Nationale leidraad kennisveiligheid

Veilig internationaal samenwerken

Juli 2026

Nationale leidraad kennisveiligheid

Veilig internationaal samenwerken

Juli 2026

Inhoudsopgave

Inleiding 5

Hoofdstuk 1 Introductie 7
- Waarom deze leidraad? 8
- Wat is kennisveiligheid? 9
- Een gezamenlijke opgave 11
- Rol van de Rijksoverheid 12

Hoofdstuk 2 Het beschermen van wetenschappelijke kernwaarden 13
- 2.1 Academische vrijheid 14
- 2.2 Gedragscodes wetenschappelijke integriteit 15
- 2.3 Open science 15
- 2.4 Ethiek in de wetenschap 16
- 2.5 Inclusiviteit en non-discriminatie 16

Hoofdstuk 3 Dreigingsbeeld 18
- 3.1 Verwerving van kennis en technologie 20
- 3.2 Beïnvloedings- en inmengingsactiviteiten 22
- 3.3 Ethische en integriteitschendingen 23

Hoofdstuk 4 Wettelijke kaders en richtlijnen 24
- 4.1 Sanctie- en dual-use verordeningen 25
- 4.2 Wet veiligheidstoets investeringen, fusies en overnames (Vifo) 27
- 4.3 Wetsvoorstel screening kennisveiligheid 27
- 4.4 Aanvullende codes, kaders, modellen en aanbevelingen 27
- 4.5 Wet open overheid 29
- 4.7 ABRO: Algemene Beveiligingseisen Rijksoverheid Opdrachten 31

Hoofdstuk 5 Het inschatten van risico's 32
- 5.1 Welke kennisgebieden binnen uw instelling hebben een verhoogd risico? 33
- 5.2 Welke landen hebben een verhoogd risico? 34
- 5.3 Ken uw samenwerkingspartners, opdrachtgevers en financiers 35
- 5.4 Waar u op moet letten bij het aangaan van een samenwerking 36
- 5.5 Kennisveiligheid bij inkopen en aanbesteden 38

Hoofdstuk 6 Risicomanagement 39
- 6.1 Organiseer risicomanagement binnen uw organisatie 40
- 6.2 Organisatorische maatregelen 41
- 6.3 Zorg voor een accurate feitenbasis voor besluitvorming 42
- 6.4 Veiligheidsbevorderende maatregelen 43
- 6.5 Veiligheidscultuur: bewustwording en alertheid 45

Hoofdstuk 7 Gastonderzoekers- en personeelsbeleid **46**
7.1 Kennisveiligheid bij werving en selectie 47
7.2 Opleiding en training 49
7.3 Risico op stigmatisering en ongewenst gedrag 50
7.4 Interne functiewisselingen en onderzoeksprogrammering 50
7.5 Toelating bezoekers, gastonderzoekers, gastdocenten en externe inhuur 51
7.6 Dienstreizen naar het buitenland 52
7.7 Beëindiging arbeidsrelatie 53

Appendix Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid **54**
Inleiding 55
1. Wettelijke kaders 56
2. Affiliaties en type organisatie 57
3. Vakgebied en type onderzoek 59
4. Afhankelijkheid en beïnvloeding 60
5. Ethiek en integriteit 61

Bronnen **62**
Contactgegevens 63

Inleiding

In januari 2022 werd de Nationale Leidraad Kennisveiligheid gepubliceerd, tegelijk met de opening van het Rijksbrede Loket Kennisveiligheid. Het markeerde de start van een gezamenlijke, lerende aanpak, waarmee de kennissector en de Rijksoverheid aan de slag gingen met het onderwerp kennisveiligheid.

