce Universitaire

[101] Parliamentary Joint Committee on Intelligence and Security (2022).

[102] Parliamentary Joint Committee on Intelligence and Security (2022).

[103] Parliamentary Joint Committee on Intelligence and Security (2022, 139).

[104] Australian Government (2023).

Buitenlandse Inmenging om het bewustzijn over openbaarmakingsvereisten en subsidiefraude te vergroten.[105]

3.2.3. Guidelines and frameworks

De regering had eerder de Guidelines to Counter Foreign Interference in the Australian University Sector gepubliceerd, die in 2019 – drie jaar vóór het onderzoek – waren opgesteld door de UFIT. Het doel van deze richtlijnen is om als toolkit te dienen voor Australische universiteiten om 'nieuwe instrumenten, kaders en middelen te ontwikkelen of bestaande te onderzoeken, die kunnen worden gebruikt voor het beoordelen en beperken van risico's van buitenlandse inmenging, in verhouding tot het risico'.[106] De toolkit richt zich echter voornamelijk op due diligence en cyberbeveiliging, en gaat niet in op frauderisico's, in overeenstemming met de bevindingen en aanbevelingen van het onderzoek. In augustus 2023 voltooide het ministerie van Onderwijs (DOE) het vervolg, het *Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector,* waarvoor een reeks rondetafelgesprekken en workshops met universiteiten werd gehouden.[107] De belangrijkste bevinding was dat er grote verschillen in de implementatie bestonden, aangezien elke universiteit een ander risicoprofiel en een andere risicotolerantie had, waardoor een uniforme strategie onmogelijk was.[108] Het DOE publiceerde in 2024 een vervolg op het rapport. Hierin werd opgemerkt dat 92% van de universiteiten de procedures in de voorgaande twaalf maanden had aangescherpt. Er werd echter ook gesignaleerd dat ongeveer de helft van de universiteiten te maken had met toenemende belemmeringen bij de implementatie van CFI-mechanismen, grotendeels als gevolg van een gebrek aan middelen.[109]

Hoewel de UFIT-richtlijnen zich voornamelijk richten op de veerkracht van instellingen voor hoger onderwijs, heeft de Australische regering ook maatregelen genomen om de veiligheid van onderzoek in het kader van overheidsbeleid te waarborgen. In december 2023, tien maanden nadat de regering opdracht had gegeven ter ondersteuning van aanbeveling 26, publiceerde de ARC het ARC Countering Foreign Interference (CFI) Framework.[110] Dit kader pakt eerdere tekortkomingen aan en introduceert een op CFI gerichte risicobeoordeling gedurende de gehele subsidiecyclus van het National Competitive Grants Program (NCGP). Het kader introduceert een beoordelingsproces, zowel vóór als na de toekenning van de subsidie. In mei 2026 is een update over het ARC Research Security Framework gepubliceerd, waarin dit beoordelingsproces tevens aan bod komt.[111]

ARC Framework: overwegingen vóór de toekenning

Het proces verloopt in vastgestelde fasen, waarbij verschillende actoren verantwoordelijk zijn voor de screening. Eerst **beoordeelt** de **universiteit de aanvragen.** Het personeel is getraind om risico's te identificeren en te melden en is op de hoogte van alle openbaarmakingsvereisten. De universiteit voert

[105] Australian Government (2023).

[106] University Foreign Interference Taskforce (2021).

[107] University Foreign Interference Taskforce (2021).

[108] Australian Department of Education (2023).

[109] Australian Department of Education (2024).

[110] Australian Research Council (2023).

[111] Australian Research Council (2026a)

controles uit op alle deelnemers aan de aanvraag. Due-diligence-controles worden uitgevoerd volgens de hierboven geïntroduceerde UFIT-richtlijnen. De universiteit is verantwoordelijk voor het valideren van alle informatie die later aan de ARC wordt doorgegeven, en moet ervoor zorgen dat alle belangenconflicten (COI's) worden gemeld. Voor potentiële risico's die in deze fase worden geïdentificeerd, wordt een risicobeperkend plan opgesteld. Zodra deze stappen zijn voltooid, wordt de aanvraag ingediend bij de ARC.

Als de **ARC** de aanvraag heeft ontvangen, **voert** zij **een beoordeling uit**. Aan de hand van de in de aanvraag verstrekte informatie en OSINT-gegevens tracht de ARC eventuele potentiële risico's in kaart te brengen. Indien de ARC bij de beoordeling geen problemen heeft vastgesteld, wordt de aanvraag **direct ter besluitvorming** voorgelegd **aan de minister.** Is er wel een probleem vastgesteld, dan **zullen Australische nationale veiligheidsdiensten de risico's beoordelen** aan de hand van niet-openbare informatie, of zal de universiteit die bij de subsidie betrokken is **aanvullende garanties voor risicobeperking bieden.** Zodra een van beide of beide maatregelen zijn genomen, zal de ARC deze aanvullende informatie beoordelen, alvorens haar door te sturen naar de minister voor een definitief besluit. In alle gevallen wordt de minister geïnformeerd over bestaande risico's en risicobeperkende strategieën.

ARC Framework: Overwegingen na toekenning

Het ARC-kader beschrijft ook een procedure die moet worden gevolgd wanneer een nieuwe onderzoeker toetreedt tot een door de ARC gefinancierd project, of wanneer een bestaande onderzoeker in het project van affiliatie verandert. Dit proces is vergelijkbaar met de beoordeling vóór de toekenning, hoewel er een definitief aangewezen afgevaardigde wordt geïntroduceerd die de uiteindelijke beslissingsbevoegdheid heeft.[112] Ten eerste **beoordeelt** de **universiteit de aanvraag** en voert zij een controle uit op de betreffende deelnemer. Ten tweede **beoordeelt** de **ARC de aanvraag** aan de hand van de aanvraaggegevens en OSINT. Als er geen problemen worden vastgesteld, gaat de aanvraag rechtstreeks naar de afgevaardigde, die bevestigt dat er voldoende risicobeperkende maatregelen zijn getroffen. Wordt toch een probleem vastgesteld, dan **zullen de nationale veiligheidsdiensten de aanvraag** aan de hand van aanvullende informatie **beoordelen** en/of **zal** de **universiteit aanvullende garanties geven.** Deze informatie wordt vervolgens ter beoordeling teruggestuurd naar de ARC, die op haar beurt de afgevaardigde op de hoogte stelt. De gedelegeerde kan tot slot bevestigen dat de problemen voldoende zijn aangepakt en de wijzigingen in de projectbezetting goedkeuren, of, indien hij van mening is dat er nog steeds risico's bestaan, zelf risicobeperkende maatregelen invoeren alvorens de minister definitief op de hoogte te stellen.

In 2026 kondigde de ARC aan dat de doorlooptijd voor succesvolle subsidieaanvragen met enkele maanden zou worden verlengd. Dit besluit heeft tot grote bezorgdheid geleid binnen de academische gemeenschap, met name wat betreft de mogelijke terugtrekking van industriële partners mochten er langdurig vertragingen optreden.[113]

3.2.4. Verordening Protecting Australia's Critical Technologies (PACT)

De Australische PACT-verordening die in 2024 van kracht werd, vormt het wettelijke kader voor het beheer van risico's in verband met gevoelig onderzoek en kritieke technologieën. Op grond van PACT zijn de

[112] Australian Research Council (2023).

[113] RAND Europe Interview – 7.

autoriteiten bevoegd om visa te weigeren of in te trekken zodra er een onredelijk risico bestaat op technologieoverdracht naar buitenlandse entiteiten. Studenten die overstappen naar opleidingen die verband houden met kritieke technologieën, zijn verplicht de relevante instanties hiervan op de hoogte te stellen. De PACT-verordening is qua reikwijdte beperkt tot twee belangrijke aspecten. Ten eerste geldt de verordening alleen voor postdoctorale studenten. Ten tweede geldt de verordening alleen voor opleidingen die gericht zijn op kritieke technologieën, waarvan een vaste lijst is gepubliceerd door het ministerie van Industrie, Wetenschap en Hulpbronnen.[114]

Deze aanpak is gebaseerd op partnerschappen voor het delen van inlichtingen, die vanaf 2020/21 begonnen met het verstrekken van briefings over opkomende bedreigingen voor de kennisveiligheid. Naar aanleiding daarvan werden speciale werkgroepen opgericht om kwetsbaarheden binnen de Australische context te beoordelen en aan te pakken. Uit vroege bevindingen bleek dat er onderzoekssamenwerkingen bestonden die de belangen van vijandige militaire partijen dienden, wat aanleiding gaf tot verder overleg met internationale partners en inspanningen om effectieve praktijken in te voeren.[115]

Hoewel deze aanpak de overheid weliswaar sterke bevoegdheden biedt om de kennisveiligheid actief te ondersteunen, heeft hij toch zijn beperkingen. Ten eerste bestaat er in Australië geen nationaal registratiesysteem voor opleidingen. Daardoor wordt er weliswaar toezicht gehouden op de gebieden met het hoogste risico, maar is naleving van de voorschriften voornamelijk afhankelijk van zelfmelding of rapportage door instellingen voor hoger onderwijs om studenten die van opleiding veranderen te identificeren. Hoewel het niet melden van een overstap kan leiden tot intrekking van een visum, gebeurt de opsporing niet automatisch.[116] In een interview met de UNSW werd echter opgemerkt dat, als er al sprake was van gevallen, er slechts weinig gevallen waren waarin studenten uit een land met een hoog risico overstapten naar een opleiding die zich richt op kritieke technologieën.[117]

Een tweede beperking is dat het bestaan van de PACT-regelgeving in sommige gevallen de verdere due diligence binnen instellingen kan verminderen. Er heerst nog steeds de hardnekkige opvatting dat, zodra de overheid een visum heeft afgegeven, alles in orde is.[118] Als gevolg hiervan verschuift de focus van de instelling zodra iemand een visum heeft ontvangen vrijwel volledig naar de ondersteuning van zijn of haar binnenkomst en integratie in Australië en vinden er na aankomst in feite geen verdere controles meer plaats. Universiteiten en onderzoeksorganisaties voeren zelden aanvullende beoordelingen uit, tenzij de persoon betrokken is bij een duidelijk defensiegerelateerd project. Dit vertrouwen op de initiële screening door de overheid kan hiaten in het lopende risicobeheer veroorzaken en kan de kwetsbaarheid voor het ontstaan van veiligheidsdreigingen na aankomst vergroten.[119]

Ten slotte wordt in een interview opgemerkt dat instellingen voor hoger onderwijs niet worden geïnformeerd wanneer en waarom specifieke aanvragen de screeningsregelgeving hadden geactiveerd,

[114] Australian Department of Industry, Science and Resources (2023).

[115] RAND Europe Interview – 7.

[116] RAND Europe Interview – 7.

[117] RAND Europe Interview – 5.

[118] RAND Europe Interview – 1.

[119] RAND Europe Interview – 1.

waardoor het moeilijk is om op institutioneel niveau vaardigheden op het gebied van doorlichting te ontwikkelen.[120]

3.3. Document- en identiteitsfraude

Hoewel mechanismen zoals de PACT-regelgeving en het ARC-kader zijn ontworpen om grondige document- en bewijscontroles uit te voeren, ligt de primaire focus niet op het verifiëren van de authenticiteit van documenten – zoals het opsporen van vervalste of nagemaakte identiteitsbewijzen en diploma's – maar veeleer op het identificeren van potentiële risico's. Tot op heden zijn er geen gevallen ontdekt van personen die onder een valse identiteit reisden.[121] Aangezien buitenlandse statelijke actoren echter de grootste bedreiging vormen, is het wellicht ook vrijwel onmogelijk om frauduleuze referenties op te sporen wanneer deze door overheidsinstanties zijn uitgegeven.[122]

In plaats daarvan betreft de belangrijkste gesignaleerde vorm van fraude in Australië het geven van onjuiste informatie, met name in cv's en subsidieaanvragen.[123] In de afgelopen twaalf tot achttien maanden is een van de duidelijkste, opkomende trends het opzettelijk verdoezelen van de herkomst van studiebeurzen.[124] Er is sprake van een toenemende, systematische onjuiste voorstelling van financiering, en van gevallen waarin personen opzettelijk aangeven banden te hebben met instellingen met een lager risico en hun banden met de daadwerkelijke (en mogelijk risicovollere) organisaties verzwijgen. Personen laten vaak bepaalde banen of stages weg op de officiële versies van cv's die zij indienen, en bewaren de volledige details voor cv's die in private sferen worden gedeeld.[125] Hetzelfde patroon is waarneembaar bij onderzoeksresultaten: onderzoek zonder dual use wordt openbaar vermeld, terwijl militair gerelateerd onderzoek wordt verborgen. Bovendien worden affiliaties met organisaties vaak niet vertaald, waardoor hun werkelijke betekenis nog verder wordt versluierd.[126] Ondanks de relatieve publieke erkenning van deze kwesties, benadrukt recent bewijs de omvang van de verkeerde voorstelling van zaken. Zo meldde de China Scholarship Council van de Volksrepubliek China in 2024 1.000 begunstigden van financiering in Australië, terwijl slechts 350 studenten openlijk erkenden deze steun te hebben ontvangen.[127] Deze aanzienlijke discrepantie onderstreept hoe vaak personen niet transparant zijn over de aard of de herkomst van de financiering voor hun onderzoek.

Een andere vastgestelde vorm van fraude betrof valse uitnodigingsbrieven voor visumdoeleinden. De UNSW registreerde in de afgelopen twee tot drie jaar in totaal 6 tot 12 gevallen hiervan.[128] Dit komt voornamelijk voor op faculteitsniveau, bij gastwetenschappers. Vaak worden gevallen gesignaleerd door andere instellingen voor hoger onderwijs die contact opnemen om te verifiëren of een uitnodiging echt is.

[120] RAND Europe Interview – 5.
[121] RAND Europe Interview – 7.
[122] RAND Europe Interview – 7.
[123] RAND Europe Interview – 7.
[124] RAND Europe Interview – 7.
[125] RAND Europe Interview – 7.
[126] RAND Europe Interview – 7.
[127] RAND Europe Interview – 7.
[128] RAND Europe Interview – 5.

Deze informatie-uitwisseling wordt mogelijk gemaakt door het Australische Informal Foreign Interference Network (INFIN), een niet-gouvernementele organisatie van 39 Australische instellingen voor hoger onderwijs, die gezamenlijk de inspanningen op het gebied van CFI en de naleving van overheidsvoorschriften bespreken.

Opvallend is dat er geen relevante casestudies zijn met betrekking tot de PACT-regelgeving. Hoewel het mechanisme is toegepast om visumaanvragen te beperken, blijven deze buiten het publieke domein. Tijdens een interview wordt opgemerkt dat eventuele fraude alleen openbaar zal worden gemaakt als een aanvrager in de toekomst besluit een beslissing aan te vechten.[129] en dat is op het moment van schrijven (mei 2026) nog niet gebeurd.

3.4. Bevindingen en conclusie

Australië heeft een alomvattende en dynamische aanpak gekozen om zijn onderzoeksecosysteem te beveiligen: het kadert de inspanningen binnen het bredere concept van 'het tegengaan van buitenlandse inmenging' in plaats van de maatregelen te beperken tot de engere term kennisveiligheid. Deze strategische kadering breidt de bescherming uit naar diverse sectoren, waaronder het hoger onderwijs, het bedrijfsleven, de media en democratische instellingen. Hieronder worden de belangrijkste aspecten van de Australische aanpak uiteengezet, evenals de belangrijkste belemmeringen die nog steeds in de strategie aanwezig zijn.

Relevant beleid en relevante procedures

Voortdurende evaluatie: Sinds de oprichting van UFIT in 2019 is de Australische regering betrokken bij een interactieve zelfevaluatie van de praktijk op het gebied van kennisveiligheid. Hierdoor heeft zij zwakke punten kunnen identificeren en daar haar aandacht op kunnen richten. Initiatieven zoals de twee vervolgrapporten over de implementatie van de UFIT-richtlijnen, en het parlementaire onderzoek van 2022 en de reactie van de regering daarop, benadrukken een essentieel aspect van een succesvolle praktijk op het gebied van kennisveiligheid. Namelijk dat veiligheid niet statisch is: het is niet iets dat eenmaal bereikt kan worden, maar iets dat voortdurende evaluatie, toewijzing van middelen en monitoring vereist om ervoor te zorgen dat best practices kunnen worden gerealiseerd. Deze voortdurende, adaptieve aanpak is direct relevant voor de Australische inspanningen om fraude op het gebied van kennisveiligheid te bestrijden. Zoals opgemerkt, werd fraude in de oorspronkelijke UFIT-richtlijnen en vervolgrapporten niet genoemd. Pas tijdens het latere parlementaire onderzoek werd (subsidie)fraude specifiek als een probleem aangemerkt, wat vervolgens leidde tot de totstandkoming van het ARC-kader en de invoering van mechanismen voor het opsporen en identificeren van fraude. Hoewel er nog aanzienlijke belemmeringen en uitdagingen bestaan in de Australische aanpak van kennisveiligheid, draagt de voortdurende aandacht van de regering bij aan concrete vooruitgang bij het aanpakken van deze kwesties.

Openbare mechanismen voor kennisveiligheid: Australië profiteert van publiekelijk toegankelijke wetgeving en mechanismen die de processen voor het uitvoeren van controles duidelijk omschrijven. Het ARC-kader beschrijft openbaar de belangrijkste actoren die betrokken zijn bij het subsidiebeoordelingsproces, en hoe aanvragen van fase naar fase verlopen, waarbij de verantwoordelijkheden

[129] RAND Europe Interview – 7.

bij elke stap worden uiteengezet. Dit concrete traject heeft het gemakkelijker gemaakt om gevallen van fraude te identificeren, waarbij subsidiefraude naar voren komt als de meest frequent geconstateerde vorm. Het blijft echter onduidelijk of subsidiefraude werkelijk de belangrijkste vorm is, of dat deze simpelweg het meest nauwgezet wordt gevolgd en geobserveerd vanwege de unieke robuustheid van het ARC-kader. Tegelijkertijd worden in de PACT-regelgeving – hoewel deze gezien de nationale veiligheidsdimensie minder transparant is – de risicogebieden, de verantwoordelijkheden van individuele onderzoekers en de mogelijke gevolgen duidelijk omschreven.

Deze transparantie en procesgerichtheid bevorderen een omgeving waarin naleving de norm is en wordt verwacht. Hiermee is een sterke structurele basis voor kennisveiligheid gelegd en vooral, zijn instellingen voor hoger onderwijs duidelijk geïnformeerd over hun rol in het systeem. In het geval van Australië maakt het INFIN communicatie tussen instellingen voor hoger onderwijs mogelijk over de implementatie van de mechanismen en richtlijnen, wat op haar beurt leidt tot een groter bewustzijn van fraudegevallen, zoals blijkt uit de discussie rond frauduleuze uitnodigingsbrieven.

Bestaande beperkingen

Beperkingen op het gebied van middelen en capaciteit: Ondanks verbeterde procedures worden de meeste Australische universiteiten geconfronteerd met aanhoudende en toenemende uitdagingen als gevolg van beperkte middelen. Grote instellingen zoals de UNSW beschikken over teams van meerdere personen die zich uitsluitend bezighouden met kennisveiligheid, terwijl kleinere instellingen voor hoger onderwijs moeite hebben om gespecialiseerd kennisveiligheid personeel of robuuste interne ecosystemen in stand te houden, wat leidt tot een ongelijkmatige implementatie binnen de sector. Dit wordt in elk interview aangemerkt als de grootste belemmering voor kennisveiligheid in Australië. Meer dan eens is opgemerkt dat identiteits- en documentfraude niet voorkomt, omdat fraude door kwaadwillende actoren als een onnodige inspanning wordt beschouwd en veel instellingen voor hoger onderwijs simpelweg niet over de middelen beschikken om controles uit te voeren. Hoewel Australië dan ook zeer succesvol is geweest in het implementeren van fraudecontroles rond subsidieaanvragen en visa, ontbreekt deze robuustheid op een meer gedetailleerd niveau.