In de eerste versie van de leidraad werden aandachtspunten, aanbevelingen en uitgangspunten uitgewerkt. Ze bakenden de scope van het kennisveiligheidsbeleid af en voorzagen de kennissector van richting bij het ontwikkelen van kennisveiligheidsbeleid binnen de eigen instellingen. Op 4 april 2022 riep minister Dijkgraaf de kennissector per brief op om de leidraad te implementeren, onder andere door het uitvoeren van een risicoanalyse, het aanwijzen van een bestuurlijke portefeuillehouder en het instellen van een adviesteam[1].

Sindsdien is er door zowel de kennisinstellingen als de Rijksoverheid veel ervaring opgedaan met kennisveiligheid. Het is belangrijk dat de leidraad goed blijft aansluiten bij die ervaring en bij de behoeften van kennisinstellingen. Daarom is er nu, door de kennissector en het Rijk gezamenlijk, een nieuwe versie van de leidraad opgesteld.

Net als de vorige versie richt ook deze leidraad zich op de kennissector als geheel. Daarmee is de leidraad nuttig voor een brede doelgroep. Zo voorziet het document bestuurders van handvatten in de sturing van het kennisveiligheidsbeleid en biedt het adviseurs, beleidsmakers en wetenschappers concrete handelingsperspectieven bij de uitvoering van dat beleid.

Op een aantal punten verschilt deze nieuwe leidraad van de vorige versie. Verouderde teksten zijn geactualiseerd, informatie is waar nodig verduidelijkt of aangevuld. Bovendien is er duidelijker onderscheid gemaakt tussen informatie die bedoeld is als handreiking, en de beschrijving van minder vrijblijvende kaders. Daarnaast zijn er inhoudelijke wijzigingen doorgevoerd. De belangrijkste zijn:

- In hoofdstuk 1 wordt de definitie van kennisveiligheid preciezer beschreven, en zoveel mogelijk in lijn gebracht met de definitie uit de verwante EU-raadsaanbeveling.
- Hoofdstuk 2 beschrijft in meer detail de verschillende relevante academische kernwaarden. Ook wordt nadrukkelijker benoemt dat er spanning kan optreden tussen kennisveiligheid en andere belangrijke academische kernwaarden en dat die spanning om een bewuste aanpak vraagt.
- Hoofdstuk 3 bevat een geactualiseerd en meer gedetailleerd dreigingsbeeld ten aanzien van de drie elementen van de definitie kennisveiligheid.
- In hoofdstuk 4 is een aantal wettelijke kaders die in ontwikkeling zijn toegevoegd. Daarnaast wordt de relatie tussen de Wet Open Overheid en het kennisveiligheidsbeleid van instellingen in dit hoofdstuk uitgelegd.
- Hoofdstuk 5 sluit in deze versie aan op de ‘indicatoren voor risico-inschatting internationale samenwerkingen kennisveiligheid’ die in het voorjaar van 2025 zijn opgesteld. Deze indicatoren zijn tevens als appendix bij deze leidraad gevoegd. Bovendien is de relevante inhoud uit hoofdstuk 7 van de vorige versie verplaatst naar hoofdstuk 5.

1 https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2022Z06535&did=2022D13337.

- Hoofdstuk 6 is uitgebreid met een weergave van wat nodig is voor een accurate feitenbasis voor bestuurders op het gebied van risicovolle buitenlandse samenwerkingen. Bovendien bevat hoofdstuk 6, in aanvulling op de ongewenste overdracht van technologie, een startpunt voor het nemen van maatregelen op de andere aspecten van kennisveiligheid.
- Het nieuwe hoofdstuk 7 (in de vorige versie hoofdstuk 8) beschrijft meer relevante aspecten van personeelsbeleid en biedt meer concrete aandachtspunten op het gebied van personeelsbeleid. Ook maakt dit hoofdstuk nu expliciet onderscheid tussen verplichte en aanvullende zorgvuldigheden in het HR-beleid van instellingen.
- Hoofdstuk 9 is vervallen. De leidraad beschrijft elders het belang van cyberveiligheid als onderdeel van kennisveiligheid, maar verwijst voor aanknopingspunten op het gebied van cyberveiligheid naar meer gespecialiseerde informatie.

Hoofdstuk 1

Introductie

Hoger onderwijs en onderzoek kunnen niet zonder internationale samenwerking en wetenschappelijk talent van over de hele wereld. Nederlandse kennisinstellingen hebben een goede reputatie en genieten wereldwijd een vooraanstaande positie. Die hebben ze onder meer te danken aan de academische vrijheid die in Nederland gegarandeerd is en de hoge mate van openheid van onze kennisinstellingen. We hebben dan ook veel van onze welvaart te danken aan onderzoekssamenwerking.

Tegelijkertijd is de wereld in beweging. Er vinden geopolitieke machtsverschuivingen plaats, waarbij economie, geopolitiek en veiligheid sterk met elkaar verweven zijn. Kennis en technologie worden in deze context steeds meer gezien als een strategisch machtsmiddel, dat kan worden ingezet naast of in combinatie met klassieke middelen, zoals spionage. Deze ontwikkelingen raken iedereen die in de Nederlandse kennissector actief is. Het is dan ook een gezamenlijke opgave om onze kennisveiligheid zo goed mogelijk te borgen.

Waarom deze leidraad?

Voor u ligt de Leidraad Kennisveiligheid van de Nederlandse kennissector en de Rijksoverheid. Dit document vormt de basis voor wie zich binnen hogescholen, universiteiten, universitair medische centra, TO2, KNAW- en NWO-instituten bezighoudt met kennisveiligheid en met het maken van afwegingen tussen kansen en (veiligheids)risico's bij internationale samenwerkingen. Deze leidraad richt zich daarbij niet alleen op bestuurders van kennisinstellingen, maar ook op anderen, zoals (kennis)veiligheidscoördinatoren, projectleiders en individuele onderzoekers en docenten.

De Nederlandse kennisinstellingen verschillen in aard, inrichting en omvang van hun onderwijs en onderzoek, maar allemaal bezitten én ontwikkelen ze waardevolle en soms sensitieve kennis en technologie. Bovendien staan ze allen voor internationale wetenschappelijke samenwerking, academische vrijheid, en open onderwijs en wetenschap.

Kennisinstellingen zijn zelf verantwoordelijk voor de inrichting en uitvoering van hun kennisveiligheidsbeleid. Daarin hebben ze veel vrijheid. Dat betekent dat kennisinstellingen, met inachtneming van relevante kaders en criteria, naar eigen inzicht kennisveiligheidsbeleid kunnen maken dat aansluit bij de specifieke aard en inrichting van de instelling.

Deze leidraad is dan ook niet bedoeld als een verplichtend kader voor toezicht en handhaving. De leidraad biedt kennisinstellingen een handreiking om invulling te geven aan hun verantwoordelijkheden op het gebied van kennisveiligheid. Daarom bevat deze leidraad, naast context en beleidskaders voor de verschillende onderwerpen, ook algemene duiding en praktische handvatten.

Internationale samenwerking in het hoger onderwijs en onderzoek moet **veilig** kunnen plaatsvinden. Dat is het overkoepelende doel van het kennisveiligheidsbeleid, zowel op nationaal niveau als op instellingsniveau. Het is zaak daarin een goede balans te vinden tussen kansen en risico's, met respect voor en inachtneming van wetenschappelijke kernwaarden. Bij het nemen van beschermende maatregelen zijn proportionaliteit en maatwerk essentieel. Het motto van kennisveiligheid is niet voor niets: 'open waar mogelijk, beschermen waar nodig'. Deze leidraad moet dan ook nadrukkelijk niet gelezen worden als oproep om alle risico's uit de weg te gaan.

Wat is kennisveiligheid?