In dit verband leiden de strenge overheidsregelingen er ook vaak toe dat instellingen voor hoger onderwijs in het ongewisse blijven over de specifieke redenen waarom aanvragen een markering krijgen of visa worden beperkt. Dit gebrek aan feedback belemmert deze instellingen om interne expertise op te bouwen, hun eigen doorlichtingsprocessen te verfijnen of te leren van eerdere gevallen, zelfs als instellingen meer middelen beschikbaar hebben. Bijgevolg is er sprake van een te grote afhankelijkheid van het oordeel van de overheid: zodra een onderzoeker of student toestemming van de staat krijgt om Australië binnen te komen, verschuift de focus van de instelling vaak naar ondersteuning van hun integratie, met minimale voortdurende controle of monitoring. Deze dynamiek creëert potentiële kwetsbaarheden, met name op het gebied van doorlopend risicobeheer en fraudedetectie.

4. Duitsland

4.1. Kennisveiligheid: algemene context

Kennisveiligheid wordt in het Duitse systeem gezien als een complexe wisselwerking tussen academische vrijheid enerzijds en het beschermen van kwetsbaar onderzoek en bijbehorende resultaten en de bredere samenleving anderzijds. Academische vrijheid is verankerd in de Duitse grondwet en behoort tot een van de artikelen die onder de Ewigkeitsgarantie vallen, een niet voor wijziging vatbare kern van de grondwet.[130] De grote waarde die wordt gehecht aan academische vrijheid heeft ervoor gezorgd dat beleid omtrent kennisveiligheid beperkt was in Duitsland en men het woord veiligheid veelal vermeed.[131] In plaats daarvan sprak men liever over bestaande praktijken rondom onderzoeksethiek en ethische samenwerking waardoor securitisatie van beleid, ofwel het expliciet definiëren van een vraagstuk als een dreiging, veelal werd vermeden.[132] Deze context verklaart waarom kennisveiligheid in Duitsland lange tijd vooral via ethische verantwoordelijkheid en institutionele zelfregulering is benaderd, in plaats van via bindende veiligheidskaders.

Het Duitse federale systeem vormt de aanpak van kennisveiligheid ook sterk. De federale overheid heeft geen bevoegdheden op het gebied van onderwijs. De zestien Duitse Bundesländer of deelstaten zijn verantwoordelijk voor hun eigen onderwijsbeleid, inclusief beleid met betrekking tot financiering en de organisatie van het hoger onderwijs en onderzoeksinstituten.[133] Daarnaast spelen semi-onafhankelijke onderzoeksorganisaties nog een belangrijke rol, die bemiddelen bij de verdeling van financiering en het bepalen van strategische prioriteiten. Denk hierbij aan instituten als het Max-Planck-Gesellschaft en Helmholtz-Gemeinschaft en intermediaire organisaties zoals de Duitse Academische Uitwisselingsdienst (DAAD) en de Duitse Onderzoeksstichting (DFG), de belangrijkste financieringsorganisatie voor onderzoek in Duitsland.[134] Dit alles zorgt ervoor dat er een zeer decentraal systeem is ontstaan waarbij veel verantwoordelijkheid ligt bij individuele onderzoekers en organisaties. De decentrale inrichting van het Duitse systeem is daarmee niet slechts een organisatorisch kenmerk, maar bepaalt in sterke mate ook welke risico's zichtbaar worden en welke buiten beeld blijven. Waar verantwoordelijkheden verspreid zijn over onderzoekers, instellingen, deelstaten en intermediaire organisaties, wordt effectieve kennisveiligheid afhankelijk van coördinatie, capaciteit en gedeelde interpretaties van risico's tussen de betrokken partijen.

[130] Speiser (2022).

[131] D'Hooghe & Lammertink (2022).

[132] D'Hooghe & Lammertink (2022).

[133] D'Hooghe & Lammertink (2022).

[134] Rüffin et al. (2025).

Pas rond 2022 begon de terminologie van kennisveiligheid op te komen in het Duitse discours, aangewakkerd door een reeks journalistieke en academische onderzoeken waaruit bleek dat Chinese onderzoekers die in Duitsland te gast waren, mogelijk opzettelijk militair relevante onderzoeksresultaten en -methoden hadden verzameld en doorgegeven aan organisaties met banden met het Chinese leger of partij- en overheidsinstanties.[135]

Het Federaal Ministerie van Onderwijs en Onderzoek (BMBF), en diens opvolger het Federaal Ministerie van Onderzoek, Technologie en Ruimtevaart (BMFTR), zet sinds 2024 in op het ontwikkelen van een meer strategische aanpak omtrent kennisveiligheid (zie Kader 5.2). Deze nieuwe aanpak moet vrijheid van de wetenschap meer in overeenstemming brengen met veiligheidsbeleidsbelangen in het licht van de huidige *Zeitenwende* (keerpunt in de geschiedenis).[136] Het BMBF plaatst dit keerpunt expliciet bij de Russische inval in Oekraïne in 2022, hoewel multipolariteit, cyberdreigingen en systematische rivaliteit, met name met China, ook voor deze tijd al in opkomst waren.[137] Ook andere Duitse instellingen, zoals de Wissenschaftsrat, Leopoldina (de Nationale Academie voor Wetenschappen) en de Deutsche Forschungsgemeinschaft, ondersteunen de nieuwe aanpak en pleiten voor meer nadruk op het belang van kennisveiligheid in academische kringen en beleid.[138]

Het BMBF hanteert hierbij het concept kennisveiligheid (*Forschungssicherheit*) zoals gedefinieerd door de G7 (zie Kader 4).[139]

Kader 4. G7-definitie van Research Security

> Research security involves the actions that protect our research communities from actors and behaviours that pose economic, strategic, and/or national and international security risks. Particularly relevant are the risks of undue influence, interference, or misappropriation of research; the outright theft of ideas, research outcomes, and intellectual property by states, militaries, and their proxies, as well as by non-state actors and organized criminal activity; and other activities and behaviours that have adverse economic, strategic, and/or national security implications.[140]

[135] Rüffin et al. (2025); German National Academy of Sciences Leopoldina and German Research Foundation (2024). Zie ook: Stoff, (2023); Deutschlandfunk.de (2022).

[136] Bundesministerium für Bildung und Forschung (2024).

[137] Bundesministerium für Bildung und Forschung (2024).

[138] Wissenschaftsrat (2025); German National Academy of Sciences Leopoldina and German Research Foundation (2024).

[139] Bundesministerium für Bildung und Forschung (2024).

[140] G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE) (2022).

Kader 5. Belangrijkste actoren in het Duitse ecosysteem voor kennisveiligheid

Overheidsactoren

Federale ministeries (BMBF/BMFTR) van de federale overheid ontwikkelen strategisch beleid rondom kennisveiligheid en werken aan een nationale aanpak, inclusief een Nationaal Platform Kennisveiligheid dat vanaf circa 2027 coördinatie en ondersteuning moet bieden.

DAAD en KIWi zijn contactpunten voor academici en bieden praktische richtlijnen en advisering over internationale samenwerking, inclusief tools voor risicoanalyse en kennisveiligheid (bijvoorbeeld KIWi Kompass).

Het **Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA)** is verantwoordelijk voor exportcontrole, inclusief dual-use-technologieën en immateriële kennisoverdracht binnen onderzoek.

Het **Bundesamt für Migration und Flüchtlinge (BAMF)** verzorgt de controle van documenten bij visumprocedures en vormt daarmee een belangrijke, maar indirecte, component van kennisveiligheid.

Het **Bundesamt für Verfassungsschutz (BfV)**, de binnenlandse veiligheidsdienst, monitort dreigingen en beschrijft methoden van buitenlandse actoren, zoals gebruik van dekmantelbedrijven en misleidende informatie, maar publiceert geen specifieke fraudecijfers.

Kennisinstellingen en -organisaties

Individuele onderzoekers dragen de primaire verantwoordelijkheid voor het identificeren en beheersen van kennisveiligheidsrisico's in hun onderzoek en internationale samenwerkingen, inclusief ethische afwegingen.

Onderzoeksinstellingen en universiteiten zijn verantwoordelijk voor het opzetten van interne structuren, procedures en governance rondom kennisveiligheid. Zij voeren zelf risicoanalyses uit en nemen beslissingen over samenwerking en toelating.

Kommissionen für Ethik sicherheitsrelevanter Forschung (KEFs). Deze interne ethische commissies adviseren over veiligheidsrelevant en dual-use-onderzoek. In 2024 bestonden er meer dan 120 van dergelijke commissies, hoewel hun effectiviteit en zichtbaarheid variëren.

Deutsche Forschungsgemeinschaft (DFG). Als grootste onderzoeksfinancier stelt de DFG-richtlijnen op voor risicobeoordeling (met name voor dual-use-onderzoek) en integreert kennisveiligheid in financieringsbesluiten.

4.2. Beleid en wetgeving

Het Duitse systeem is, zoals eerder benoemd, zeer gedecentraliseerd en bottom-up. Als gevolg hiervan zijn de verantwoordelijkheden voor het beleid rondom kennisveiligheid ook verspreid over vele actoren. Mede door het belang dat wordt gegeven aan academische vrijheid, ligt het gros van de verantwoordelijkheden op het niveau van individuele onderzoekers en de organisaties waarvoor zij werken. Richtlijnen die door landelijke partijen zijn opgezet, worden niet afgedwongen maar blijven aanbevelingen.[141] Er zijn wel verschillende partijen die onderzoek financieren, waaronder de federale overheid, die regels omtrent kennisveiligheid opnemen in hun voorwaarden.[142] Ook is er wet- en regelgeving voor aangrenzende gebieden, zoals onderzoek dat onder exportcontroles komt te vallen en dual-use-toepassingen die de

[141] James et al. (2025).

[142] German National Academy of Sciences Leopoldina and German Research Foundation (2024).

Europese Unie voorschrijft[143] en onderzoeksdomeinen die onder Duitse wetgeving vallen, zoals de Wet genetische aanpassingen en Wet inzake bescherming tegen infecties.[144]

4.2.1. Nieuw kennisveiligheidsbeleid in ontwikkeling

De nieuwe Duitse aanpak voor kennisveiligheid wordt momenteel opgezet. De aanpak, die sinds 2024 in ontwikkeling is, kwam in respons op de Zeitenwende na de Russische inval in Oekraïne die duidelijk maakte dat er meer ingezet moest worden op alle soorten veiligheid.[145] Voor kennisveiligheid wordt het principe 'zo open mogelijk, zo gesloten als nodig' aangehouden.[146]

Het toekomstige beleid inzake kennisveiligheid zal bestaan uit een systeem met gelaagde verantwoordelijkheden waarin alle actoren volgens het subsidiariteitsbeginsel hun verantwoordelijkheid moeten nemen.[147] Deze zijn verdeeld over het individuele, institutionele, organisatie-, Länder- en federale niveau, waarbij taken voortvloeien uit de specifieke verantwoordelijkheden van elk niveau. Op individueel niveau ligt de primaire verantwoordelijkheid bij het herkennen van veiligheidsrelevantie en -risico's van het eigen wetenschappelijk werk en het betrekken van relevante contacten en autoriteiten om risico's te beperken. Wetenschappelijke instellingen, organisaties en gast-Länder moeten zorgen voor passende structuren en processen voor kennisveiligheid, terwijl de federale overheid een samenhangende benadering ontwikkelt, belanghebbenden verbindt en middelen beschikbaar stelt ter ondersteuning van alle niveaus.

Daarnaast wordt een Nationaal Platform voor Kennisveiligheid ingericht dat een centrale coördinerende en integrerende rol krijgt binnen het Duitse kennis- en onderzoeksstelsel.[148] Het platform zal wetenschappelijke instellingen en organisaties ondersteunen bij het identificeren, analyseren en afwegen van kansen en risico's van onderzoeksactiviteiten en (internationale) samenwerkingen. Hierin zal ook de geopolitieke context worden meegenomen. Het platform krijgt drie kernfuncties: coördinatie van relevante actoren en expertise uit wetenschap en overheid, het ontsluiten en bundelen van informatie over risico's en dreigingen en het bieden van gerichte begeleiding bij het toepassen van risico-gebaseerde beschermingsmaatregelen binnen bestaande institutionele structuren.

Organisatorisch zal het platform bestaan uit een strategisch sturingscomité en een uitvoerend servicecentrum, dat is ondergebracht bij het BMFTR en zal fungeren als centraal aanspreekpunt voor kennisinstellingen.[149] Het platform werkt nauw samen met bestaande nationale, Europese en internationale advies- en informatievoorzieningen en met relevante veiligheidsautoriteiten, onder meer voor het opstellen van een doorlopende nationale risicoanalyse op het gebied van kennisveiligheid. Hiermee draagt het platform bij aan het versterken van expertise en handelingsvermogen binnen instellingen, het voorkomen van versnippering en duplicatie en het borgen van een samenhangende, toekomstbestendige aanpak van

[143] Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (herschikking).

[144] German National Academy of Sciences Leopoldina and German Research Foundation (2024).

[145] Bundesregierung (2022).

[146] Bundesministerium für Forschung, Technologie und Raumfahrt (2026).

[147] Bundesministerium für Forschung, Technologie und Raumfahrt (2025).

[148] Bundesministerium für Forschung, Technologie und Raumfahrt (2025).

[149] Bundesministerium für Forschung, Technologie und Raumfahrt (2025).

kennisveiligheid. De volledige operationele inzet is voorzien vanaf begin 2027. In reactie op de veranderende geopolitieke realiteit heeft het BMFTR in 2024 een nieuwe divisie opgesteld die zich richt op kennisveiligheid en investeringsscreening. Na een proces waarbij diverse belanghebbenden betrokken waren om de kennisveiligheid te versterken, richt de divisie zich momenteel op de conceptualisering en de ontwikkeling van het Nationaal Platform voor Kennisveiligheid. Het platform zal fungeren als instrument voor coördinatie en integratie en zal met name onderzoeksinstellingen en -organisaties ondersteunen bij hun inspanningen om de kansen en risico's van onderzoeksactiviteiten en internationale samenwerkingsverbanden op passende wijze te analyseren en te beoordelen.

De oprichting van het platform kan worden gelezen als een poging om de nadelen van decentralisatie te mitigeren zonder het Duitse uitgangspunt van academische autonomie volledig los te laten. De beleidsmatige uitdaging ligt daarbij in het versterken van samenhang en expertise, terwijl besluitvorming over concrete samenwerkingen grotendeels bij instellingen en onderzoekers blijft.

4.2.2. DFG – richtlijnen en aanbevelingen voor nationale onderzoeksfinanciering

De Duitse Onderzoeksstichting (Deutsche Forschungsgemeinschaft, DFG) is de grootste organisatie voor de financiering van onderzoek en de centrale, zelfbesturende organisatie voor de wetenschappen en geesteswetenschappen in Duitsland. Financiering voor de DFG komt van de Duitse federale regering en de deelstaatregeringen. De DFG opereert wel als een onafhankelijke organisatie die al haar procedures baseert op wetenschappelijke criteria, waardoor de Duitse regering slechts beperkt invloed heeft op de organisatie.[150]

In 2014 publiceerde de DFG samen met Leopoldina aanbevelingen voor de omgang met veiligheidsrelevant of dual-use-onderzoek.[151] Een geüpdatete versie van deze aanbevelingen werd in 2022 gepubliceerd.[152] De richtlijnen benadrukken dat wetenschappers naast de wettelijk beschermde vrijheid van onderzoek ook een eigen ethische verantwoordelijkheid hebben om mogelijke misbruikrisico's van hun werk te herkennen en af te wegen. Onderzoekers dienen systematisch risicoanalyses uit te voeren, passende maatregelen te nemen om risico's te beperken en zorgvuldig om te gaan met de publicatie en verspreiding van gevoelige resultaten. Daarnaast roepen de aanbevelingen instellingen op om hun onderzoekers in dit proces te ondersteunen met duidelijke ethiekregels, training, compliancestructuren en speciale commissies voor ethiek in veiligheidsrelevant onderzoek.

Naast de specifieke aanbevelingen voor veiligheidsrelevant onderzoek heeft de DFG ook aanbevelingen opgesteld voor het omgaan met risico's in internationale onderzoekssamenwerkingen in het algemeen.[153] Deze zijn minder uitgebreid dan de aanbevelingen voor veiligheidsrelevant onderzoek en zijn voornamelijk bedoeld voor onderzoeken waarbij onderzoekers uit autoritaire landen betrokken worden.[154]

Hoewel de aanbevelingen vooral dienen om aanvragers en onderzoeksinstituten te ondersteunen, kunnen ze ook gebruikt worden tijdens het beoordelings- en besluitvormingsproces van samenwerkingen met

[150] DFG (2026b).

[151] DFG & Leopoldina (2014).

[152] Nationale Akademie der Wissenschaften Leopoldina und Deutsche Forschungsgemeinschaft (2022).

[153] DFG (2023).

[154] DFG (2026b).

buitenlandse onderzoekers en instituten.[155] Bij aanvragen voor DFG-financiering worden aanvragers gevraagd om risicobeoordelingen uit te voeren met behulp van deze richtlijnen en zo de risico's van projecten en partners in kaart te brengen. DFG neemt deze risicobeoordelingen mee in haar besluitvormingsproces om financiering goed, dan wel af te keuren. Hierbij wordt wel nog altijd expliciet rekening gehouden met het beschermde principe van academische vrijheid.[156]

De DFG-richtlijnen laten zien dat onderzoeksfinanciering in Duitsland een belangrijk indirect sturingsmechanisme vormt voor kennisveiligheid. Tegelijkertijd blijft de werking ervan afhankelijk van de kwaliteit van zelfrapportage en risicobeoordeling door aanvragers en instellingen, waardoor verschillen in bewustzijn en expertise kunnen doorwerken in de praktijk.

4.2.3. DAAD & KIWi – contactpunt voor academici

Het Competentiecentrum voor Internationale Academische Samenwerking (Kompetenzzentrum Internationale Wissenschaftskooperationen - KIWi) van de Duitse Academische Uitwisselingsdienst (Deutscher Akademischer Austauschdienst - DAAD) speelt een belangrijke rol bij het versterken van kennisveiligheid binnen internationale wetenschappelijke samenwerking. KIWi ondersteunt universiteiten, onderzoeksinstellingen en individuele onderzoekers bij het herkennen en afwegen van veiligheidsrelevante risico's, onder meer door gerichte advisering over geopolitieke context, dual-use-problematiek, exportcontrole, intellectueel eigendom en wetenschappelijke integriteit. In reactie op toenemende geopolitieke spanningen heeft KIWi zijn kennisveiligheidsactiviteiten in 2023 uitgebreid met praktische instrumenten zoals de KIWi Compass "No Red Lines" en een bijbehorende Knowledge Security Checklist.[157] Dit kompas is een leidraad gebaseerd op verschillende criteria die universiteiten en onderzoeksinstellingen ondersteunt bij het zorgvuldig afwegen van kansen, risico's en kennisveiligheidsaspecten in internationale samenwerking. In plaats van vaste samenwerkingsverboden hanteert het kompas een contextspecifieke benadering, gebaseerd op zes samenhangende beoordelingscriteria:[158]

1. **Algemene veiligheidssituatie**. Analyse van conflicten, instabiliteit, sancties en veiligheidsrisico's die samenwerking kunnen beïnvloeden.
2. **Algemene politieke randvoorwaarden**. Buitenlands beleid, internationale verplichtingen, sanctieregimes en geopolitieke belangen.
3. **Rechtsstatelijke en maatschappelijk-politieke context**. Academische vrijheid, mensenrechten, autonomie van instellingen en rechtszekerheid.
4. **Kansen en risico's van het wetenschapssysteem**. Structuur, governance, financiering en mogelijke kennis- of technologieafvloeiing.

[155] DFG (2023).

[156] DFG (2023).

[157] DAAD (2023); DAAD KIWi (2024); DAAD KIWi (2025).

[158] DAAD KIWi (2024, 9).

5. **Kwaliteit van de partnerinstelling**. Wetenschappelijke reputatie, governance, integriteit en eerdere samenwerkingservaringen.
6. **Inbedding in de eigen institutionele strategie**. Mate waarin samenwerking past binnen strategische doelen, risicobereidheid en verantwoordelijkheden van de instelling.

De bijbehorende checklist gaat in op zaken als partners en financiering, exportcontroles, gebruik van resultaten en intellectuele eigendomsrechten, en ethische vraagstukken. Zo wordt een gestructureerde en transparante basis voor interne besluitvorming en risicobeheersing geboden en wordt tegelijkertijd de openheid van de wetenschap gerespecteerd en de verantwoordelijkheid expliciet bij instellingen en onderzoekers gelegd.

KIWi biedt daarnaast hulp aan onderzoekers en instellingen wanneer zij vragen hebben over kennisveiligheid. Dit gebeurt via individuele advisering, de ontwikkeling van praktische hulpmiddelen en het aanbieden van workshops, seminars en kennisproducten die instellingen helpen bij het opzetten of versterken van interne processen omtrent kennisveiligheid. KIWi fungeert daarbij als laagdrempelig aanspreekpunt en als schakel tussen het wetenschappelijke veld en beleids- en informatiebronnen, zodat vragen over internationale samenwerking, risico's en verantwoordelijkheden tijdig en zorgvuldig kunnen worden geadresseerd binnen de eigen institutionele context.

De meerwaarde van KIWi ligt vooral in het bieden van handelingsperspectief binnen een systeem zonder harde centrale screeningsplicht. Tegelijkertijd onderstreept deze aanpak dat kennisveiligheid in Duitsland primair wordt vormgegeven via ondersteuning en advisering, niet via verplichtingen of wetgeving.

4.2.4. Exportcontroles

Het risico op oneigenlijk gebruik van kennis en onderzoek wordt in Duitsland deels ondervangen door exportcontrolemechanismen, die een belangrijk onderdeel vormen van het bredere kader voor kennisveiligheid. Naast algemene strafwetgeving en internationale verdragen, zoals de Biologische en Chemische Wapenverdragen, speelt het Bundesamt für Wirtschaft und Ausfuhrkontrolle (BAFA) een centrale rol bij de implementatie van EU-regelgeving inzake dual-use-goederen. Deze regelgeving omvat zowel tastbare goederen (zoals laboratoriumapparatuur, chemicaliën en software) als immateriële overdracht van kennis, waaronder technische assistentie en digitale informatie-uitwisseling via e-mail of cloudsystemen. Exportcontrole in de academische context heeft niet alleen betrekking op fysieke export, maar ook op samenwerking met buitenlandse onderzoekers, inclusief gastonderzoekers.[159]

Om instellingen te ondersteunen bij de naleving van exportcontroleverplichtingen publiceerde BAFA in 2023 een geactualiseerde editie van het handboek *Export Control and Academia Manual*.[160] Ook geeft het document aandacht aan de inrichting van Internal Compliance Programmes (ICP's), in lijn met de niet-bindende EU-richtsnoeren uit 2021. Daarnaast wordt kennis over risico's versterkt via initiatieven zoals maandelijkse webinars van het BMBF en de HRK over internationale samenwerking en dual-use-vraagstukken, alsmede specifieke trainingsprogramma's en instrumenten van BAFA.[161]

[159] German National Academy of Sciences Leopoldina and German Research Foundation (2024).

[160] German Federal Office for Economic Affairs and Export Control [BAFA] (2023).

[161] D'Hooghe & Lammertink (2022).

Exportcontrole vormt daarmee het meest juridisch verankerde onderdeel van de Duitse kennisveiligheidsaanpak, maar de reikwijdte ervan blijft beperkt tot specifieke technologieën, kennisoverdracht en toepassingsgebieden. Risico's die samenhangen met personen, affiliaties of misrepresentatie vallen slechts gedeeltelijk onder de strekking van de wetgeving.

4.3. Screeningsprocedures

4.3.1. Individuele verantwoordelijkheid

De screening van onderzoekers in het kader van kennisveiligheid is, zoals eerder besproken, primair de verantwoordelijkheid van onderzoekers en universiteiten zelf. Wettelijke verantwoordelijkheden zijn momenteel beperkt tot exportcontroles op militaire en dual-use-technologieën. Bestaande richtlijnen van koepelorganisaties en onderzoeksinstituten benadrukken de verantwoordelijkheid die onderzoekers en onderzoeksorganisaties zelf dienen te nemen. Wetenschappers en instellingen zijn momenteel aangewezen op het zelf verzamelen van specifieke informatie over veiligheidsrelevante aspecten van hun projecten en moeten daarbij vertrouwen op bronnen zoals de ASPI-tracker, die slechts beperkte informatie bevatten of waarvan onduidelijk is aan welke kwaliteitsnormen zij voldoen.[162] Om het screeningsproces te ondersteunen en institutioneel in te kaderen, maken veel onderzoeksinstellingen gebruik van commissies om ethische vraagstukken omtrent onderzoekssamenwerking te beoordelen, de zogenoemde KEFs (zie 4.3.2.).

Deze inrichting maakt screening sterk afhankelijk van het risicobewustzijn en de beschikbare expertise van individuele onderzoekers en instellingen, welke niet overal even goed op peil kunnen zijn. Ze biedt ruimte voor contextspecifieke afwegingen, maar creëert ook kwetsbaarheden wanneer kennis, capaciteit of toegang tot betrouwbare informatiebronnen beperkt is. Door de gebrekkige inbedding in officiële kanalen en organisaties die toegang hebben tot de vereiste informatie, kan het Duitse systeem kwetsbaar zijn, vooral voor geraffineerde vervalsingen door bijvoorbeeld statelijke actoren.

4.3.2. KEFs als interne screening

Veel Duitse universiteiten en onderzoeksinstellingen kennen commissies voor de ethiek van veiligheidsrelevant onderzoek (KEFs - Kommissionen für Ethik sicherheitsrelevanter Forschung). In 2024 waren er minstens 122 KEFs of vergelijkbare organen in Duitsland die in totaal meer dan 300 onderzoeksinstituten adviseerden over ethische vraagstukken gerelateerd aan veiligheidsrelevant onderzoek.[163] Het merendeel van universiteiten en onderzoeksinstituten hebben KEFs opgezet in een samenwerkingsverband, maar er zijn ook organisaties waar slechts één contactpersoon is aangewezen voor deze taak of waar geen specifieke procedures zijn opgezet.[164]

In de praktijk ondervinden veel KEFs problemen. Zo blijken hun zichtbaarheid en effectiviteit vaak beperkt.[165] Veel onderzoekers zijn onvoldoende bekend met het bestaan en de rol van KEFs, terwijl de commissies vaak kampen met een gebrek aan tijd, middelen en ondersteunende capaciteit, waardoor

[162] Wissenschaftsrat (2025).

[163] Leopoldina and German Research Foundation (2024).

[164] Leopoldina and German Research Foundation (2024).

[165] Wissenschaftsrat (2025); Leopoldina and German Research Foundation (2024).

continuïteit en expertiseopbouw onder druk staan. Daarnaast verschilt de institutionele inbedding sterk tussen instellingen en worden KEFs steeds vaker gevraagd om brede kennisveiligheids- en geopolitieke vraagstukken te beoordelen, wat het risico op overbelasting en rolvervaging vergroot.[166]

4.3.3. BAMF - Federale dienst voor Migratie en Vluchtelingen

Het Bundesamt für Migration und Flüchtlinge (BAMF) is verantwoordelijk voor de controle van vereiste documenten in het visumproces. Documenten die studenten en wetenschappers uit derde landen moeten aanleveren, blijven beperkt tot ze nodig zijn voor het verkrijgen van een visum. Daarbij gaat het onder meer om identiteitsdocumenten en eventueel documenten met betrekking tot de financiën en arbeidsgeschiedenis van de aanvrager. De rol van het BAMF in screening is daarom vooral administratief: de dienst controleert de volledigheid en betrouwbaarheid van documenten in het kader van de migratie- en visumprocedure, maar lijkt geen primaire actor te zijn in de inhoudelijke kennisveiligheids- of onderzoeksscreening.

4.4. Document- en identiteitsfraude

Er is weinig publieke informatie over document- en identiteitsfraude in Duitsland. Cijfers over het aantal incidenten zijn niet openbaar. Ook over het aantal incidenten rondom kennisveiligheid wordt niet openbaar bericht. De Duitse binnenlandse veiligheidsdienst (BfV) geeft wel een overzicht van methoden die risicovolle landen inzetten om gevoelige technologieën en kennis te vergaren, maar richt zich daarbij niet specifiek op identiteits- en documentfraude.

Volgens het BfV gebruiken risicostaten uiteenlopende heimelijke verwervingsmethoden om hun betrokkenheid te verhullen en controles te omzeilen.[167] Zij opereren via door de staat aangestuurde inkoop- en verwervingsnetwerken, waarin dekmantelbedrijven en ogenschijnlijk legitieme organisaties worden ingezet om de werkelijke opdrachtgever en eindgebruiker te maskeren. Daarnaast worden leveringsroutes bewust omgeleid via tussenhandelaren en derde landen, waardoor herkomst en bestemming moeilijk te traceren zijn. Het BfV wijst er ook op dat export- en kenniscontroles worden ontweken met misleidende informatie in aanvragen, door het testen van toezicht via proefverwervingen en door het opsplitsen van transacties in kleinere, ogenschijnlijk onschuldige delen. Of deze methoden in Duitsland ook daadwerkelijk zijn ingezet wordt niet duidelijk uit openbare bronnen.

4.5. Bevindingen en conclusies

In deze sectie worden de belangrijkste bevindingen uit de Duitse casestudie samengebracht. Op basis van de analyse van beleid, wetgeving en praktijk rondom kennisveiligheid en screening ontstaat een beeld van een sterk gedecentraliseerd systeem, waarin verantwoordelijkheden primair bij onderzoekers en instellingen liggen. Tegelijkertijd laat de casestudie zien dat deze benadering zowel specifieke sterktes kent als duidelijke beperkingen, met name op het gebied van consistentie, zichtbaarheid en informatievoorziening. Hoewel

[166] Wissenschaftsrat (2025); Leopoldina and German Research Foundation (2024).
Bundesamt für Verfassungsschutz (2026).

het nieuwe kennisveiligheidsbeleid nog in ontwikkeling is, laat dit zien dat kennisveiligheid een steeds belangrijkere rol krijgt in Duitsland.

De Duitse casus laat vooral zien hoe kennisveiligheid vorm krijgt in een systeem waarin academische vrijheid, decentralisatie en institutionele autonomie zwaar wegen. De centrale vraag is niet alleen of er voldoende instrumenten bestaan, maar ook of deze instrumenten in de praktijk voldoende consistent, zichtbaar en effectief worden toegepast.

Relevant beleid en procedures

Ontwikkeling van ondersteunende instrumenten en richtlijnen: Hoewel wettelijke verplichtingen beperkt zijn, bestaan er diverse richtlijnen en praktische hulpmiddelen die instellingen ondersteunen bij het omgaan met kennisveiligheidsrisico's. Initiatieven zoals de DFG-richtlijnen voor dual-use-onderzoek en de KIWi-tools bieden een gestructureerd kader voor risicobeoordeling en besluitvorming. De kracht van deze instrumenten ligt vooral in hun compatibiliteit met het Duitse model van zelfregulering: zij bieden structuur zonder centrale verplichting. Tegelijkertijd maakt juist deze vorm het mogelijk om kennisveiligheid te versterken zonder een abrupte breuk met bestaande academische normen.

Opkomst van nationale coördinatie en strategische aandacht: Sinds circa 2022 is sprake van een duidelijke beleidsontwikkeling richting een meer samenhangende nationale aanpak van kennisveiligheid. De voorgenomen oprichting van een nationaal platform en de toenemende aandacht vanuit federale ministeries wijzen op een groeiend besef van het belang van coördinatie en ondersteuning. Deze ontwikkeling kan bijdragen aan het versterken van kennisdeling, het bundelen van expertise en het verminderen van versnippering in de toekomst.

Bestaande beperkingen

Sterke fragmentatie en gebrek aan uniformiteit: De sterk gedecentraliseerde inrichting van het Duitse systeem leidt tot aanzienlijke verschillen tussen instellingen in de manier waarop kennisveiligheid en screening worden vormgegeven. Omdat er weinig bindende nationale kaders bestaan, is de diepgang en consistentie van risicobeoordelingen sterk afhankelijk van individuele onderzoekers en instellingen. Dit vergroot de kans dat risico's ongelijk worden geïdentificeerd en behandeld, en belemmert een uniforme aanpak van risico's omtrent identiteits- en documentfraude en het in kaart brengen van de omvang van deze fraude.

Beperkte zichtbaarheid en effectiviteit van screeningsmechanismen: Hoewel instrumenten zoals KEFs en richtlijnen van organisaties als DFG en KIWi beschikbaar zijn, blijkt dat ze in de praktijk nog beperkt worden toegepast. Onderzoekers zijn niet altijd bekend met deze structuren, en commissies kampen regelmatig met capaciteitsproblemen en beperkte middelen. Hierdoor is de effectiviteit van interne screening en ethische toetsing verschillend per casus, en bestaat het risico dat kennisveiligheidsvraagstukken onvoldoende systematisch worden opgepakt.

Beperkte focus op identiteits- en documentfraude als specifiek risico: Binnen het Duitse beleid ligt de nadruk voornamelijk op bredere kennisveiligheidsrisico's, zoals ongewenste kennisoverdracht en dual-use-onderzoek. Identiteits- en documentfraude wordt minder expliciet geadresseerd als afzonderlijk risico, waardoor specifieke detectie- en verificatiemechanismen wellicht onderontwikkeld blijven. Dit kan ertoe leiden dat fraudevormen die juist gericht zijn op toegang tot instellingen minder goed worden herkend en

aangepakt. Een screening van wetenschappers of studenten waarbij informatie wordt opgevraagd bij relevante veiligheidsdiensten bestaat ook in Duitsland niet op dit moment.

5. Zweden

5.1. Kennisveiligheid: algemene context

De Zweedse regering hanteert het concept verantwoorde internationalisering (*ansvarsfull internationalisering*) bij het bespreken van kennisveiligheid. De *National support function for responsible internationalisation* geeft de volgende definitie:

> 'Verantwoorde internationalisering omvat de aspecten waarmee een nationale actor in het hoger onderwijs, onderzoek en innovatie rekening moet houden om op verantwoorde wijze een relatie met één of meerdere actoren in andere landen tot stand te brengen, in stand te houden en op te volgen'[168]

Deze aanpak wordt ondersteund door een Zweedse visie op kennisveiligheid die in de eerste plaats capaciteitsgericht is, en niet dreigingsgericht. De inspanningen van de Zweedse staat zijn gericht op het versterken van de capaciteit van het onderzoeksecosysteem om problemen aan te pakken zodra deze zich voordoen, in plaats van op het voorkomen van de risico's zelf.[169] Er zijn twee belangrijke structurele drijfveren die de ontwikkeling van de Zweedse aanpak hebben gevormd: de structuur van het Zweedse politieke systeem en het concept professorenvoorrecht (*lärarundantag*) in het Zweedse intellectuele-eigendomsrecht.

De eerste belangrijke structurele drijfveer die de Zweedse aanpak van verantwoorde internationalisering en kennisveiligheid heeft gevormd, is het politieke systeem van het land, dat is gebaseerd op sterke principes van decentralisatie en autonomie. In Zweden genieten overheidsinstanties, waaronder zowel universiteiten als onderzoeksinstellingen, van oudsher een aanzienlijke mate van onafhankelijkheid van directe politieke controle. Hierdoor kan de staat zich niet mengen in de vastgestelde bevoegdheden van specifieke instellingen en mogen instellingen zich ook niet mengen in de bevoegdheden van andere instellingen.[170] Dit systeem is ontworpen om staatsinmenging tot een minimum te beperken en deskundigen en professionals in staat te stellen hun eigen zaken te regelen. In de context van kennisveiligheid betekent dit dat nationale richtlijnen door individuele instellingen worden geïnterpreteerd en geïmplementeerd, in plaats van via strikte, van bovenaf opgelegde mandaten.

De tweede belangrijke factor is het bovengenoemde professorenvoorrecht, een onderscheidend kenmerk van het Zweedse intellectuele-eigendomsrecht. Volgens dit beginsel behouden individuele onderzoekers, en

[168] Swedish Council for Higher Education, Swedish Research Council, & Vinnova (2025).

[169] RAND Europe Interview – 11.

[170] RAND Europe Interview – 9. This rule only operates in peace time.

niet hun universiteiten of werkgevers, de rechten op hun uitvindingen en intellectuele eigendom die voortvloeien uit academisch werk. Dit wettelijke kader versterkt de autonomie van onderzoekers en geeft hen aanzienlijke zeggenschap over de richting, het eigendom en de commercialisering van hun onderzoeksresultaten. Bijgevolg zijn de Zweedse strategieën voor een verantwoorde internationalisatie niet sterk afhankelijk van gecentraliseerde controle of ingrijpende beperkingen, maar richten ze zich in plaats daarvan op adviserende richtlijnen en mechanismen.

Ondanks deze structurele beperkingen heeft de Zweedse regering een reeks beleidsmaatregelen en richtlijnen ingevoerd om verantwoorde internationalisering te bevorderen. Gezien het ontbreken van een gecentraliseerde autoriteit zijn deze in gezamenlijkheid ontwikkeld en worden ze uitgevoerd door een breed scala aan actoren. In het onderstaande kader worden de belangrijkste actoren in het Zweedse ecosysteem voor kennisveiligheid beschreven, waarnaar in deze casestudie zal worden verwezen.

Kader 6. Belangrijkste actoren in het Zweedse ecosysteem voor kennisveiligheid

Overheidsactoren

Onderzoeksfinancieringsinstanties: Er zijn zes primaire financieringsinstanties in Zweden. De meest relevante voor kennisveiligheid zijn de Zweedse Onderzoeksraad (Vetenskapsrådet, SRC), de grootste financier, en Vinnova (Verket för innovationssystem), het Zweedse innovatieagentschap, dat de op één na grootste is. SRC en Vinnova kregen de opdracht om voorstellen voor verantwoorde internationalisering te ontwikkelen.

Instellingen voor hoger onderwijs: Gezien het gedecentraliseerde staatssysteem van Zweden vormen de Instellingen voor hoger onderwijs de primaire doelgroep voor alle nationale inspanningen op het gebied van verantwoorde internationalisering. Zij speelden ook een rol bij de ontwikkeling van een gezamenlijke aanpak: de instellingen voor hoger onderwijs waren vóór 2024 de belangrijkste drijvende kracht achter verantwoorde internationalisering. Dit werd bereikt op individuele basis en via samenwerkingsorganen zoals de Vereniging van Zweedse instellingen voor hoger onderwijs (SUHF) en de Gecoördineerde Beoordeling voor Strategische Internationalisering (CASI).[171]

Ministerie van Onderwijs en Onderzoek (Utbildningsdepartementet**) en het ministerie van Justitie (**Justitiedepartementet**):** Deze ministeries zijn naar internationale maatstaven relatief klein en richten zich voornamelijk op beleidsontwikkeling. De ministeries publiceerden in 2024 witboeken over internationalisering. Hun rol houdt traditioneel op bij het vaststellen van beleid, waarna de uitvoering en activiteiten worden gedelegeerd aan relevante overheidsinstanties.[172]

Zweedse Raad voor Hoger Onderwijs (UHR): Tot de kernactiviteiten van deze instantie behoren het beheer van het nationale toelatingsportaal, het beoordelen en valideren van buitenlandse kwalificaties, en het op verzoek verstrekken van advies over aanvragers aan universiteiten.