Kennisveiligheid is het anticiperen op en het beheren van risico's in verband met:

a) de ongewenste overdracht van sensitieve kennis en technologie, die van invloed kan zijn op de nationale veiligheid en/of de wetenschappelijke positie van instellingen;
b) 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, waarmee inbreuk wordt gemaakt op de academische vrijheid en de integriteit van onderzoek en onderwijs in Nederland,
c) 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.

Toelichting

De driedeling hierboven is gebaseerd op de beschrijving van het begrip *onderzoeksveiligheid* in de Raadsaanbeveling onderzoeksveiligheid.[2] In deze leidraad wordt het meer gangbare (maar vergelijkbare) begrip kennisveiligheid gehanteerd. Een aantal termen uit de definitie worden hieronder verduidelijkt:

Academische vrijheid en wetenschappelijke integriteit

In het kennisveiligheidsbeleid staat het waarborgen van de vrije open wetenschap centraal. Veilig internationaal samenwerken is daarbij een belangrijk aspect. Essentiële kernwaarden van de vrije open wetenschap zijn internationale samenwerking, academische vrijheid en wetenschappelijke integriteit. Deze kernwaarden zijn van toepassing op alle Nederlandse kennisinstellingen. Ongeacht het type, de aard of de inrichting, en ongeacht of men spreekt over academisch, wetenschappelijk, klinisch, toegepast of praktijkgericht onderzoek.

Kennisveiligheidsrisico's kunnen deze kernwaarden ondermijnen en kunnen zich voordoen bij allerlei vormen van internationale wetenschappelijke samenwerking. Denk daarbij niet alleen aan de samenwerking met buitenlandse instellingen, maar ook aan uitwisselingen van studenten en onderzoekers, samenwerking met buitenlandse bedrijven, het ontvangen van gastonderzoekers en gastdocenten of het aannemen en aanstellen van personen met affiliaties met buitenlandse instellingen. Om de vrije open wetenschap te waarborgen, is het belangrijk de kennisveiligheidsrisico's te beheersen. Hoofdstuk 2 'Het beschermen van wetenschappelijke kernwaarden' gaat hier uitgebreid op in.

2 https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=OJ:C_202403510

Nationale veiligheid

Bij nationale veiligheid gaat het om het beschermen van de Nederlandse veiligheidsbelangen[3]. De Veiligheidsstrategie voor het Koninkrijk der Nederlanden identificeert zes veiligheidsbelangen binnen de nationale veiligheid:

1. Territoriale veiligheid
2. Fysieke veiligheid
3. Economische veiligheid
4. Ecologische veiligheid
5. Sociale en politieke stabiliteit
6. Internationale rechtsorde en stabiliteit

Ook binnen de context van kennisveiligheid kunnen deze veiligheidsbelangen in het geding zijn. Ze worden bijvoorbeeld aangetast als kennisoverdracht bijdraagt aan de militaire capaciteiten van een risicovolle statelijke actor, of wanneer het kan leiden tot een belemmering van de continuïteit van vitale processen[4].

Statelijke actoren

Kennisveiligheidsbeleid is bedoeld om onderwijs en wetenschap te beschermen tegen dreigingen vanuit statelijke actoren. Statelijke actoren zijn personen of (overheids-)organisaties die voor of namens een staat handelen. Hiermee worden in dit geval statelijke actoren bedoeld die een bedreiging vormen voor de nationale veiligheid, zoals jaarlijks wordt beschreven in het Dreigingsbeeld Statelijke Actoren (DBSA)[5]. Daarnaast gaat het bij kennisveiligheid ook om statelijke actoren met een slecht trackrecord op het gebied van mensenrechten, academische vrijheid en democratie.