Veiligheidsdiensten: Dit is een overkoepelende term die het volgende omvat: de Zweedse Dienst voor Defensiematerieel (FMV), de Zweedse strijdkrachten, de Nationale Inspectiedienst voor Strategische Producten (ISP), de Zweedse Migratiedienst, het Zweedse Agentschap voor Civiele Rampenbestrijding (MSB), de Zweedse Veiligheidsdienst (Säpo) en het Zweedse Agentschap voor Defensieonderzoek (FOI). Deze instanties vervullen, in het kader van verantwoorde internationalisering, voornamelijk een adviserende rol.

Kennisinstellingen en -organisaties

Individuele onderzoekers: Individuele onderzoekers staan in de voorhoede van het Zweedse ecosysteem voor kennisveiligheid en fungeren als uitvoerders en als hoeders van verantwoorde internationalisering. Onderzoekers dragen de verantwoordelijkheid voor het naleven van nationale richtlijnen, beleidsregels en ethische normen met betrekking tot onderzoekssamenwerking.

[171] Swedish Council for Higher Education, Swedish Research Council, & Vinnova (2025).

[172] RAND Europe Interview – 11.

Zweedse Stichting voor Internationale Samenwerking op het gebied van Onderzoek en Hoger Onderwijs (Stiftelsen för internationalisering av högre utbildning och forskning, STINT)**:** Als onafhankelijke actor werkt STINT nauw samen met universiteiten en onderzoeksinstellingen en helpt ze om hun weg te vinden in de complexiteit van internationalisering. Tot haar activiteiten behoren het bieden van begeleiding op het gebied van risicobeheer en capaciteitsopbouw en het verstrekken van financiering, expertise en netwerkmogelijkheden om verantwoorde en strategische internationale partnerschappen te faciliteren.

5.2. Beleid

5.2.1. Vroege ontwikkelingen

In 2019 publiceert de Zweedse regering een regeringsmededeling waarin ze haar aanpak van aangelegenheden met betrekking tot China uiteenzet. In een paragraaf over onderzoek en onderwijs worden weliswaar de voordelen van samenwerking genoemd, maar wordt eveneens een reeks uitdagingen geïdentificeerd, waaronder ethiek, academische vrijheid, bescherming van intellectueel eigendom en mogelijke technologieoverdracht voor militaire doeleinden.[173]

Als reactie op deze uitdagingen wordt in dit document het toenmalige ecosysteem voor kennisveiligheid in Zweden geschetst. Cruciaal is dat de verantwoordelijkheid voor kennisveiligheid in de betrekkingen met China, met inbegrip van het verzamelen van gegevens en het aanpakken van risico's, 'bij de instellingen voor hoger onderwijs en de kennisveiligheid bedrijfswereld ligt'.[174] De Zweedse Stichting voor Internationale Samenwerking op het gebied van Onderzoek en Hoger Onderwijs (STINT) wordt, naast andere instellingen, genoemd vanwege haar rol bij het versterken van de strategieën en inspanningen van de instellingen voor hoger onderwijs. Zelf stuurt ze geen van deze inspanningen aan.

5.2.2. STINT-richtlijnen

In 2020 publiceert STINT *Responsible internationalisation: Guidelines for reflection on international academic collaboration.* Dit document schetst de noodzaak voor het Zweedse onderzoeksecosysteem om een robuuster systeem te ontwikkelen om 'de kansen en risico's van internationale samenwerkingen te identificeren, te beoordelen, aan te pakken en te monitoren'. Net als in de mededeling over China leggen de STINT-richtlijnen de verantwoordelijkheid bij de instellingen voor hoger onderwijs, waarbij wordt opgemerkt dat elke instelling haar eigen aanpak voor verantwoorde internationalisering moet bepalen. Opvallend is dat deze aanbeveling niet dwingend is en dat wordt erkend dat sommige instellingen ervoor zullen kiezen om geen procedures te ontwikkelen.[175]

De STINT-aanbeveling benadrukt de structuur die in 2020 van kracht is: aangestuurd door de instellingen voor hoger onderwijs, met weinig tot geen rol voor overheidsactoren. In de daaropvolgende jaren maakt een reeks opvallende incidenten op het gebied van kennisveiligheid in de media duidelijk dat dit systeem niet geschikt is om de risico's te beheersen die gepaard gaan met verantwoorde internationalisering van onderzoek in de 21e eeuw. Bijgevolg begint de Zweedse regering (via de ministeries van Onderwijs en

[173] Swedish Government (2019).

[174] Swedish Government (2019).

[175] Shih, Albin, & Östlund (2020).

Onderzoek, Defensie en andere) zich actiever te interesseren voor kennisveiligheid en strategische technologiebeveiliging, wat leidt tot meer coördinatie met de Zweedse veiligheidsdienst (Säpo) en financieringsinstanties (zoals Vetenskapsrådet en Vinnova).

5.2.3. Moderne richtlijnen en ondersteunende functie

In 2023 verzoekt de regering de Zweedse Raad voor Hoger Onderwijs (SCHE), de Zweedse Onderzoeksraad (SRC) en Vinnova formeel om robuustere, modernere richtlijnen te ontwikkelen en mechanismen voor te stellen voor kennisuitwisseling tussen instellingen voor hoger onderwijs, financieringsinstanties en de regering.[176] Deze behoefte wordt opnieuw bevestigd in het wetsvoorstel Onderzoek en innovatie voor de toekomst, nieuwsgierigheid en nut uit 2024 (Prop. 2024/25:60), waarin de Zweedse aanpak van onderzoek voor de periode 2025-2028 wordt uiteengezet.[177] Het interim-rapport[178], gepubliceerd in 2024, en het eindrapport[179], gepubliceerd in 2025, vormen de belangrijkste bronnen voor de huidige structuur en ambities van de Zweedse aanpak van verantwoorde internationalisering. Beide rapporten pleiten voor de ontwikkeling van twee afzonderlijke mechanismen: nationale richtlijnen voor verantwoorde internationalisering en een ondersteunende functie voor verantwoorde internationalisering.

Nationale richtlijnen voor verantwoorde internationalisering

De voorgestelde nationale richtlijnen zijn opgesteld met de bedoeling zowel risico's als kansen te verduidelijken, terwijl belanghebbenden voldoende flexibiliteit wordt geboden om zelfstandig in te spelen op nieuwe uitdagingen. Bovendien zijn de richtlijnen ontworpen om afstemming met Zweedse en EU-kaders te waarborgen en om de huidige geopolitieke context te weerspiegelen. De richtlijnen zijn in maart 2026 gepubliceerd onder de naam *En ansvarsfull internationalisering – Vägledande nationella riktlinjer 2026* [Verantwoorde internationalisering – Nationale richtlijnen 2026].[180]

De richtlijnen vormen het centrale onderdeel van de drieledige aanpak van Zweden op het gebied van verantwoorde internationalisering. Op het hoogste niveau staat Prop. 2024/25:60, waarin verantwoorde internationalisering is geïntegreerd in de bredere strategische onderzoeksagenda van Zweden. De nationale richtlijnen bieden een gemeenschappelijk kader voor belangrijke overwegingen bij internationale samenwerking, die op hun beurt weer als basis dienen voor de instellingsspecifieke richtlijnen op het basisniveau. Cruciaal is dat 'de leidende nationale richtlijnen een koers voor verantwoorde internationalisering beschrijven en moeten worden toegepast op een manier die is afgestemd op de specifieke omstandigheden van de organisatie'.[181]

De richtlijnen zijn bewust breed geformuleerd, vanuit de veronderstelling dat instellingen voor hoger onderwijs deze zullen aanpassen en afstemmen op hun specifieke omstandigheden. Na de publicatie zijn de

[176] Swedish Ministry of Education and Research (2023).

[177] Swedish Ministry of Climate and Enterprise & Ministry of Education and Research (2024).

[178] Swedish Council for Higher Education, Swedish Research Council, & Vinnova (2024).

[179] Swedish Council for Higher Education, Swedish Research Council, & Vinnova (2025).

[180] Swedish Research Council & Vinnova (2026).

[181] Swedish Research Council & Vinnova (2026).

meeste universiteiten begonnen met het ontwikkelen van hun eigen implementatiestrategieën.[182] Er is al sprake van een merkbare acceptatie en verwacht wordt dat de meerderheid van de instellingen voor hoger onderwijs tegen het einde van het jaar eigen richtlijnen zal hebben vastgesteld. Er zijn ambities geformuleerd om toekomstige herzieningen van de nationale richtlijnen te baseren op de ervaringen en praktijken die op institutioneel niveau zijn ontwikkeld.[183]

Gedurende het hele ontwikkelingsproces speelden de instellingen voor hoger onderwijs een centrale rol bij het bepleiten van een algemeen karakter van de richtlijnen. Er werd overeengekomen dat de toepassing van instrumenten zoals risicobeoordelingen op institutioneel niveau moest worden geregeld en niet op nationaal niveau. Er werd echter ook opgemerkt dat wanneer er gemeenschappelijke zorgen of behoefte aan gedeelde instrumenten ontstaan, deze kunnen worden opgenomen in volgende edities van de nationale richtlijnen.[184]

Er was aanvankelijk weerstand tegen de richtlijnen vanuit de Zweedse Vereniging van Universitaire Docenten en Onderzoekers (SULF), voornamelijk vanwege bezorgdheid over staatsinmenging in de autonomie van de universiteiten.[185]

Ondersteunende functie voor verantwoorde internationalisering

Het eindrapport van 2025 schetst tevens de ontwikkeling van een mechanisme dat hopelijk een succesvolle implementatie van de richtlijnen in de toekomst mogelijk zal maken. Er staat: 'Vanaf 2025 zal een nationale ondersteuningsfunctie voor verantwoorde internationalisering worden ingesteld.'[186] Cruciaal is dat, in tegenstelling tot de richtlijnen, de ondersteuningsfunctie op het moment van schrijven (mei 2026) nog niet door de regering is goedgekeurd. Toch is het de moeite waard om het voorgestelde systeem te beschrijven, omdat het nog steeds kan worden geïmplementeerd.

De voorgestelde ondersteuningsfunctie zal worden georganiseerd volgens een interactief model, waarbij verschillende instanties gezamenlijk belast zijn met het opzetten en beheren van de ondersteuningsfunctie. Eén van de instanties krijgt de taak om leiding te geven aan de werkzaamheden van het bureau van de ondersteuningsfunctie en fungeert als de geregistreerde organisatorische zetel ervan. Relevante overheidsinstanties met kennis en bevoegdheden op het gebied van civiele bescherming, sancties, veiligheid en defensie moeten worden belast met het bijstaan van de ondersteuningsfunctie bij veiligheidskwesties die niet duidelijk onder de bevoegdheid van een van de afzonderlijke instanties vallen. De ondersteuningsfunctie moet een startfinanciering van 7 miljoen Zweedse kronen (SEK) per jaar ontvangen om de oprichting en werking ervan te dekken. Na drie jaar moet een grondige evaluatie van de activiteiten van de ondersteuningsfunctie worden uitgevoerd.

Bij de ontwikkeling van het mechanisme voor de nationale ondersteuningsfunctie is inspiratie geput uit bestaande modellen, zoals het Nederlandse Loket Kennisveiligheid en het Research Collaboration Advice Team (RCAT) in het Verenigd Koninkrijk.[187] Uit overleg met Zweedse universiteiten bleek echter dat er

[182] RAND Europe Interview – 11.

[183] RAND Europe Interview – 11.

[184] RAND Europe Interview – 11.

[185] Myklebust (2024).

[186] Swedish Council for Higher Education, Swedish Research Council, & Vinnova (2025).

[187] RAND Europe Interview – 11.

weinig enthousiasme bestond voor de oprichting van een soortgelijke ondersteuningsfunctie. De belangrijkste reden voor deze terughoudendheid was dat, hoewel veiligheidskwesties een belangrijk punt blijven en universiteiten de noodzaak van ondersteuning op dit gebied erkennen, zij er de voorkeur aan geven zaken die verband houden met ernstige kennisveiligheid, zoals exportcontroles, rechtstreeks met de relevante veiligheidsinstanties af te handelen. Bijgevolg is de beoogde ondersteuningsfunctie ontworpen om kwesties aan te pakken die zich binnen de zogenoemde grijze zone voordoen, met name de zaken die buiten het werkterrein van gevestigde veiligheidsdiensten vallen en daarom gecoördineerde hulp van meerdere instanties vereisen.[188]

5.3. Document- en identiteitsfraude

Zweden maakt gebruik van een gecentraliseerd aanmeldingssysteem voor het hoger onderwijs – iedereen die zich wil aanmelden voor een bachelor- of masteropleiding moet dit doen via een portaal dat wordt beheerd door de Zweedse Raad voor Hoger Onderwijs (UHR). De UHR vervult een adviserende rol en biedt referentiezaken en contactpunten aan, maar alle individuele universiteiten en hogescholen nemen hun eigen beslissingen over de toelatingen. Bijgevolg is het ook de verantwoordelijkheid van de instellingen voor hoger onderwijs om kwalificaties te controleren, frauduleuze gevallen te identificeren en aanvragers in die gevallen te screenen.[189]

Volgens een geïnterviewde is het aantal gemelde fraudegevallen bij academische toelatingen via het UHR-portaal aanzienlijk gestegen, van 30 in 2024 tot 130 in 2025.[190] Dit werd grotendeels toegeschreven aan het gebruik van AI-agenten uit landen als Pakistan, Nigeria en Bangladesh.[191] Vanwege de AVG-regelgeving bestaat er binnen de Zweedse overheid echter terughoudendheid om gegevens extern tussen verschillende instanties te delen. Soms kan informatie zelfs niet intern worden gedeeld tussen afdelingen binnen een specifieke instantie, bijvoorbeeld wanneer bij de toelating blijkt dat iemand valse referenties heeft opgegeven.[192] UHR is het door Zweden aangewezen ENIC-NARIC-bureau, dat verantwoordelijk is voor de erkenning van diploma's en onderwijskwalificaties met het oog op de arbeidsmarkt. Aanvragen die vervalste documenten bevatten, worden afgewezen en worden bij de politie gemeld. UHR biedt ook een aanmeldingssysteem voor de gezamenlijke toelatingsprocedure, dat wil zeggen erkenning met het oog op vervolgstudies, maar de gegevens in het systeem zijn eigendom van de universiteiten en hogescholen. Om redenen van gegevensbescherming is het delen van informatie tussen de twee procedures verboden, zelfs wanneer een persoon voor beide doeleinden een aanvraag heeft ingediend.[193]

Deze verantwoordelijkheid is nog sterker geconcentreerd bij aanvragen voor een doctoraat, waarbij aanvragers zich rechtstreeks aanmelden bij de instelling en individuele laboratoria en onderzoekers verantwoordelijk zijn voor de beslissing over de aanvraag. In deze gevallen speelt de UHR geen rol, evenmin

[188] RAND Europe Interview – 11.
[189] RAND Europe Interview – 14.
[190] RAND Europe Interview – 14.
[191] RAND Europe Interview – 14.
[192] RAND Europe Interview – 14.
[193] RAND Europe Interview – 14.

als enige andere overheidsinstantie. Er bestaat geen verplichting voor instellingen voor hoger onderwijs om deze gegevens te rapporteren, waardoor de UHR geen inzicht had in eventuele fraudecijfers op het niveau van de instellingen voor hoger onderwijs.[194] Uit interviews blijkt dat kandidaten met vervalste diploma's van diplomafabrieken, instanties en personen die zich bezighouden met de verkoop van diploma's en academische graden zonder dat er een studieprogramma is gevolgd[195], zijn toegelaten tot PhD-programma's, wat de ernst van de kwestie onderstreept.

Andere geïnterviewden bevestigen dat er op het niveau van de instellingen voor hoger onderwijs weinig tot geen documentcontroles plaatsvinden. Bij KTH, een van de instellingen voor hoger onderwijs in Zweden die vooroplopen op het gebied van verantwoorde internationalisering, ligt de nadruk sterk op veiligheid. Dit blijkt uit de aanwezigheid van 16 gespecialiseerde medewerkers die zich bezighouden met veiligheid, en een werkgroep voor verantwoorde internationalisering waaraan meerdere seniorbestuurders om de twee weken deelnemen.[196] Er wordt echter benadrukt dat KTH en andere instellingen voor hoger onderwijs op het gebied van kennisveiligheid voornamelijk een adviserende rol vervullen, aangezien zij structureel beperkt zijn in de omvang van hun onderzoeksbevoegdheden.[197] Bij KTH zijn identiteitscontroles van studenten niet toegestaan, en ook identiteitscontroles van docenten worden sterk beperkt door de Zweedse wetgeving.[198] Hierdoor is de enige belangrijke controle op instellingsniveau de beoordeling van cv's en vindt alleen plaats als een situatie om andere redenen onder de aandacht van de adviesgroep is gebracht.[199] Het is essentieel om te benadrukken dat KTH waarschijnlijk een van de meest, zo niet de meest, robuuste benaderingen van verantwoorde internationalisering vertegenwoordigt onder Zweedse instellingen voor hoger onderwijs. Het instituut wordt in andere interviews genoemd als een voorbeeld van de beste praktijken.[200] Bijgevolg is het een bevinding van dit rapport dat er geen bestaande gegevens of bewijsbasis zijn die documentfraude in verband met kennisveiligheid in Zweden bijhouden.

Het Zweedse systeem controleert documenten echter wel, zij het net buiten het traditionele directe toepassingsgebied van verantwoorde internationalisering. Twee belangrijke aspecten worden geïdentificeerd die relevant zijn voor de kennisveiligheid.

Ten eerste is de UHR weliswaar niet direct betrokken bij toelatingsbeslissingen van universiteiten, maar fungeert deze wel als beoordelaar van diploma's voor buitenlanders die in Zweden willen werken. UHR beoordeelt buitenlandse documenten op basis van drie hoofdcriteria:

1. Is het document afkomstig van een authentieke en geloofwaardige instelling?
2. Zijn de diploma's zelf echt?
3. Is de aanvrager de rechtmatige eigenaar van de overgelegde diploma's?

---

[194] RAND Europe Interview – 14.

[195] Nederlands-Vlaamse Accreditatieorganisatie (NVAO).

[196] RAND Europe Interview – 9.

[197] Dit komt door de opzet van het Zweedse politieke stelsel en het 'professorenvoorrecht', die beide in paragraaf 5.1 worden toegelicht.

[198] RAND Europe Interview – 9.

[199] RAND Europe Interview – 9.

[200] RAND Europe Interview – 11.

Aan alle criteria moet worden voldaan voor validatie, maar elk criterium vertoont specifieke kwetsbaarheden voor fraude, namelijk diplomafabrieken, valse diploma's en valse identiteiten. Met name diplomafabrieken vormen een groeiende uitdaging. Het is vaak gemakkelijker om te bevestigen dat een instelling geen diplomafabriek is dan om te bewijzen dat ze er wel een is. Diplomafabrieken worden in verband gebracht met economische criminaliteit en vormen een bredere maatschappelijke bedreiging, aangezien ze aanzienlijke inkomsten genereren voor criminele actoren.[201] Identiteitsverificatie is ook moeilijk, aangezien onderwijzend personeel vaak onvoldoende is opgeleid om vervalste identiteiten te herkennen. Hoewel deze beoordelingen niet direct verband houden met het hoger onderwijs, bieden ze wel een preventieve screening van buitenlandse staatsactoren die in het Zweedse bedrijfsleven willen werken, wat weer kan worden teruggekoppeld naar kennisveiligheid bij het overwegen van technologiecommercialisering.

Ten tweede beoordeelt de Zweedse Migratiedienst visumaanvragen van buitenlanders zodra zij als student of docent zijn toegelaten tot een instelling voor hoger onderwijs.[202] Indien er een risico wordt vastgesteld – meestal op basis van de contacten van de individuele onderzoeker of het onderzoeksgebied – kunnen visumzaken worden doorverwezen naar de Zweedse veiligheidsdiensten. Dit proces van visumbeoordeling en doorverwijzing geldt voor alle buitenlandse aanvragen om Zweden binnen te komen en is geworteld in het bredere migratie- en nationale veiligheidsbeleid van het land, niet in academische of onderzoeksspecifieke overwegingen. Hoewel het systeem dus parallel loopt aan de kennisveiligheid, is het strikt genomen geen mechanisme voor kennisveiligheid; het primaire doel ervan is de Zweedse grenzen te bewaken en bedreigingen voor de nationale belangen af te wenden.

5.4. Bevindingen en conclusies

De Zweedse aanpak van verantwoorde internationalisering en kennisveiligheid wordt gekenmerkt door een evenwicht tussen nationale richtlijnen en institutionele autonomie, sterke adviserende ondersteuning en een op capaciteiten gericht ethos. Toch leidt deze decentralisatie tot inconsistenties en hiaten in de opsporing van fraude, terwijl wettelijke beperkingen en beperkingen op het gebied van gegevensuitwisseling een effectief systeemoverschrijdend risicobeheer verder belemmeren. In de zich ontwikkelende nationale richtlijnen en ondersteunende functies van Zweden wordt rekening gehouden met deze uitdagingen, maar er is nog veel werk te doen om te komen tot een geharmoniseerde, veerkrachtige nationale kennisveiligheidspositie.

Relevant beleid en procedures

Geïnstitutionaliseerd mechanisme voor buitenlandse documenten: De UHR fungeert als nationaal knooppunt voor het screenen en valideren van buitenlandse academische diploma's, hoewel dit voornamelijk voor visumdoeleinden is bedoeld. De centralisatie van dit proces waarborgt een mate van consistentie en nauwkeurigheid die moeilijk te bereiken zou zijn als het screenen van diploma's volledig aan individuele instellingen zou worden overgelaten. De UHR bouwt bovendien expertise op waar andere instellingen een beroep op kunnen doen.

[201] RAND Europe Interview – 14.

[202] RAND Europe Interview – 9.

Adviesmechanismen: De Zweedse aanpak van verantwoorde internationalisering leunt sterk op het gebruik van advieskanalen. Zo kan de Zweedse Migratiedienst, indien gewenst, aanvragen voor studentenvisa doorverwijzen naar de veiligheidsdiensten. Er zijn geen strikte vereisten om dit proces in gang te kunnen zetten, het kan bijvoorbeeld gebaseerd zijn op nationaliteit of onderzoeksgebied, en als de beoordelaar van mening is dat er aanvullende, niet-openbare informatie nodig is, kan hij of zij de zaak escaleren. De UHR vervult een vergelijkbare rol via het beheer van het portaal voor het hoger onderwijs. Hoewel de UHR geen directe verantwoordelijkheid draagt voor het beoordelen van documenten van aanvragers, kan zij op verzoek advies verstrekken aan instellingen voor hoger onderwijs, wat zeer waardevol is gezien de hierboven besproken expertise op het gebied van de validatie van buitenlandse documenten.

Zoals uiteengezet in recente overheidsrapporten, zijn er plannen om deze adviesfuncties verder te consolideren en te stroomlijnen door de oprichting van een nationaal ondersteuningsmechanisme voor verantwoorde internationalisering. Dit voorgestelde ondersteuningsbureau zal relevante instanties en expertise samenbrengen en zich bezighouden met gevallen in de grijze zone die buiten de strikte mandaten van individuele instanties of veiligheidsdiensten vallen.

Bestaande beperkingen

Structurele belemmeringen voor toezicht: De grootste uitdaging voor verantwoorde internationalisering in Zweden vloeit voort uit het diepgewortelde structurele en juridische kader. De onafhankelijkheid van overheidsdepartementen, in combinatie met het professorenvoorrecht dat onderzoekers eigendom van intellectueel eigendom toekent, beperkt de ruimte voor gecentraliseerde beleidsinterventies die verder gaan dan algemene adviesrichtlijnen. Hierdoor ligt de verantwoordelijkheid voor kennisveiligheid grotendeels bij individuele onderzoekers en instellingen voor hoger onderwijs. Deze autonomie leidt tot sterk uiteenlopende praktijken en procedures binnen de sector. Sommige instellingen, met name kleinere of instellingen met minder middelen, geven mogelijk onvoldoende prioriteit aan verantwoorde internationalisering of beschikken niet over de capaciteit om robuuste veiligheidsmaatregelen te ontwikkelen, wat leidt tot een ongelijkmatige nationale bescherming. Deze belemmeringen bestaan ook op horizontaal niveau tussen verschillende overheidsinstanties: beperkingen op het delen van gegevens binnen en tussen instanties als gevolg van de Zweedse AVG en gefragmenteerde communicatie belemmeren de ontwikkeling van best practices buiten individuele actoren om. Deze systeemzwakheden worden nog duidelijker wanneer we kijken naar fraude. Hoewel de UHR centraal toezicht uitoefent op de toelating tot bachelor- en masteropleidingen, ligt de verantwoordelijkheid voor het screenen van promovendi en de aanwerving van docenten vrijwel volledig bij de afzonderlijke instellingen, met minimale vereisten of capaciteit voor document- of identiteitscontroles. Er zijn op nationaal niveau weinig tot geen geaggregeerde gegevens over onderzoeksgerelateerde fraude, en het veelvuldig voorkomen van diplomafabrieken en frauduleuze diploma's benadrukt de bestaande kwetsbaarheden in het systeem.

6. Het Verenigd Koninkrijk en Frankrijk

Dit hoofdstuk biedt een beknopt overzicht van het beleid en de screeningsmechanismen in het Verenigd Koninkrijk en Frankrijk. Net als Zweden, Australië en Duitsland zijn deze landen actief op het terrein van kennisveiligheid. De Nederlandse overheid onderhoudt intensieve banden met de twee landen, waardoor al een goed inzicht bestaat in hun relevante wet- en regelgeving. Om die reden is in deze studie besloten deze landen niet als volwaardige casestudies te onderzoeken. Toch kunnen enkele waardevolle lessen uit hun aanpak worden getrokken en daarom worden zij in dit hoofdstuk summier behandeld.

6.1. Het Verenigd Koninkrijk

In het Verenigd Koninkrijk is het Department of Business, Innovation, Science and Trade (DBIST) verantwoordelijk voor het beleid rondom kennisveiligheid. Dit ministerie vervult een coördinerende rol. Onder dit departement valt het Research Collaboration Advice Team (RCAT), een organisatie die enigszins vergelijkbaar is met het Nederlandse Loket Kennisveiligheid, maar dan op een meer gedecentraliseerde manier. RCAT werkt met accounthouders binnen verschillende kennisinstellingen, die als aanspreekpunt fungeren voor vragen over kennisveiligheid en direct contact onderhouden met het ministerie. De accounthouders hebben een goed overzicht van internationale samenwerkingen binnen hun instelling. Door deze persoonlijke benadering kunnen accounthouders proactief signaleren wanneer sprake is van potentieel gevoelig onderzoek. In Nederland is er geen centraal landelijk overzicht, mede door de institutionele autonomie: instellingen bepalen zelf met wie ze samenwerken. Kennisveiligheidscoördinatoren hebben wel zicht op samenwerkingen binnen hun eigen instelling. De anonimiteit bij het Nederlandse Loket volgt uit de verantwoordelijkheidsverdeling: de overheid adviseert, maar de instelling beslist zelf over samenwerkingen.[203]

Naast het accounthoudersysteem kent het Verenigd Koninkrijk een screeningsmechanisme genaamd ATAS (Academic Technology Approval Scheme), dat zich specifiek richt op massavernietigingswapens en dual-use-onderzoek. ATAS is primair bedoeld voor counterproliferatie en verwerkte in 2025 circa 30.000 aanvragen. In 2007 waren het er een paar duizend, dus dit aantal is sterk gegroeid in de afgelopen jaren. Slechts een klein percentage aanvragen wordt afgewezen. Tegen een afwijzing kan procedureel (niet inhoudelijk) beroep worden aangetekend, maar dit gebeurt zelden. Het Britse beleid is landneutraal en

[203] RAND Europe Interview – 2.

gebaseerd op een risicomodel, waarbij risico's worden afgewogen tegen de baten. De exacte criteria voor deze risicoafweging zijn niet openbaar.[204]

Binnen ATAS wordt niet alleen gekeken naar de inhoud van de aanvraag, maar ook naar mogelijke omissies, zoals hiaten in het cv. De aangeleverde documenten worden vergeleken met open-source-informatie, en als bepaalde zaken niet worden genoemd, kan dit aanleiding zijn voor verder onderzoek. De screening kent een escalatieladder: eenvoudige gevallen worden door een frontoffice afgehandeld en krijgen snel groen licht, terwijl twijfelgevallen worden doorgestuurd naar een team met meer technische expertise. In complexe situaties wordt ook gekeken naar de risico's rondom de persoon en kan er contact zijn met inlichtingen- of veiligheidsdiensten. Er wordt beoordeeld of risico's geaccepteerd of gemitigeerd kunnen worden, waarbij elk geval als eenvoudig, complex of twijfelachtig wordt geclassificeerd.[205]

Om de scope van de screening te bepalen, wordt gebruikgemaakt van het subjectcodesysteem, waarmee sensitieve vakgebieden worden aangewezen. Hiervoor wordt samengewerkt met de Russell Group, een koepelorganisatie van universiteiten die zich richten op STEM-disciplines. Deze groep levert input over welke vakgebieden relevant zijn, hoewel het door de snelle ontwikkelingen binnen de wetenschap lastig is om dit nauwkeurig te definiëren.[206]

Het Britse systeem biedt enkele nuttige best practices, zoals de sterke nadruk op technische expertise en duiding. Dit is essentieel, omdat ambtenaren vaak niet over de benodigde kennis van sensitieve vakgebieden beschikken. Het is belangrijk om experts te hebben die inzicht hebben in de risico's en die hun kennis voortdurend bijhouden, gezien de snelle veranderingen binnen de wetenschap.[207]

6.2. Frankrijk

In Frankrijk wordt het beleid rondom kennisveiligheid aangeduid als PPST (Protection du potentiel scientifique et technique de la Nation), dat zich richt op de bescherming van het wetenschappelijke en technische potentieel van het land. Dit beleid is minder breed dan de Nederlandse interpretatie van kennisveiligheid, aangezien het zich niet richt op wetenschappelijke integriteit. Het PPST-systeem bestaat al aanzienlijk langer dan het Nederlandse systeem en vindt zijn oorsprong in de bescherming van nucleaire wapens en de defensie-industrie.[208] De coördinatie van het PPST-beleid is centraal belegd bij het Franse Algemeen Secretariaat voor Defensie en Nationale Veiligheid (SGDSN). De uitvoering vindt plaats door ambtenaren op het gebied van defensie en veiligheid (HFDS) op zes ministeries en door ambtenaren op het gebied van defensie en veiligheid (FSD's) die werkzaam zijn binnen kennisinstellingen, maar wel via een officieel besluit benoemd worden door de minister. Het mechanisme stelt HFDS in staat om adviezen te geven over internationale samenwerkingen op wetenschappelijk en technisch gebied. Dit gebeurt, omdat het wettelijk verplicht is om internationale samenwerkingen ter goedkeuring voor te leggen aan het

[204] RAND Europe Interview – 2.

[205] RAND Europe Interview – 2.

[206] RAND Europe Interview – 2.

[207] RAND Europe Interview – 2.

[208] RAND Europe Interview – 2.

ministerie van Hoger Onderwijs en Onderzoek.[209] Opvallend is dat de scope van het Franse beleid zowel publieke als private sectoren omvat, wat een belangrijk verschil is ten opzichte van andere landen.[210]

Het PPST-beleid richt zich primair op het beschermen van het wetenschappelijke en technische potentieel door de toegang tot gevoelige kennis te beperken. Dit beleid maakt geen onderscheid naar nationaliteit van betrokkenen en richt zich met name op fysieke ruimtes en laboratoria waar sensitief onderzoek plaatsvindt, de zogenaamde ZRR (zones à régime restrictif). Toegang tot deze zones wordt zowel fysiek als digitaal beperkt. De screening is dan ook gericht op het al dan niet verkrijgen van toegang tot deze zones. Er bestaat een online overzicht van sensitieve onderzoeksgebieden binnen het PPST-kader, op basis waarvan ZRR's worden aangewezen. Dit overzicht, oorspronkelijk uit 2011-2012, is in 2024-2025 geactualiseerd, met toevoeging van onder andere sociale wetenschappen en artificial intelligence. Het beleid richt zich vooral op technologische disciplines met dual-use-toepassingen, maar andere vakgebieden kunnen ook onder het PPST-kader vallen. De drempel voor toepassing is hoog: het PPST-kader wordt alleen ingezet bij aanzienlijke risico's dat kennis en knowhow in handen van derden kunnen vallen.[211] Ongeveer zestig procent van de screenings valt onder het ministerie van Hoger Onderwijs en Onderzoek, maar er zijn teams binnen meerdere ministeries die zich met het PPST-beleid bezighouden.[212]

Elke kennisinstelling beschikt over een FSD, wat in Frankrijk een vertrouwelijke functie is, waardoor zij veel meer kunnen dan de kennisveiligheidscoördinatoren in Nederland. In Frankrijk worden deze ambtelijke coördinatoren door de instelling voorgedragen en vervolgens officieel benoemd door de premier. Zij worden centraal aangestuurd door het ministerie van Hoger Onderwijs en Onderzoek. De screeningsprocedure start wanneer iemand een verzoek indient om toegang te krijgen tot een ZRR of laboratorium. De instelling stelt een dossier samen met informatie over het onderzoeksproject, het contract, de duur en het type financiering. Dit dossier wordt eerst goedgekeurd door de directeur van het laboratorium. Vervolgens voert de FSD een eerste screening uit en stuurt het dossier door naar het ministerie, waar de officiële screening plaatsvindt. De inlichtingendiensten worden standaard betrokken, maar de meeste kandidaten krijgen groen licht. Alleen bij risico's, zoals een relevante (criminele) geschiedenis of bepaalde affiliaties, kan het advies negatief uitvallen. In complexe gevallen worden ook wetenschappelijke experts geraadpleegd. In Frankrijk hebben onderzoekers de status van ambtenaar, wat de samenwerking met de ambtenaren bij overheidsinstellingen vergemakkelijkt.[213]

Het ministerie neemt de uiteindelijke beslissing door te toetsen op vier potentiële doelen van de toe-eigening of het misbruik van kennis, expertise of technologieën van openbare en particuliere instellingen op Frans grondgebied:

1. Het schaden van de economische en wetenschappelijke belangen van de natie;

[209] Ministère de l'Enseignement supérieur, de la Recherche et de l'Espace (2016).

[210] RAND Europe Interview – 2.

[211] Office français de l'intégrité scientifique (2026).

[212] RAND Europe Interview – 2.

[213] RAND Europe Interview – 2.

2. Het versterken van de militaire capaciteiten van andere landen of het verzwakken van de Franse defensiecapaciteiten;
3. Het bijdragen aan de verspreiding van massavernietigingswapens en hun draagraketten; en
4. Het gebruik voor terroristische doeleinden op het nationale grondgebied of in het buitenland.[214]

De beoordeling is gebaseerd op een kosten-batenanalyse, waarbij de precieze afweging niet openbaar is. De uitkomst van de screening is bindend: bij toestemming kan een instelling alsnog besluiten geen toegang te verlenen, maar bij afwijzing is toegang definitief uitgesloten.[215]

De Franse aanpak verschilt van de Nederlandse, doordat Frankrijk zich primair richt op fysieke ruimtes, waardoor alles wat binnen die ruimte gebeurt als veilig wordt beschouwd. Nederland richt zich meer op vakgebieden, wat betekent dat toegang mogelijk blijft voor activiteiten die net buiten een gescreend vakgebied vallen. Naast screening zet Frankrijk ook in op bewustwording rondom kennisveiligheid. Een belangrijke les uit het Franse systeem is het belang van technische expertise en duiding.[216]

[214] SGDSN (2025).

[215] RAND Europe Interview – 2.

[216] RAND Europe Interview – 2.

7. Conclusies en lessen voor Nederland

In dit slothoofdstuk beantwoorden we de onderzoeksvragen aan de hand van de eerdere hoofdstukken. Vervolgens gaan we in op de lessen voor Nederland en bespreken we welke waarborgen kunnen worden gecreëerd om de diverse vormen van fraude te bestrijden ten behoeve van onze kennisveiligheid.

Vergelijking casestudielanden

Uit de casestudies blijkt dat er tussen de onderzochte landen onderling aanzienlijke verschillen bestaan in hoe het kennisveiligheidsbeleid wordt vormgegeven. Het ene land hanteert bijvoorbeeld een uitgesproken top-downbenadering (Australië), waar anderen meer bottom-up gericht zijn (Duitsland). De oorsprong en inrichting van het beleid is veelal gedreven door hun historische context. Tabel 3 vat de situatie kort samen per land.

Tabel 3. Vergelijking van de casestudies, aangevuld met het Verenigd Koninkrijk en Frankrijk

Land	Beleid	Screening	Verantwoordelijke organisaties
Nederland	Leidraad Kennisveiligheid	Screening vindt plaats door kennisinstellingen, centraal Loket als adviespunt	Verantwoordelijkheid op het niveau van de instelling voor hoger onderwijs en de onderzoeker
Australië	ARC Act 2001; ARC Framework; PACT Regulations	Gecentraliseerd screeningsproces voor visa en beurzen, dit geldt voor technologieën uit de *List of Critical Technologies in the National Interest*; communicatie tussen instellingen voor hoger onderwijs	Department of Education, Department of Home Affairs, veiligheidsdiensten
Duitsland	Geen. Nieuw beleid in ontwikkeling	Sterk gedecentraliseerd op niveau van kennisinstellingen	Verantwoordelijkheid op het niveau van de instelling voor hoger onderwijs en de onderzoeker
Zweden	*En ansvarsfull internationalisering – Vägledande nationella riktlinjer 2026; Prop. 2024/25:60*	Screening die voornamelijk door instellingen voor hoger onderwijs wordt uitgevoerd, en een gecentraliseerd systeem voor de beoordeling van diploma's van studenten	Verantwoordelijkheid op het niveau van de instelling voor hoger onderwijs en de onderzoeker

Land	Beleid	Screening	Verantwoordelijke organisaties
Verenigd Koninkrijk	Trusted research and innovation	Gecentraliseerd screeningsmechanisme gericht op massavernietigingswapens en dual-use-onderzoek, hier wordt gebruikgemaakt van het subject code-systeem, waarmee sensitieve vakgebieden worden aangewezen. Overige screening op niveau kennisinstellingen	Department of Science, Innovation & Technology (beleid), RCAT (advies), ATAS (gecentraliseerde screening), universiteiten (overige screening)
Frankrijk	Protection du potentiel scientifique et technique	Gecentraliseerde screening gericht op fysieke ruimtes en laboratoria waar sensitief onderzoek plaatsvindt, dit gaat om disciplines met technologische toepassingen, met name dual-use-doeleinden	SGDSN (coördinatie), HFDS/FSD (uitvoering), Ministeries (beleid), kennisinstellingen

Wat is bekend over de wijze waarop identiteits- en documentatiefraude wordt gepleegd om toegang te krijgen tot kennisinstellingen in Nederland en daarbuiten?

Informatie over fraude met betrekking tot kennisveiligheid in Nederland wordt niet centraal geregistreerd of geanalyseerd. De verschillende actoren in deze gefaseerde aanpak zijn slechts in staat om een deel van het fraudebeeld te schetsen. In de interviews komen verschillende modus operandi van fraude aan bod. Wat het Loket Kennisveiligheid regelmatig hoort van kennisinstellingen, is dat informatie over bijvoorbeeld defensiegerelateerde banden soms bewust wordt weggelaten uit cv's. Dit gebeurt mede door de toegenomen aandacht voor kennisveiligheid en het groeiende bewustzijn bij kennisinstellingen van de risico's die bepaalde connecties met zich meebrengen. Waar dergelijke banden voorheen als prestigieus werden gezien, zijn instellingen zich nu meer bewust van de mogelijke risico's en de rol van statelijke actoren. Het achterhouden van dergelijke informatie is een bekende werkwijze, maar het Loket is niet verantwoordelijk voor de controle hierop; wel geeft het hierover voorlichting. De voornaamste kwetsbaarheid ligt kortom niet noodzakelijkerwijs in klassieke vervalsing van documenten, maar in strategische misrepresentatie en omissies. Dergelijke vormen van fraude zijn moeilijker te detecteren met traditionele documentcontroles en vragen om een bredere, contextuele risicobeoordeling.