Ook in Nederland zijn verschillende statelijke actoren actief op zoek naar kennis en technologie, vanuit de intentie om de eigen militaire, technologische, politieke en economische macht en capaciteiten te vergroten. Daarnaast vinden bij kennisinstellingen ook beïnvloedings- en inmengingsactiviteiten plaats door statelijke actoren. Daarbij probeert een actor bijvoorbeeld wetenschappelijk onderzoek te beïnvloeden en publicaties te censureren. Hierbij wordt misbruik gemaakt van de openheid van de Nederlandse kennisinstellingen en de in Nederland gegarandeerde academische vrijheid. Deze activiteiten zijn niet altijd gemakkelijk te herkennen. Vaak is er sprake van een glijdende schaal, waarbij het onderscheid tussen illegale activiteiten, heimelijke intenties en legitieme samenwerking niet altijd eenvoudig te maken is. In hoofdstuk 3 ‘Dreigingsbeeld’ zijn de dreigingen vanuit statelijke actoren uitgebreid beschreven.

Voorbeelden van risicovolle situaties

Ter illustratie een drietal voorbeeldsituaties waarbij kennisveiligheidsrisico’s zich kunnen voordoen. Deze casussen zijn fictief, maar instellingen en medewerkers kunnen met vergelijkbare casussen geconfronteerd worden. Deze leidraad geeft handvatten voor het omgaan met dergelijke situaties.

---

3 De Veiligheidsstrategie voor het Koninkrijk der Nederlanden: https://www.nctv.nl/onderwerpen/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden/documenten/publicaties/2023/04/03/veiligheidsstrategie-voor-het-koninkrijk-der-nederlanden

4 Overzicht vitale processen: https://www.nctv.nl/onderwerpen/vitale-infrastructuur/overzicht-vitale-processen

5 https://www.nctv.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025

Risico op ongewenste kennisoverdracht

Regelmatig zetten Nederlandse kennisinstellingen langdurige onderzoeksprojecten op met buitenlandse kennisinstellingen. Zulke samenwerkingen zijn zeer gebruikelijk. Maar soms heeft een samenwerkingspartner banden met een statelijke actor, waarvan dreiging uitgaat voor de Nederlandse (kennis)veiligheid. In de overeenkomsten die voorafgaand aan een samenwerking gesloten worden, worden lang niet altijd specifieke details opgenomen over het te uit te voeren onderzoek en de toepassing van de resultaten. Terwijl het wel van groot belang is hierover afspraken te maken. De opgedane kennis of het eindresultaat van het onderzoek, kan immers militaire toepassingen hebben, zoals bij (on)conventionele wapenprogramma's. En ook als het onderzoek in algemene zin niet gericht is op militaire toepassingen, kan dit risico zich voordoen.

Ook andere factoren van een samenwerking kunnen risicovol zijn. Zo kan de financiering van onderzoek ongewenste afhankelijkheden met zich meebrengen. En kunnen risico's zich voordoen bij wederzijdse bezoeken aan elkaars instellingen, bijvoorbeeld om gebruik te kunnen maken van hoogtechnologische wetenschappelijke onderzoeksinstrumenten.

Risico op heimelijke beïnvloeding

Regelmatig verwelkomen kennisinstellingen gastdocenten en gastonderzoekers, die mogelijk geaffilieerd zijn aan statelijke actoren die een risico vormen voor de kennisveiligheid. Zo'n statelijke actor kan belang hebben bij een bepaalde richting of interpretatie van het onderzoek en proberen invloed uit te oefenen op de eigen onderzoekers. Bijvoorbeeld als het onderzoek of onderwijs betrekking heeft op een ideologie die sterk geassocieerd wordt met een statelijke actor, of op onderwerpen die onderdeel zijn van internationale spanningen en kritiek. Extra risicovol wordt het, als de instelling waaraan de gastdocent of gastonderzoeker verbonden is, gefinancierd wordt door diezelfde statelijke actor.