Nuffic adviseert Nederlandse kennisinstellingen over de waardering van buitenlandse diploma's en verstrekt jaarlijks circa 30.000 niet-bindende adviezen. Daarbij controleert Nuffic de authenticiteit en erkenning door de bevoegde autoriteit en beoordeelt bijbehorende documenten zoals cijferlijsten. Door te kijken of het gehele opleidingstraject logisch en consistent is verlopen, kan Nuffic mogelijke fraude opsporen. De controle vindt doorgaans plaats op basis van kopieën (waaronder scans of fotobestanden), omdat buitenlandse studenten zich vaak nog niet in Nederland bevinden en geen originele documenten kunnen overleggen. Doordat gebruikgemaakt wordt van kopieën, kan het lastiger zijn om fraude vast te stellen, zeker als er sprake is van fraude waarbij statelijke actoren betrokken zijn. Nuffic signaleert dat fraude met diploma's vaker voorkomt uit bepaalde landen, maar onderzoekt niet expliciet of er een link is met kennisveiligheid. Fraude wordt opgespoord door te letten op inconsistenties in documenten of onlogische onderwijsloopbanen. Daarnaast bestaan er bekende diploma mills waar valse diploma's kunnen worden

besteld; informatie hierover wordt gedeeld binnen het internationale netwerk van Nuffic, waardoor deze gevallen snel kunnen worden herkend en aangepakt.

In Australië zijn regelgevingsmechanismen zoals de PACT-voorschriften en het ARC-kader ontworpen om grondige controles van documenten en bewijsstukken uit te voeren. Echter ligt hun primaire focus niet op het opsporen van fraude en het verifiëren van de authenticiteit van documenten zoals identiteitsbewijzen en diploma's, maar veeleer op het identificeren van potentiële risico's.

Uit interviews met Australische experts komt naar voren dat het geven van onjuiste informatie de belangrijkste vorm van fraude is die in Australië wordt aangetroffen, met name in cv's en subsidieaanvragen. Een van de meest zorgwekkende trends die zich de afgelopen twaalf tot achttien maanden heeft afgetekend, is het opzettelijk achterhouden van de herkomst van studiebeurzen. Er is sprake van een toenemende, systematische verkeerde voorstelling van financiering en van gevallen waarin personen opzettelijk banden vermelden met instellingen met een lager risico in plaats van hun banden met de daadwerkelijke (en mogelijk risicovollere) organisaties verzwijgen. Op cv's laten personen vaak bepaalde banen of stages weg in de officiële versies die zij indienen, en bewaren zij de volledige details voor cv's die privé worden gedeeld. Hetzelfde patroon is waarneembaar bij onderzoeksresultaten: onderzoek zonder dual use wordt openbaar gemaakt, terwijl militair gerelateerd onderzoek wordt verborgen. Bovendien worden affiliaties met organisaties vaak niet vertaald, waardoor hun werkelijke betekenis nog verder wordt achtergehouden. Een andere vastgestelde vorm van fraude betreft valse uitnodigingsbrieven voor visumdoeleinden. Vaak worden gevallen gesignaleerd door andere instellingen voor hoger onderwijs, die contact opnemen om te bevestigen dat een uitnodiging authentiek is. Deze informatie-uitwisseling wordt mogelijk gemaakt door het Australische Informal Foreign Interference Network (INFIN), een niet-gouvernementele organisatie van 39 Australische instellingen voor hoger onderwijs die gezamenlijk de inspanningen tegen ongewenste inmenging en de naleving van overheidsvoorschriften bespreken.

In Duitsland ligt de verantwoordelijkheid voor screening bij de onderzoekers en universiteiten zelf. De wettelijke verplichtingen beperken zich tot exportcontroles op militaire en dual-use-technologieën. Instellingen moeten zelf informatie verzamelen over veiligheidsrelevante aspecten, vaak met behulp van externe bronnen zoals de ASPI-tracker, die echter beperkte en soms onduidelijke informatie bieden. De Duitse binnenlandse veiligheidsdienst (BfV) geeft wel een overzicht van methoden die risicovolle landen inzetten om gevoelige technologieën en kennis te vergaren, waarbij het ontwijken van export- en kenniscontrole door misleidende informatie in aanvragen te verwerken direct relevant is voor kennisveiligheid en overeenkomt met trends in andere landen. Of deze methoden van identiteits- en documentfraude in Duitsland ook daadwerkelijk zijn ingezet wordt niet duidelijk uit de geconsulteerde bronnen.[217]

Zweden hanteert een gecentraliseerd aanmeldingssysteem voor het hoger onderwijs, beheerd door de Zweedse Raad voor Hoger Onderwijs (UHR). De UHR adviseert en biedt referenties, maar universiteiten en hogescholen beslissen zelf over toelating en zijn verantwoordelijk voor het controleren van kwalificaties en het opsporen van fraude. Bij PhD-aanmeldingen ligt deze verantwoordelijkheid volledig bij de instellingen zelf. Er is geen centrale rapportageplicht, waardoor de UHR geen inzicht heeft in het aantal

[217] Bundesamt für Verfassungsschutz (2026).

fraudegevallen bij de instellingen. In een interview werd benoemd dat kandidaten met vervalste diploma's van diploma mills zijn toegelaten tot PhD-programma's, wat de ernst van de kwestie onderstreept. Diploma mills vormen een groeiende uitdaging. Het is vaak eenvoudiger om te bevestigen dat een instelling geen diploma mill is dan om te bewijzen dat ze er wel een is. Diploma mills worden in verband gebracht met economische criminaliteit en vormen een bredere maatschappelijke bedreiging, aangezien ze aanzienlijke inkomsten genereren voor criminele exploitanten.

In het Verenigd Koninkrijk is er ook aandacht voor informatie die wordt achtergehouden. Binnen ATAS wordt niet alleen gekeken naar de inhoud van een aanvraag, maar ook naar mogelijke omissies, zoals hiaten in cv's. De aangeleverde documenten worden vergeleken met open-source-informatie, en als bepaalde zaken niet worden genoemd, kan dit aanleiding zijn voor verder onderzoek.

Samenvattend lijken de belangrijkste modus operandi wat betreft identiteits- en documentatiefraude in de context van kennisveiligheid:

- Het gebruik van onvolledige documenten en het bewust achterhouden van informatie, bijvoorbeeld over affiliaties of herkomst van financiering.
- Het verdraaien of geven van onjuiste informatie, door bijvoorbeeld minder risicovolle affiliaties te vermelden. Het niet vertalen van dergelijke affiliaties kan het moeilijker maken om de werkelijke betekenis te achterhalen.
- Valse diploma's, bijvoorbeeld gefabriceerd door diploma mills.
- Valse uitnodigingsbrieven voor visumdoeleinden.

In hoeverre is er een beeld van de frequentie waarin dit soort fraude plaatsvindt in Nederland en daarbuiten?

Uit het literatuuronderzoek en de interviews is gebleken dat het zeer lastig is om een goed beeld te krijgen van de frequentie waarin dit soort fraude plaatsvindt in Nederland. Dit komt met name doordat er sprake is van een gedecentraliseerd systeem, waarbij een groot deel van de verantwoordelijkheid van screening bij de kennisinstellingen zelf ligt. Mogelijk zouden zij dus een beeld kunnen geven van de frequentie van fraude op het niveau van hun instelling. Er bestaan echter grote verschillen tussen kennisinstellingen wat betreft hun capaciteit om inkomende studenten en onderzoekers te screenen. Verschillende instanties zijn betrokken bij een deel van het proces, bijvoorbeeld het controleren van de authenticiteit van diploma's. Zoals uit de casestudies blijkt, hebben zij soms zicht op fraude voor dit deel van het proces. Maar zelf geven zij ook aan dat ze geen compleet beeld hebben. Nuffic in Nederland heeft bijvoorbeeld een adviserende rol, waarbij universiteiten niet verplicht zijn om authenticiteit van diploma's door Nuffic te laten controleren.

Volgens geïnterviewde experts in Australië zijn er tot op heden geen gevallen ontdekt van personen die onder een valse identiteit reisden. Zij geven hierbij echter aan dat, aangezien buitenlandse staatsactoren de grootste bedreiging vormen, het wellicht vrijwel onmogelijk is om frauduleuze referenties op te sporen wanneer deze door overheidsinstanties zijn uitgegeven. Zoals aangegeven is de belangrijkste vorm van fraude in Australië, het geven van onjuiste informatie, met name in cv's en subsidieaanvragen. Ook hier bestaat geen compleet beeld van de omvang van dit fenomeen. Maar dat het gebeurt is duidelijk: de China Scholarship Council rapporteerde in 2024 1.000 ontvangers van financiering in Australië en slechts 350

studenten gaven openlijk toe deze steun te ontvangen. Deze aanzienlijke discrepantie onderstreept hoe vaak personen niet transparant zijn over de aard of de bron van hun onderzoeksfinanciering. Omdat het hier slechts gaat om een enkele bron van financiering, is het denkbaar dat het slechts een indicatie is van een groter probleem waarbij ook andere informatie wordt achtergehouden. Wat betreft valse uitnodigingsbrieven voor visumdoeleinden registreerde de Australische universiteit van New South Wales in de afgelopen twee tot drie jaar in totaal 6 tot 12 gevallen. Dit komt voornamelijk voor op faculteitsniveau, bij gastwetenschappers. Opvallend is dat er geen relevante casestudies zijn met betrekking tot de PACT-voorschriften. Hoewel het mechanisme is toegepast om visumaanvragen te beperken, blijven beslissingen hierover buiten het publieke domein. Tijdens een interview is opgemerkt dat dit alleen openbaar zal worden gemaakt als een aanvrager in de toekomst besluit een beslissing aan te vechten.

Zoals in de paragraaf hierboven naar voren komt, is er in Duitsland sprake van een zeer gedecentraliseerd systeem. Daardoor is het ook hier niet mogelijk om een beeld te krijgen van de frequentie van fraude. Daarnaast gaat de Duitse overheid, net als veel andere overheden, vanwege nationale veiligheidsbelangen slechts zeer beperkt in op vragen over de frequentie en schaal van dit soort fraude.

Ook in Zweden ligt de verantwoordelijkheid bij de kennisinstellingen zelf, waardoor het in dit land eveneens lastig is om een beeld te krijgen van de frequentie. Wel worden toelatingen van bachelor- en masterstudenten gecentraliseerd bij de UHR behandeld. Uit een interview komt naar voren dat voor academische toelatingen via het UHR-portaal het aantal gemelde fraudegevallen is gestegen, van 30 in 2024 tot 130 in 2025. Dit wordt grotendeels toegeschreven aan het gebruik van AI-agenten waardoor de aanmeldingsprocedure toegankelijker zou zijn geworden. Hier is echter geen directe link met kennisveiligheid te maken, want het kan bijvoorbeeld ook gaan om fraude om economische migratiedoeleinden. Het geeft echter wel een beeld van de schaal en de mogelijk groeiende rol van AI.

Welke waarborgen kunnen worden gecreëerd om de verschillende manieren waarop fraude wordt gepleegd tegen te gaan?

Uit dit onderzoek blijkt dat de risico's binnen de context van kennisveiligheid divers zijn. Onderliggende motivaties voor fraude kunnen bijvoorbeeld voortkomen uit structurele beperkingen in het land van herkomst, via anticiperend gedrag van individuele onderzoekers, tot doelbewuste misleiding of spionage. Deze diversiteit betekent dat een uniforme, generieke aanpak zelden effectief of proportioneel zal zijn.

In veel gevallen is het aan de ontvangende instelling of screener om, op basis van kennis van de context en de individuele situatie, een afgewogen oordeel te vellen. Dit vraagt om het vermogen om op basis van duidelijke kaders, actuele informatie en voldoende expertise genuanceerde beslissingen te nemen. Tegelijkertijd brengt een te vergaande centralisatie of het hanteren van generieke uitsluitingscriteria het risico met zich mee dat de academische vrijheid en openheid worden aangetast.

Het ontbreken van systematische data over de prevalentie en aard van verschillende risico's bemoeilijkt bovendien de ontwikkeling van een zuiver risicogestuurd beleid. Zolang niet duidelijk is welke risico's het meest voorkomen en hoe deze zich manifesteren, blijft het vormen van effectief beleid lastig. Dit onderstreept het belang van heldere conceptuele kaders, betere dataverzameling en het investeren in kennisdeling en expertise binnen en tussen instellingen.

Uit het literatuuronderzoek en de interviews komen meerdere lessen voor Nederland naar voren, dan wel waarborgen die kunnen worden gecreëerd om de verschillende manieren waarop fraude gepleegd wordt tegen te gaan.

Screening op individueel en institutioneel-/landenniveau beter samenbrengen

Uit de interviews en praktijkervaringen komt naar voren dat het controleren op inconsistenties een van de belangrijkste manieren is om fraude te signaleren, omdat fraudeopsporing op basis van enkele documenten, en zeker kopieën van documenten, lastig te doen is. Dit is zeker het geval als er sprake is van fraude waarbij statelijke actoren betrokken zijn.[218] Uit een interview voor de casestudie over Zweden blijkt bijvoorbeeld dat het verifiëren van publicaties een van de voornaamste manieren is waarop gecontroleerd wordt op mogelijke defensielinks. Dit gebeurt niet alleen voor de student of onderzoeker zelf, maar ook voor de begeleider. Dit is nuttig indien de PhD-onderzoeker zelf geen uitgebreide trackrecord heeft.[219] Tevens kunnen publicaties worden vergeleken met de informatie die op een cv wordt vermeld, waardoor inconsistenties aan het licht kunnen komen.[220] In Nederland mag het Loket Kennisveiligheid geen persoonsgegevens ontvangen en heeft het niet de taak om informatie op individueel niveau (zoals publicaties) te controleren.[221] Het kijkt slechts naar affiliaties op het niveau van de kennisinstelling, waardoor de eerdergenoemde mogelijke risico-indicatoren (bijvoorbeeld militaire technologiepatenten van onderzoekers) die op individueel niveau gelden, niet door het Loket worden gecontroleerd. Kennisinstellingen zijn verantwoordelijk voor deze controles op individueel niveau, maar hebben slechts beperkte middelen om de benodigde landenkennis op te bouwen. Een compleet beeld vormen is dus afhankelijk van goede coördinatie en kennisindeling tussen instanties, zoals kennisinstellingen en het Loket Kennisveiligheid. Maar dit gebeurt momenteel slechts op vrijwillige basis. In bijvoorbeeld Frankrijk komt kennis over risico's op individueel en institutioneel-/landenniveau meer samen, doordat de kennisveiligheidscoördinator binnen kennisinstellingen een vertrouwelijke functie betreft die wordt aangesteld door de overheid.

Verken informatievoorziening voor kennisinstellingen over kennisdeling

Controles ten behoeve van kennisveiligheid zijn momenteel in alle onderzochte landen versnipperd over meerdere instanties. Dit wordt verder gecompliceerd doordat de nodige informatie doorgaans persoonsgegevens omvat, en het delen daarvan secuur en in overeenstemming met privacywetgeving moet gebeuren. In Zweden wordt dit bijvoorbeeld als heikel punt ervaren. Zelfs als fraude wordt vastgesteld tijdens een toelatingsprocedure kan deze informatie vaak niet extern, of zelfs niet intern gedeeld worden.[222] In Zweden geeft de UHR zowel erkenning met het oog op de arbeidsmarkt als met het oog op vervolgstudies. Om redenen van gegevensbescherming is het delen van informatie tussen de twee procedures verboden, zelfs wanneer een persoon voor beide doeleinden een aanvraag heeft ingediend.[223] Daarnaast

[218] RAND Europe Interview – 8.

[219] RAND Europe Interview – 9.

[220] RAND Europe Interview – 4.

[221] RAND Europe Interview – 4.

[222] RAND Europe Interview – 14.

[223] RAND Europe Interview – 14.

geven in Nederland betrokken instanties zoals Nuffic adviezen; kennisinstellingen zijn niet verplicht om advies in te winnen en behouden altijd de bevoegdheid om zelf te beslissen over toelating. Hierdoor kan het voorkomen dat een student, voor wie Nuffic zich heeft onthouden van advies vanwege twijfels over de authenticiteit of erkenning van documenten, bij de ene instelling niet wordt toegelaten, maar elders wel. In de praktijk vragen kennisinstellingen voor bepaalde landen vrijwel altijd advies aan, maar de interpretatie en uiteindelijke beslissing ligt bij de instelling zelf.[224] Kennisinstellingen delen ook onderling geanonimiseerde fraudegevallen. Het is lastig in te schatten hoe structureel dit gedaan wordt en hoe effectief deze aanpak is. Eerder onderzoek concludeerde al dat kennisinstellingen het zonder duidelijke wettelijke kaders lastig vinden in te schatten wat ze AVG-technisch mogen opvragen en wie ze wel en niet moeten toetsen.[225] De belangrijkste les die hieruit volgt, is dat kennisinstellingen dringend behoefte hebben aan heldere richtlijnen en praktische ondersteuning over wat zij op grond van privacywetgeving mogen opvragen, wie zij wel of niet moeten screenen, en hoe persoonsgegevens intern en tussen instanties gedeeld mogen worden. Ook is er behoefte aan duidelijke richtlijnen over wanneer en op welke wijze fraudegevallen moeten worden opgeschaald of doorgezet naar andere instanties, zoals de inlichtingendiensten. Uit de interviews blijkt dat informatie over fraude soms wordt teruggekoppeld aan de kennisinstellingen en in andere gevallen wordt doorgegeven aan inlichtingendiensten, maar dat hiervoor geen eenduidige procedures of richtlijnen bestaan. Zonder deze duidelijkheid blijft kennisveiligheid kwetsbaar voor versnippering en onbedoelde hiaten in het screeningsproces.

Organiseer herhaalde en gelaagde screening

Een andere conclusie uit dit onderzoek is dat in veel landen formele controles al zijn ingebouwd in de visumaanvraag of in financiering, bijvoorbeeld in Australië. Hierdoor zijn meerdere instanties actief betrokken bij de screening. Echter komt in een interview over Australië naar voren dat dit er ook voor kan zorgen dat kennisinstellingen volledig vertrouwen op het oordeel van de overheid. Als gevolg hiervan verschuift de aandacht van de instellingen, zodra iemand een visum heeft ontvangen, vrijwel volledig naar ondersteuning bij zijn of haar binnenkomst en integratie in Australië en vinden er na aankomst in feite geen verdere controles meer plaats. Universiteiten en onderzoeksorganisaties voeren zelden aanvullende beoordelingen uit, tenzij de persoon betrokken is bij een duidelijk defensie-gerelateerd project. Deze afhankelijkheid van de initiële screening door de overheid kan hiaten in het lopende risicobeheer veroorzaken en kan de kwetsbaarheid voor veiligheidsdreigingen die zich na aankomst ontwikkelen vergroten.[226]

De Zweedse Migratiedienst beoordeelt visumaanvragen van buitenlandse aanvragers zodra zij als student of docent zijn toegelaten tot een instelling voor hoger onderwijs.[227] Indien er een risico wordt vastgesteld, meestal op basis van de affiliaties van de individuele onderzoeker of het onderzoeksgebied, kunnen visumzaken worden doorverwezen naar de Zweedse veiligheidsdiensten. Dit proces van visumbeoordeling en doorverwijzing geldt voor alle buitenlandse aanvragen en is geworteld in het bredere migratie- en

[224] RAND Europe Interview – 8.

[225] Bokdam et al. (2023).

[226] RAND Europe Interview – 1.