Ethische kwesties

Ook ethische aspecten kunnen ervoor zorgen dat de kennisveiligheid in het geding komt. Stel, een Nederlandse kennisinstelling doet, in samenwerking met internationale partners, onderzoek naar het veilig inrichten en monitoren van de openbare ruimte. En stel, die internationale partners hebben banden met statelijke actoren met een slecht trackrecord op het gebied van mensenrechten, academische vrijheid en democratie. Dan bestaat het risico dat kennis en vaardigheden, die opgedaan zijn bij het onderzoek, kunnen worden ingezet voor bijvoorbeeld (massa)surveillanceprogramma's en het onderdrukken van bepaalde bevolkingsgroepen.

Een gezamenlijke opgave

Het structureel verhogen van veiligheidsbewustzijn en de weerbaarheid tegen kennisveiligheidsrisico's van de Nederlandse universiteiten, hogescholen en onderzoeksinstituten is van groot belang. Hierbij is de institutionele autonomie van de kennisinstellingen het uitgangspunt. Zelfregulering speelt dan ook een centrale rol. Dat betekent dat de kennissector zelf - binnen de wettelijke kaders - veiligheidsrisico's monitort, een aanpak formuleert, instrumenten ontwikkelt en zo actief mogelijk investeert in de weerbaarheid van de kennisinstellingen.

Organisaties zoals VH, UNL, KNAW, NWO, UMCNL en de TO2-federatie, kunnen daarbij een initiërende en faciliterende rol spelen, onder meer door instellingen met elkaar in gesprek te brengen en *best practices* in beeld te brengen en uit te wisselen. Zo beschikken UNL, NWO, KNAW, UMCNL en de TO2-federatie over eigen werkgroepen kennisveiligheid.

Rol van de Rijksoverheid

Het beschermen van de nationale veiligheid is een kerntaak van de overheid. Daarom is er ook voor de Rijksoverheid een actieve rol weggelegd. De Rijksoverheid werkt samen met de kennissector aan het bieden van handelingsperspectief. Daarmee kunnen kennisinstellingen zelf invulling geven aan de verantwoordelijkheid die zij op grond van hun - in Nederland wettelijk geborgde - institutionele autonomie hebben. Dit betekent dat de Rijksoverheid informeert, meedenkt, faciliteert en adviseert. Maar ook, waar dat vanwege de nationale veiligheid nodig is, kaders stelt en toeziet op de naleving daarvan.

Tussen de verschillende onderdelen van de overheid is sprake is van een *whole of government approach* op het gebied van kennisveiligheid. Dat betekent dat de overheid er naar streeft om als geheel eenduidig op samenhangende en verenigbare doelen te sturen.

Op een aantal onderdelen van het kennisveiligheidsbeleid zijn kennisinstellingen afhankelijk van de dienstverlening van de Rijksoverheid. Kennisinstellingen moeten redelijkerwijs in staat worden gesteld om succesvol invulling te geven aan hun verantwoordelijkheden. Daarom moeten instellingen kunnen vertrouwen op de tijdigheid en juistheid van adviezen, instructies en essentiële informatie.

De Rijksoverheid streeft in internationaal verband naar een gelijk wetenschappelijk speelveld, waarin verwante landen vergelijkbaar kennisveiligheidsbeleid voeren, zodat Nederlandse kennisinstellingen niet uit de markt geprijsd worden.

Rijksbreed Loket Kennisveiligheid

Om ervoor te zorgen dat kennisinstellingen met vragen over kennisveiligheid bij één centraal punt terecht kunnen, is er een Rijksbreed Loket Kennisveiligheid opgezet. Hierbij zijn alle relevante onderdelen van de Rijksoverheid aangesloten. Zo is de brede expertise van de ministeries en diensten op een centrale plek te raadplegen voor iedereen die binnen kennisinstellingen te maken heeft met internationale samenwerking en daarbij tegen dilemma's aanloopt. Het loket verstrekt informatie en adviseert. Deze informatie kan de instelling gebruiken bij het maken van de afweging tussen kansen en risico's.

Ook deze leidraad is een voorbeeld van de samenwerking tussen de kennissector en de Rijksoverheid om het veiligheidsbewustzijn te versterken. Het is een gezamenlijk initiatief van de Nederlandse kennissector (KNAW, NWO, UNL, VH, UMCNL en de TO2-federatie) en verschillende onderdelen van de Rijksoverheid (OCW, EZ, NCTV, BZ, AIVD en MIVD). Deze brede samenwerking laat zien dat kennisveiligheid een uitdaging is waarvoor we op nationaal niveau samen verantwoordelijkheid dragen.

Het dreigingsbeeld is dynamisch. Er is toenemende aandacht voor de risico's die daarmee samenhangen. Zowel nationaal als internationaal wordt nieuw beleid ontwikkeld. Deze leidraad is dan ook nadrukkelijk bedoeld als een levend document dat als basis kan dienen voor discussies met vakgenoten en experts en steeds wordt bijgewerkt als nieuwe ervaringen en inzichten daar aanleiding toe geven.

Hoofdstuk 2

Het beschermen van wetenschappelijke kernwaarden

Academische vrijheid, wetenschappelijke integriteit en openheid zijn belangrijke wetenschappelijke kernwaarden. Samen met het streven om inclusief, non-discriminatoir en in algemene zin ethisch te werken, vormen deze kernwaarden uitgangspunten van het handelen van kennisinstellingen.

Kennisveiligheidsbeleid heeft ten doel deze kernwaarden te beschermen tegen statelijke dreigingen. Veiligheidsbevorderende maatregelen zelf kunnen echter ook nadelig uitpakken voor deze kernwaarden. Om dat negatieve effect zoveel mogelijk te beperken, is een bewuste en zorgvuldige weging van belangen nodig. Dit hoofdstuk gaat in op de wetenschappelijke kernwaarden en op de soms complexe relatie tussen deze kernwaarden en kennisveiligheid.

2.1 Academische vrijheid

Academische vrijheid vormt het fundament voor het hoger onderwijs en de wetenschap in Nederland. Onderzoek in Nederland moet worden uitgevoerd in overeenstemming met de nationaal en internationaal aanvaarde normen van wetenschappelijk handelen. Het respecteren van deze kernwaarden is een voorwaarde om volwaardig mee te draaien in de academische gemeenschap.

Wat houdt academische vrijheid in?

Academische vrijheid houdt in dat medewerkers aan wetenschappelijke instellingen in vrijheid hun wetenschappelijk onderzoek kunnen doen, hun bevindingen naar buiten kunnen brengen en onderwijs kunnen geven[6]. Deze vrijheid geldt onder meer voor:

- de keuze van te onderzoeken thema's,
- de keuze en toepassing van de eigen onderzoeksvragen en -methoden,
- de toegang tot informatiebronnen,
- het publiceren en delen van informatie via conferenties, lezingen en lidmaatschap van wetenschappelijke groepen,
- de keuze om samenwerking met wetenschappelijke partners aan te gaan, en
- de invulling van het wetenschappelijk onderwijs.

Academische vrijheid is essentieel voor goede wetenschapsbeoefening en wettelijk geborgd in artikel 1.6 van de WHW en artikel 13 van het EU Handvest. Academische vrijheid kan hierbij niet losgekoppeld worden van professionele normen en waarden, zoals vastgelegd in de Nederlandse Gedragscode Wetenschappelijke Integriteit. Daarnaast bestaat academische vrijheid niet in isolatie, maar is zij ingebed in bredere verantwoordelijkheden voor instellingen en overheid, waaronder het beschermen van de nationale veiligheid. Instellingsbesturen kunnen oordelen dat bepaalde samenwerkingen een te groot risico opleveren voor de academische vrijheid. Daarnaast kan de overheid in zeer uitzonderlijke gevallen beperkingen stellen als er risico's zijn voor de nationale veiligheid. Hierbij moet een wettelijke grondslag voor de beperkingen aanwezig zijn, en moeten de beperkingen een legitiem doel dienen.