[227] RAND Europe Interview – 9.

nationale veiligheidsbeleid, niet in kennisveiligheidsoverwegingen. In Duitsland is het Bundesamt für Migration und Flüchtlinge (BAMF) verantwoordelijk voor de controle van documenten die vereist zijn in het visaproces.

Bij de aanvraag van een visum via de IND hoeft de kennisinstelling als erkende referent alleen een kopie van het paspoort en een eigen verklaring toe te voegen aan het dossier.[228] De formele beoordeling van en beslissing op aanvragen blijft bij de IND. Het systeem gaat daarbij uit van een vertrouwensrelatie tussen de overheid en de kennisinstelling als erkende referent, waarbij controles door de IND mede op basis van signalen en achteraf steekproefsgewijs plaatsvinden.[229] Dit systeem is gebaseerd op het moderne migratiebeleid (wet MoMi), waarbij universiteiten en hogescholen als erkende referenten optreden en een belangrijke verantwoordelijkheid dragen voor het indienen en onderbouwen van aanvragen.[230] Bij het visumproces is dus een belangrijke rol voor de kennisinstellingen weggelegd, terwijl in andere landen de overheid hier een grotere rol speelt. In een interview komt naar voren dat dit ook in Nederland voor betere controle zou kunnen zorgen.[231]

Zoals in de casestudie aan bod komt, is in Australië door ARC ook een screening ingebouwd in het financieringsproces. In Nederland zijn aanvragers van financiering verplicht de nationale richtlijnen inzake kennisveiligheid na te leven, waarbij de NWO partij is. In geval van twijfel kan de NWO de aanvrager om een nadere toelichting vragen. Daarnaast kan ze besluiten om in de toekenningsbrief aanvullende voorwaarden op te nemen ter bescherming van de kennisveiligheid.[232] Er is echter geen sprake van een uitgebreid screeningsproces zoals dit in Australië het geval is.

De belangrijkste les die hieruit volgt, is dat effectieve kennisveiligheid vraagt om herhaalde en gelaagde screening, waarbij zowel overheidsinstanties als kennisinstellingen een actieve rol blijven spelen gedurende het hele traject. Door overheidsinstanties stelselmatig te betrekken bij controles tijdens de visum- of financieringsaanvraag, kan een extra waarborg worden gecreëerd.

Zet technische expertise in bij screening

Het Britse systeem biedt enkele nuttige best practices, zoals de sterke nadruk op technische expertise en duiding. Dit is essentieel, omdat ambtenaren vaak niet over de benodigde kennis van sensitieve vakgebieden beschikken. Het is belangrijk om experts te hebben die inzicht hebben in de risico's en die hun kennis voortdurend bijhouden, gezien de snelle veranderingen binnen de wetenschap.[233] Het belang van technische expertise en duiding komt ook in het Franse systeem naar voren.[234] Daar krijgen onderzoekers een ambtelijke aanstelling, waardoor het makkelijker is om zowel ambtenaar als onderzoeker te zijn of hiertussen te wisselen. Zo worden wetenschappers direct onderdeel van het screeningsproces.[235] In haar reactie op de

[228] RAND Europe Interview – 8.

[229] Lodder (2019).

[230] Lodder (2019).

[231] RAND Europe Interview – 4.

[232] European Union (2025).

[233] RAND Europe Interview – 2.

[234] RAND Europe Interview – 2.

[235] RAND Europe Interview – 2.

eerder voorgestelde Wet screening kennisveiligheid geeft de NWO aan dat kennisinstellingen niet beschikken over de vereiste achtergrondinformatie om de strategische context van de verschillende statelijke actoren te beoordelen. Dit geldt onder meer bij de voorziene toepassing bij fundamenteel onderzoek TRL *1-2*. Kennisinstellingen geven aan dat de overheid hun hierover moet informeren.[236] Samenwerking tussen ambtenaren en onderzoekers zoals dit in Frankrijk gebeurt zou hierin nuttig kunnen zijn. De belangrijkste les is dat effectieve kennisveiligheid vraagt om een structurele samenwerking tussen ambtenaren, kennisveiligheidscoördinatoren en wetenschappelijke experts, zodat technische en strategische duiding altijd beschikbaar is bij de beoordeling van risico's. Het opzetten van vaste overlegstructuren of expertgroepen, kan hierbij als best practice dienen.

Coördineer informatieverstrekking en landenkennis om fraude te herkennen

Een van de belangrijkste lessen uit dit onderzoek is het belang van het verkrijgen van de juiste informatie, en het hebben van de (landen)kennis en data om deze juist te interpreteren.

Wat duidelijk werd uit meerdere casestudies is dat een van de vormen van fraude die het vaakst wordt waargenomen het achterhouden of verdraaien van informatie is, waardoor bijvoorbeeld defensielinks niet zichtbaar worden. Het Loket Kennisveiligheid krijgt regelmatig vragen van kennisinstellingen over buitenlandse entiteiten die van naam veranderen of fuseren met andere instituten, wat het lastiger maakt om ze te volgen.[237] Dit is een bekend probleem wat betreft aanmeldingen vanuit China, zoals besproken in de introductie van dit rapport. Ook het achterhouden van informatie over financiering is gangbaar, zoals blijkt uit de Australische casestudie. De China Scholarship Council rapporteerde in 2024 1.000 ontvangers van financiering in Australië, maar in het aanmeldingsproces gaven slechts 350 studenten openlijk toe deze steun te ontvangen.[238]

Landenkennis

Een belangrijke waarborg voor effectieve kennisveiligheidsscreening is het beschikken over specifieke landenkennis, zodat aangeleverde documenten en informatie correct kunnen worden geïnterpreteerd. Het Loket Kennisveiligheid heeft bijvoorbeeld medewerkers met kennis van relevante talen en culturele context, waardoor zij risico's beter kunnen inschatten. Inzicht in financieringsbronnen uit risicolanden, waarvan de China Scholarship Council er slechts een is, helpt beoordelen of er sprake is van financiering met mogelijke defensielinks. Daarnaast maakt deze expertise het eenvoudiger om ontwikkelingen bij buitenlandse entiteiten, zoals naamswijzigingen, te volgen. Landenspecialisatie draagt bovendien bij aan het herkennen van terugkerende fraudepatronen, zoals ook uit interviews met Nuffic en hun Zweedse tegenhanger blijkt. Daar zijn landenspecialisten werkzaam die door hun ervaring snel bekende risico's en signalen kunnen identificeren.

Goed begrip van en data over risico-indicatoren

In meerdere interviews komt naar voren dat tijdens het screeningsproces veelvuldig gebruik wordt gemaakt van de ASPI-tracker, een tracker van het Australian Strategic Policy Institute dat defensielinks van Chinese

[236] NWO (2025).

[237] RAND Europe Interview – 4.

[238] RAND Europe Interview – 7.

universiteiten in kaart brengt. Dergelijke instrumenten kunnen ondersteunen bij het juist interpreteren van informatie die wordt aangeleverd tijdens een aanmelding, bijvoorbeeld historische institutionele namen of acroniemen. Hierdoor kunnen ze helpen om bepaalde risico's tegen te gaan.

In Sectie 1.2 gaan we in op risico-indicatoren voor defensielinks, zoals adviesfuncties, onderscheidingen, financiering, patenten of publicaties met defensielinks.[239] Advies vanuit de overheid en afstemming tussen risico-indicatoren en tools om hierop te checken zouden welkom zijn, zodat kennisinstellingen vergelijkbare afwegingen maken.[240] Een Europees antwoord kan een toegevoegde waarde hebben, omdat de veelgebruikte ASPI-tracker is ontwikkeld in Australië vanuit het oogpunt van Australische en Amerikaanse belangen.[241] Hier zijn de eerste stappen al voor genomen. De Europese Commissie werkt aan de ontwikkeling van een beveiligd IT-platform dat betrouwbare informatie over buitenlandse onderzoeksinstellingen zal verzamelen om kennisinstellingen te helpen inzicht te krijgen in de mogelijke risico's die gepaard gaan met het aannemen van buitenlandse onderzoekers. Het due-diligence-platform is bedoeld om onderzoekers en onderzoeksorganisaties in de EU te ondersteunen bij het nemen van weloverwogen beslissingen en het versterken van het algemene vertrouwen in internationale samenwerking. Naar verwachting zal eind 2026 een eerste proefversie beschikbaar zijn.[242] Het is wenselijk dat kennisinstellingen actief participeren in de ontwikkeling en het gebruik van het Europese due-diligence-platform. Door ervaringen en best practices te delen, kan het platform optimaal aansluiten bij de behoeften van de praktijk.

Een duidelijk beeld van de risico-indicatoren kan er ook voor zorgen dat de opgevraagde informatie proportioneel is en niet een te grote inbreuk op de privacy van kandidaat-studenten en -onderzoekers vormt. Het laatste was een van de bezwaren vanuit de KNAW tegen de voorgestelde screeningswet: het gaf aan dat informatie aangeleverd zou moeten worden over het 'sociaal en wetenschappelijk netwerk, landen van verblijf […] en eventuele risico's verbonden aan een partner, ouders of kinderen' (memorie van toelichting, 41). De KNAW vond dit een vergaande inbreuk op de privacy van de kandidaten.[243]

Disclosure-voorwaarden

In Australië gelden in het ARC-proces disclosure-voorwaarden voor risico-indicatoren: onderzoekers met niet-Australische affiliaties, financiering en deelname aan talentprogramma's moeten deze verplicht melden.[244] Het ARC Research Security Framework geeft aan welke informatie verstrekt moet worden en legt de verantwoordelijkheid bij de universiteiten om te controleren of studenten of onderzoekers de juiste informatie verstrekken.[245] Het overzicht van risico-indicatoren en disclosure-eisen dat uit het framework volgt, schept helderheid aan kennisinstellingen welke informatie zij moeten opvragen en garandeert dat dit stelselmatig gebeurt. Bovenstaande cijfers over het achterhouden van financiering van de China Scholarship Council zijn enkel te verkrijgen doordat Australië zulke heldere disclosure-voorwaarden heeft die centraal

[239] RAND Europe (2026).

[240] Bokdam et al. (2023).

[241] Bokdam et al. (2023).

[242] European Union (2026).

[243] KNAW (2025).

[244] Australian Research Council (2026a).

[245] Australian Research Council (2026a).

belegd zijn. Zo ontstaat een duidelijker beeld van de frequentie van fraude. Daarnaast maakt het duidelijk of informatie bewust is weggelaten, en dat dit niet is gebeurd vanuit onduidelijke richtlijnen of onwetendheid. Eventuele consequenties van het achterhouden van informatie, zoals het niet verkrijgen van financiering, zijn van tevoren expliciet gecommuniceerd. Het invoeren van heldere, centraal vastgelegde disclosure-voorwaarden, vergelijkbaar met het Australische model, kan bijdragen aan meer transparantie en een eerlijker speelveld. Het maakt aan kennisinstellingen ook duidelijk welke informatie zij moeten opvragen en welke consequenties er zijn bij het achterhouden van informatie.

Zorg voor Europese coördinatie om weglekken te voorkomen

Het Loket Kennisveiligheid hoort regelmatig van kennisinstellingen dat er behoefte is aan een gelijker speelveld binnen Europa. Er bestaat concurrentie tussen Europese universiteiten, waardoor het problematisch is als in Nederland bepaald onderzoek wordt gehinderd vanwege veiligheidsrisico's omtrent buitenlandse onderzoekers, terwijl universiteiten in andere landen dergelijke onderzoekers ongehinderd toelaten. Dit kan Nederlandse instellingen op achterstand zetten.[246] Dit is ook een punt wat duidelijk naar voren komt in de officiële reacties van de KNAW en NWO op de eerder voorgestelde screeningswetgeving.[247] Nederlandse kennisinstellingen werken bovendien nauw samen met kennisinstellingen in omliggende landen, waardoor sensitieve kennis en technologie alsnog kan weglekken als er geen sprake is van een gecoördineerde aanpak. Een ongelijk speelveld kan ook implicaties hebben voor samenwerking binnen de EU, omdat het het vertrouwen kan ondermijnen. Het zou bijvoorbeeld kunnen betekenen dat onderzoekers uit een lidstaat worden uitgesloten van consortia omdat hun land geen kennisveiligheidsbeleid heeft, of andersom omdat de veiligheidsmaatregelen van een land als te streng en belastend worden beschouwd.[248] De belangrijkste les is dan ook dat Europese coördinatie op het gebied van kennisveiligheid essentieel is.

Reflecties en vervolgonderzoek

Dit onderzoek kent enkele belangrijke beperkingen. Ten eerste was het gebruik van AI bij identiteits- en documentfraude in de context van kennisveiligheid geen expliciete focus van deze studie. Hoewel AI naar verwachting grote gevolgen kan hebben voor kennisveiligheid, is dit onderwerp slechts beperkt aan bod gekomen in de interviews, mede omdat het om een relatief nieuwe ontwikkeling gaat. Alleen in het interview met de Zweedse UHR wordt melding gemaakt van een sterke toename van fraudegevallen bij toelatingen tot het hoger onderwijs, grotendeels als gevolg van AI-toepassingen. Toekomstig onderzoek zou daarom expliciet aandacht kunnen besteden aan de rol van AI bij identiteits- en documentfraude en de implicaties hiervan voor kennisveiligheidsbeleid.

Ten tweede richt dit onderzoek zich uitsluitend op identiteits- en documentfraude als middel om toegang te krijgen tot sensitieve technologie en kennis. Andere relevante risico's, zoals heimelijke beïnvloeding van onderwijs en onderzoek door statelijke actoren of ethische dilemma's bij samenwerking met landen die mensenrechten schenden, vallen buiten de reikwijdte van deze studie. Eveneens zijn andere aspecten van

[246] RAND Europe Interview – 4.

[247] KNAW (2025), NWO (2025).

[248] European Union (2026).

kennisveiligheid, zoals fysieke beveiliging, cybersecurity en bescherming van intellectueel eigendom, niet of slechts zijdelings behandeld. Voor een integrale benadering van kennisveiligheid is het echter van belang dat toekomstige studies en beleidsdiscussies ook deze thema's meenemen.

Tot slot zijn de beschikbare data over fraude in de context van kennisveiligheid zeer beperkt en gefragmenteerd. Het kennisveiligheidsbeleid in veel landen staat bovendien nog in de kinderschoenen, waardoor het moeilijk is om uitspraken te doen over de effectiviteit en proportionaliteit van bestaande screeningsmaatregelen. Verdere investeringen in systematische dataverzameling, kennisdeling en onderzoek naar opkomende risico's – zoals die rondom AI – zijn noodzakelijk om de effectiviteit en proportionaliteit van bestaande screeningsmechanismen beter te kunnen beoordelen en onderbouwen. Alleen met een solide kennisbasis kunnen screeningsmaatregelen gericht worden geëvalueerd, bijgestuurd en toekomstbestendig gemaakt.

Bronnen

Algemene Inlichtingen- en Veiligheidsdienst (AIVD). 2025. 'Themaverhaal: Streven naar dominantie bepaalde China's acties in 2024.' *AIVD Jaarverslag 2024*. Ministerie van Binnenlandse Zaken. Geraadpleegd op 14 mei 2025: https://www.aivd.nl/documenten/2025/04/24/jaarverslag-2024

Australian Department of Education. 2023. *Report on implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector*. Geraadpleegd op 27 mei 2026: https://www.education.gov.au/countering-foreign-interference-australian-university-sector/resources/report-implementation-guidelines-counter-foreign-interference-australian-university-sector

———. 2024. *Pulse Check on the implementation of the Guidelines to Counter Foreign Interference in the Australian University Sector*. Geraadpleegd op 27 mei 2026: https://www.education.gov.au/download/18668/pulse-check-implementation-guidelines-counter-foreign-interference-australian-university-sector/39343/document/pdf

———. 2025. 'University Foreign Interference Taskforce.' Geraadpleegd op 27 mei 2026: https://www.education.gov.au/countering-foreign-interference-australian-university-sector/university-foreign-interference-taskforce

Australian Department of Education. University Foreign Interference Taskforce. 2021. *Guidelines to Counter Foreign Interference in the Australian University Sector*. November. Geraadpleegd op 27 mei 2026: https://www.education.gov.au/countering-foreign-interference-australian-university-sector/guidelines-counter-foreign-interference-australian-university-sector

Australian Department of Home Affairs. 2024a. *Countering Foreign Interference in Australia: Working towards a more secure Australia*. Geraadpleegd op 27 mei 2026: https://www.homeaffairs.gov.au/nat-security/files/cfi-australia.pdf

———. 2024b. 'Countering Foreign Interference'. Laatst gewijzigd 28 februari 2024: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference

Australian Department of Industry, Science and Resources. 2026. 'List of Critical Technologies in the National Interest.' 19 May. Geraadpleegd op 27 mei 2026, voor de update op 1 juli 2026: https://www.industry.gov.au/publications/list-critical-technologies-national-interest

Australian Government. 2001. *Australian Research Council Act 2001 (Cth).*

———. 2023. *Australian Government response to the Parliamentary Joint Committee on Intelligence and Security report: National security risks affecting the Australian higher education and research sector*. Geraadpleegd op 27 juni 2026: https://www.homeaffairs.gov.au/reports-and-pubs/PDFs/government-response-national-security-risk-affecting-higher-education-research-sector.pdf

Australian Research Council. 2023. *ARC Countering Foreign Interference Framework*. December. Geraadpleegd op 27 mei 2026: https://www.arc.gov.au/sites/default/files/2023-12/ARC%20Countering%20Foreign%20Interference%20Framework.pdf

———. 2026a. *ARC Research Security Framework*. Geraadpleegd op 17 juni 2026: https://www.arc.gov.au/system/files/2026-05/arc-research-security-framework.pdf

———. 2026b. 'Research Security.' Geraadpleegd op 27 mei 2026: https://www.arc.gov.au/funding-research/research-security

Bitzinger, Richard A. 2021. 'China's Shift from Civil-Military Integration to Military-Civil Fusion.' *Asia Policy* 16, nr. 1, 5-24. Geraadpleegd op 14 juli 2026: https://muse.jhu.edu/pub/136/article/781800/pdf

Blom, Tesse, Timon de Boer & Iris van Vugt, I. 2025. *Aan de poort: Inventarisatie van de identificatie en authenticatie van persoons- en andere officiële documenten door Nederlandse kennisinstellingen*. https://repository.wodc.nl/server/api/core/bitstreams/eecc7e7d-7dc3-44fa-ab36-b92d2a222dc4/content

Bokdam, Johan, Timon de Boer, José van der Geest, Max Kemman, Anne Wester & Femke van Wijk. 2023. 'Kennisveiligheidsbeleid in het hoger onderwijs en onderzoek'. In *Sectorbeeld Universiteiten*. Geraadpleegd op 17 juni 2026: https://www.rijksoverheid.nl/documenten/2023/09/11/bijlage-1-oberon-dialogic-sectorbeeld-kennisveiligheid-universiteiten-2023

BMBF (German Federal Ministry of Education and Research). 2024. *Position Paper of the German Federal Ministry of Education and Research on Research Security in Light of the Zeitenwende*. Geraadpleegd op 14 april 2026: https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2024/position-paper-research-security.pdf?__blob=publicationFile&v=4

Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR). 2025. *Eckpunkte zur Stärkung der Forschungssicherheit und zum Aufbau einer Nationalen Plattform für Forschungssicherheit*. 18 december. Geraadpleegd op 15 april 2026: https://www.bmftr.bund.de/SharedDocs/Downloads/DE/2025/25-eckpunkte-forschungssicherheit.pdf?__blob=publicationFile&v=1

———. n.d.'Research Security'. In: *Bmftr.bund.de*. https://www.bmftr.bund.de/EN/Research/InternationalAffairs/ResearchSecurity/researchsecurity_node.html

Bundesregierung. 2022. 'Regierungserklärung von Bundeskanzler Olaf Scholz am 27. Februari 2022.' Geraadpleegd op 27 mei 2026: https://www.bundesregierung.de/breg-de/service/archiv-bundesregierung/regierungserklaerung-von-bundeskanzler-olaf-scholz-am-27-februar-2022-2008356

Bundesamt für Verfassungsschutz. 2026. *Zusammenarbeit gegen Proliferation: Technologien schützen – Sicherheit stärken*. Geraadpleegd op 27 mei 2026: https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/spionage-und-proliferationsabwehr/2026-01-proliferation.pdf?__blob=publicationFile&v=9

Clarke, Michael & Matthew Sussex. 2022. *China, Australia's National Security Choices and Great Power Competition in the Indo-Pacific*. Sydney: Australia-China Relations Institute, University of Technology Sydney. August. Geraadpleegd op 27 mei 2026: https://www.uts.edu.au/globalassets/sites/default/files/20220817-australia-china-relations-institute_china-australias-national-security-choices-and-great-power-competition-in-the-indo-pacific_michael-clarke-and-matthew-sussex.pdf

Deutscher Akademischer Austauschdienst (DAAD). 2023. 'DAAD Expands Guidance Services for German Higher Education Institutions.' 19 april. Geraadpleegd op 15 april 2026: https://www.daad.de/en/press-releases/daad-baut-kiwi-aus_2023/

DAAD KIWi. 2024. *KIWi Kompass: „Keine roten Linien":Wissenschaftskooperationen unter komplexen Rahmen bedingungen*. 2e editie. Geraadpleegd op 15 april 2026: https://blog.daad.de/kiwi-kompass/files/2023/10/DAAD_KIWi_Kompass_KeineRotenLinien_2.-Auflage.pdf

———. 2025. *KIWi Checklist Knowledge Security: A Self-assessment Tool for Evaluating Security-Relevant Dimensions of International Academic Cooperation*. 1e editie. Geraadpleegd op 16 april 2026: https://static.daad.de/media/daad_de/pdfs_nicht_barrierefrei/infos-services-fuer-hochschulen/kompetenzzentrum/dokumente/kiwi_checkliste_wissenssicherheit_en.pdf

Delta. 2026. 'Geen screening kennisveiligheid voor bedrijfsleven, besluit kabinet.' *Delta.tudelft.nl*. Geraadpleegd 17 juni 2026: https://delta.tudelft.nl/article/geen-screening-kennisveiligheid-voor-bedrijfsleven-besluit-kabinet

Deutsche Forschungsgemeinschaft (DFG). 2023. *Dealing with Risks in International Research Cooperation: Recommendations from the Deutsche Forschungsgemeinschaft*. September. Geraadpleegd op 27 mei 2026: https://www.dfg.de/resource/blob/289704/risiken-int-kooperationen-en.pdf

———. 2025a. 'Potential Risks of International Cooperation.' *Dfg.de*. Geraadpleegd op 27 mei 2026: https://www.dfg.de/en/basics-topics/basics-and-principles-of-funding/security-relevant-research/risks-inter-cooperation

———. 2025b. 'What is the DFG?' *dfg.de*. Geraadpleegd op 27 mei 2026: https://www.dfg.de/en/about-us/about-the-dfg/what-is-the-dfg

DFG & Nationale Akademie der Wissenschaften Leopoldina. 2014. *Scientific Freedom and Scientific Responsibility: Recommendations for Handling Security-Relevant Research*. Mei. Geraadpleegd op 27 mei 2026: https://www.security-relevant-research.org/wp-content/uploads/2022/10/2014_DFG-Leopoldina_Scientific_Freedom_Responsibility.pdf

d'Hooghe, Ingrid, & Jonas Lammertink. 2022. *How National Governments and Research Institutions Safeguard Knowledge Development in Science and Technology*. Den Haag: Adviesraad voor wetenschap, technologie en innovatie (AWTI); Leiden: Asia Centre. 28 november. https://www.awti.nl/documenten/2022/11/29/index-achtergrondstudie-lac

DUB. 2025. 'VVD: Zijn 'bedreigde' wetenschappers een gevaar voor onze kennisveiligheid?' *DUB.UU.nl*. 31 oktober. Geraadpleegd 18 juni 2026: https://dub.uu.nl/nl/nieuws/vvd-zijn-bedreigde-wetenschappers-een-gevaar-voor-onze-kennisveiligheid

D66, VVD & CDA. 2026. *Aan de slag: Coalitieakkoord 2026-2030: Bouwen aan een beter Nederland.* 30 januari. Geraadpleegd op 15 juni 2026: https://www.kabinetsformatie2025.nl/documenten/2026/01/30/aan-de-slag---coalitieakkoord-2026-2030

Engelbrecht, Sebastian, Panajotis Gavrilis & Moritz Metz. 2022. 'China Science Investigation - Chinas Militärinteresse an Forschungskooperation.' *Deutschlandfunk*. Geraadpleegd op 14 april 2026: https://www.deutschlandfunk.de/china-science-investigation-hintergrund-recherche-100.html

Europese Commissie. 2021. *Mededeling van de Commissie aan het Europees Parlement, de Raad, het Europees Economisch en Sociaal Comité en het Comité van de Regio's over de totaalaanpak voor onderzoek en innovatie: De strategie van Europa voor internationale samenwerking in een veranderende wereld*. COM(2021) 252 final. Mei. Geraadpleegd op 27 mei 2025: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0252

———. 2025. 'Commission Announces New Measures to Strengthen Research Security.' 28 oktober. Geraadpleegd op 9 juli 2026: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/commission-announces-new-measures-strengthen-research-security-2025-10-28_en

———. 2026a. 'EU Strengthens Science Diplomacy and Research Security to Support Global Research Cooperation.' 27 februari. Geraadpleegd op 27 mei 2026: https://research-and-innovation.ec.europa.eu/news/all-research-and-innovation-news/eu-strengthens-science-diplomacy-and-research-security-support-global-research-cooperation-2026-02-27_en

———. 2026b. *Research Security Monitor 2025: Raising Awareness and Building Resilience: Staff Working Document*. Geraadpleegd op 17 juni 2026: https://op.europa.eu/en/publication-detail/-/publication/7348956d-1389-11f1-8870-01aa75ed71a1/language-en

German Federal Office for Economic Affairs and Export Control (BAFA). 2023. *Manual Export Control and Academia*. 2e editie. Geraadpleegd op 27 mei 2026: https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_manual_export_control_and_academia.html?nn=1444524

German National Academy of Sciences Leopoldina & German Research Foundation. 2024. *Scientific Freedom and Security Interests in Times of Geopolitical Polarisation: Fifth Report of the Joint Committee of DFG and Leopoldina on November 1, 2024*. Geraadpleegd op 14 april 2026: https://www.security-relevant-research.org/publication-progressreport2024/

G7 Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE). 2022. *G7 Common Values and Principles on Research Security and Research Integrity*. Juni. Geraadpleegd op 27 mei 2026: https://www.bmftr.bund.de/SharedDocs/Downloads/EN/2022/g7_common_values.pdf?__blob=publicationFile&v=1

James, A., Kieron Flanagan, Alexander Naisbitt & John Rigby. 2025. *European Research Security: Threat Perspectives and the Responses of Policy Makers and Research Performing Organisations*. Manchester Institute of Innovation Research. https://research.manchester.ac.uk/en/publications/european-research-security-threat-perspectives-and-the-responses-/

Joske, Alex. 2018. *Picking Flowers, Making Honey: The Chinese Military's Collaboration with Foreign Universities*. Policy Brief, Report no. 5/2018. Australian Strategic Policy Institute (ASPI). 30 oktober. Geraadpleegd op 17 juni 2026: https://www.aspi.org.au/report/picking-flowers-making-honey/

Koninklijke Nederlandse Academie van Wetenschappen (KNAW). 2025. 'Invoering screeningswet verzwakt kennispositie Nederland.' 18 juni. Geraadpleegd op 17 juni 2026: https://www.knaw.nl/nieuws/invoering-screeningswet-verzwakt-kennispositie-nederland

Lodder, Gerrie. 2019. *Selectief naar restrictief. Evaluatie van de Wet modern migratiebeleid.* WODC. Geraadpleegd op 15 oktober 2026: https://repository.wodc.nl/server/api/core/bitstreams/b4183ddc-43d5-4bac-8825-0699a2f7e6b2/content

Loket Kennisveiligheid. 2026. *Nationale leidraad kennisveiligheid: Veilig internationaal samenwerking.* Geraadpleegd op 9 oktober 2026: https://www.loketkennisveiligheid.nl/site/binaries/site-content/collections/documents/2026/06/04/nationale-leidraad-kennisveiligheid-2026/nationale-leidraad-kennisveiligheid-2026.pdf

Militaire Inlichtingen- en Veiligheidsdienst (MIVD). 2025. *Openbaar jaarverslag 2024: Militaire Inlichtingen- en Veiligheidsdienst*. Geraadpleegd op 12 oktober 2026: https://open.overheid.nl/documenten/204ba7fc-ee17-4209-b5c7-fdeaa21180ca/file

Minister van Onderwijs, Cultuur en Wetenschap. 2026. *Brief van de minister van Onderwijs, Cultuur en Wetenschap aan de Voorzitter van de Tweede Kamer der Staten-Generaal inzake stand van zaken screening kennisveiligheid*. Kamerstuk 31 288, nr. 1260. Den Haag, 11 juni. Geraadpleegd op 12 oktober 2026: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026D29090&did=2026D29090

Ministerie van Economische Zaken en Klimaat. 2026. Ongewenste kennis- en technologieoverdracht via kenniswerkers bij bedrijven: Verkenning naar nieuwe (beleids)maatregelen – rapportage januari 2026. Geraadpleegd op 18 juni 2026: https://www.rijksoverheid.nl/documenten/2026/04/24/ongewenstekennisentechnologieoverdrachtviakenniswerkersbijbedrijven

Ministerie van Economische Zaken en Klimaat, Ministerie van Justitie en Veiligheid, en Ministerie van Onderwijs, Cultuur en Wetenschap. 2025. 'Wet screening kennisveiligheid.' *Internetconsultatie.nl*. 7 april. Geraadpleegd op 27 mei 2026: https://www.internetconsultatie.nl/screeningkennisveiligheid/b1

Ministry of Climate and Enterprise & Ministry of Education and Research. 2024. Research and innovation for the future, curiosity and benefit [Forskning och innovation för framtid, nyfikenhet och nytta]. Prop. 2024/25:60. Government Offices of Sweden. 12 December. Geraadpleegd op 27 mei 2026: https://www.regeringen.se/rattsliga-dokument/proposition/2024/12/prop.-20242560

Ministère de l'Enseignement supérieur, de la Recherche et de l'Espace. 2016. 'Protection du potentiel scientifique et technique et intelligence économique (P.P.S.T.)' [Protection of Scientific and Technical Potential and Economic Intelligence (P.P.S.T.)]. 12 september. Geraadpleegd op 12 oktober 2026: https://www.enseignementsup-recherche.gouv.fr/fr/protection-du-potentiel-scientifique-et-technique-et-intelligence-economique-ppst-46370

Myklebust, Jan Petter. 2024. 'Universities oppose guidelines on internationalisation.' University World News. 30 september. Geraadpleegd op 27 mei 2026: https://www.universityworldnews.com/post.php?story=20240930174150195

Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). 2023. *Samenvatting Decentrale contacten met China.* Geraadpleegd op 14 mei 2025: https://www.nctv.nl/documenten/2023/06/14/samenvatting-decentrale-contacten-met-china

———. 2025. *Dreigingsbeeld Statelijke Actoren (DBSA) 2025*. 17 juli. Geraadpleegd op 12 oktober 2026: https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025

Nationale Akademie der Wissenschaften Leopoldina & Deutsche Forschungsgemeinschaft. 2022. *Wissenschaftsfreiheit und Wissenschaftsverantwortung: Empfehlungen zum Umgang mit sicherheitsrelevanter Forschung /Scientific Freedom and Scientific Responsibility: Recommendations for Handling of Security-Relevant Research*. 2ee geactualiseerde editie. 10 oktober. Geraadpleegd op 27 mei 2027: https://www.dfg.de/resource/blob/349944/dual-use-empfehlungen-de-en.pdf

Nederlands-Vlaamse Accreditatieorganisatie (NVAO). 2026. 'Diploma Mills.' Geraadpleegd op 8 juli 2026: https://www.nvao.net/en/diploma-mills

Office français de l'intégrité scientifique (Ofis). 2026. *Research Integrity and Research Security: Towards a coordinated approach in response to foreign interference*. Prospective Note. 12 februari. Geraadpleegd op 27 mei 2026: https://www.ofis-france.fr/wp-content/uploads/2026/02/February2026_Research_Security_Integrity_Interference.pdf

Parliamentary Joint Committee on Intelligence and Security. 2022. *Inquiry into National Security Risks Affecting the Australian Higher Education and Research Sector*. Australian Parliament. Maart. As of 27 May 2026: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024611/toc_pdf/Inquiryintonationalsecurityrisksaffectingthe Australianhighereducationandresearchsector.pdf;fileType=application%2Fpdf

Pernin, Christopher G., Cortney Weinbaum, Fiona Quimbre, Shanshan Mei, Shay Hershkovitz, Libby Weaver & Catherine Kish. 2026. 'Research Security in Science and Technology'. RAND. 31 maart. Geraadpleegd op 16 juni 2026: https://www.rand.org/pubs/perspectives/PEA4104-1.html

RAND Europe. 2026. 'Using the CAS Directory: Indicators of Defence Participation.' *Chinese Academy of Sciences Directory*. Geraadpleegd op 16 juni 2026: https://www.rand.org/pubs/tools/TLA4687-1/tool/user-guide.html

Rijksdienst voor Ondernemend Nederland. 2026. 'Ondernemersloket Economische Veiligheid (OLEV): voor kennisintensieve bedrijven.' Laatst gewijzigd op 2 juni 2026. Geraadpleegd op 17 juni 2026: https://www.rvo.nl/onderwerpen/veilig-en-weerbaar-internationaal-ondernemen/over-olev#ondernemersloket-economische-veiligheid

Rijksoverheid. 2022. *Nationale leidraad kennisveiligheid: Veilig internationaal samenwerken*. 14 januari. Geraadpleegd op 27 mei 2026: https://www.loketkennisveiligheid.nl/site/binaries/site-content/collections/documents/2022/01/14/nationale-leidraad-kennisveiligheid/Nationale-leidraad-kennisveiligheid.pdf

———. 2025. ‘Screening voor wetenschappers die met sensitieve kennis willen werken.’ 7 april. Geraadpleegd op 14 mei 2025: https://www.rijksoverheid.nl/actueel/nieuws/2025/04/07/screening-voor-wetenschappers-die-met-sensitieve-kennis-willen-werken

Rüffin, Nicolas V., Katharina C. Cramer., Maximilian Mayer, & Peter J. Nock. 2025. “‘Research Security” in Germany and the United States: Shifting Governance of Scientific Collaboration Under Geopolitical Pressure. *Global Policy* 17, no. 1: 47–57. https://doi.org/10.1111/1758-5899.70103

Secrétariat général de la défense et de la sécurité nationale (SGDSN). 2025. ‘Protecting the Nation's Scientific and Technical Potential’ [Protéger le potentiel scientifique et technique de la nation]. 1 januari Geraadpleegd op 26 mei 2026: https://www.sgdsn.gouv.fr/nos-missions/proteger/proteger-le-potentiel-scientifique-et-technique-de-la-nation

Sharma, Yashee. 2023. ‘Australian Universities Teaching Students in China “Offensive” Cyber Hacking Tactics Sparks ’Alarming’ Concerns.’ *Sky News*. 7 maart. Geraadpleegd op 27 May 2026: https://www.skynews.com.au/australia-news/australian-universities-teaching-students-in-china-offensive-cyber-hacking-tactics-sparks-alarming-concerns/news-story/e8896b60de77d3ff60094c5195481a65

Shih, Tommy, Albin Gaunt & Stefan Östlund. 2020. *Responsible internationalisation: Guidelines for reflection on international academic collaboration*. STINT. Februari. Geraadpleegd op 27 mei 2026: https://www.stint.se/wp-content/uploads/2020/02/STINT__Responsible_Internationalisation.pdf

Speiser, Guido. 2022. ‚Wissenschaftsfreiheit im Grundgesetz.‘ In *Wissenschaftsrecht*, G. Speiser (eds) 45-60. https://doi.org/10.1007/978-3-662-64722-6_4

Stichting Nederlands Wetenschappelijk Onderzoek Instituten (NWO-I). 2025. *Reactie NWO-I: Zorgen over het wetsvoorstel screening kennisveiligheid*. Juni. Geraadpleegd op 17 juni 2026: https://www.nwo.nl/sites/nwo/files/media-files/NWO-I%20reactie%20wetsvoorstel%20screening%20kennisveiligheid%20-%20juni%202025.pdf

Stoff, Jeffrey. 2023. *Should Democracies Draw Redlines around Research Collaboration with China?: A Case Study of Germany*. The Center for Research Security & Integrity (CSRI). Geraadpleegd op 14 april 2026: https://researchsecurity.org/wp-content/uploads/2023/01/Click-here-to-download-the-full-publication.-Stoff-DrawingRedlinesFINAL.pdf

Swedish Council for Higher Education, Swedish Research Council, & Vinnova. 2024. *Responsible internationalisation: Interim report on a Government assignment*. Swedish Council for Higher Education. Geraaadpleegd op 27 mei 2026: https://www.uhr.se/globalassets/_uhr.se/publikationer/2024/responsible-internationalisation---interim-report-on-a-government-assignment-2024.pdf

———. 2025. *National support function for responsible internationalisation: Final report on a Government assignment*. Swedish Council for Higher Education, Maart. Geraadpleegd op 27 2026: https://www.uhr.se/globalassets/_uhr.se/english/about-the-council/national-support-function-for-responsible-internationalisation---final-report-2025.pdf

Swedish Research Council & Vinnova. 2026. *Responsible internationalisation: National guidelines 2026* [En ansvarsfull internationalisering: Vägledande nationella riktlinjer 2026]. Geraadpleegd op 27 mei 2026: https://www.vr.se/5.520d986e19c9897ed7435a14.html

TO2-federatie (Deltares, MARIN, NLR, TNO, Wageningen Research). 2025. *Reactie TO2-organisaties op voorstel Wet screening kennisveiligheid*. 30 juni. Geraadpleegd op 14 juli 2026: https://www.internetconsultatie.nl/screeningkennisveiligheid/reactie/a7db45d3-9aaf-47de-b065-788a49d56c9c

The University of Western Australia. 2026. 'Foreign Interference.' Geraadpleegd op 27 mei 2026: https://www.uwa.edu.au/about/leadership-and-governance/integrity-and-standards/foreign-interference

Tweede Kamer der Staten-Generaal. 2026. *Brief van de minister van Onderwijs, Cultuur en Wetenschap aan de Voorzitter van de Tweede Kamer der Staten-Generaal inzake de aanpak kennisveiligheid – voortbouwen op een solide basis*. Kamerstuk 31 288, nr. 1261. Geraadpleegd op 13 juli 2026: https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2026Z12878&did=2026D29095

Tweede Kamer der Staten-Generaal. 2025. *Vergaderjaar 2024–2025, 29 338, nr. 297*. Geraadpleegd 18 juni 2026: https://zoek.officielebekendmakingen.nl/kst-29338-297.html

Universiteiten van Nederland (UNL). 2025. Universiteiten: Wetsvoorstel kennisveiligheid schiet zijn doel voorbij. 18 juni. Geraadpleegd op 29 juni 2026: https://www.universiteitenvannederland.nl/actueel/nieuws/universiteiten-wetsvoorstel-kennisveiligheid-schiet-zijn-doel-voorbij.

Verordening (EU) 2021/821 van het Europees Parlement en de Raad van 20 mei 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik (herschikking). PbEU 2021, L 206/1. Geraadpleegd op 27 mei 2026: https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:32021R0821

Wissenschaftsrat (German Science and Humanities Council). 2025. *Science and Security in Times of Global Political Upheaval: Position Paper*. Document no. Drs. 2485-25_en. Geraadpleegd op 12 oktober 2026: https://doi.org/10.57674/v8dp-8269