6 KNAW, 'Academischie vrijheid in Nederland: een begripsanalyse en richtsnoer', https://storage.knaw.nl/2022-05/20210217-webversie-advies-Academische-vrijheid.pdf

2.2 Gedragscodes wetenschappelijke integriteit

De Nederlandse kennissector is gebonden aan nationale en internationale gedragscodes op het gebied van wetenschappelijke integriteit. Deze codes zijn richtinggevend voor onderwijs en onderzoek in Nederland, óók als het gaat om activiteiten met buitenlandse partijen.

Daarmee bieden zij houvast bij het aangaan van internationale partnerschappen of onderzoeksprojecten, bijvoorbeeld bij het opstellen van een samenwerkingscontract met een internationale partner (zie hoofdstuk 5). Ook betekent het dat (gast)docenten en onderzoekers naar deze codes zullen moeten handelen, ongeacht waar ze vandaan komen.

Nederlandse gedragscode wetenschappelijke integriteit

De Nederlandse gedragscode wetenschappelijke integriteit is opgesteld door de kennissector (KNAW, UMCNL, NWO, TO2-federatie, VH en UNL). In deze code zijn de vijf principes die de grondslag vormen van integer onderzoek (eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid) uitgewerkt in 61 normen voor goede onderzoekspraktijken. Ook bevat de code richtlijnen hoe om te gaan met veronderstelde schendingen van de wetenschappelijke integriteit[7]. De Gedragscode benoemt dat wetenschappelijke integriteit raakvlakken heeft met Kennisveiligheid. Kennisveiligheid kan invloed hebben op de integriteit van onderzoek en andersom.

European Code of Conduct for Research Integrity

Er bestaat ook een Europese gedragscode: de *European Code of Conduct for Research Integrity*. Deze is uitgewerkt door ALLEA, de Europese Federatie van Wetenschapsacademies, waar vanuit Nederland de KNAW bij is aangesloten. De Europese Commissie erkent deze code als het referentiedocument voor wetenschappelijke integriteit voor alle door de EU gefinancierde onderzoeksprojecten en als een model voor organisaties en onderzoekers in heel Europa.

Diverse kennisinstellingen beschikken over eigen gedragscodes waarin de interne regels rond wetenschappelijke integriteit en/of veiligheid nader worden uitgewerkt. Zo hebben de Universitaire Medisch Centra zogenaamde research codes.

2.3 Open science

Nederland onderschrijft het Europese streven om onderzoeksresultaten die met publieke middelen zijn gefinancierd voor iedereen toegankelijk te maken. Denk aan het geven van *open access* tot publicaties en het FAIR (Findable, Accessible, Interoperable, Reusable) maken van onderzoeksdata. Het vrijelijk delen van nieuwe inzichten is een belangrijk uitgangspunt van wetenschapsbeoefening en een belangrijke aanjager voor de ontwikkeling van nieuwe kennis en innovaties.

Binnen de Europese Unie is afgesproken dat open science de norm wordt in wetenschappelijk onderzoek. Dat wil echter niet zeggen dat ook alle internationale partners op basis van open science werken. Bovendien kunnen er legitieme redenen zijn om sommige onderzoeksresultaten te beschermen en niet of slechts ten dele openbaar te maken. Denk daarbij aan privacy, nationale veiligheid, intellectueel eigendom en aan commerciële redenen.

---

7 In deze versie van de Leidraad wordt verwezen naar de NGWI uit 2018. Ten tijde van schrijven wordt de NGWI herschreven. Bij gebruik van de Leidraad is het raadzaam de laatste versie van de NGWI te raadplegen.

Het is belangrijk na te gaan of er beperkingen zitten aan de mate van openheid van onderzoek binnen de instelling en welke afspraken daarover gemaakt kunnen worden met uw internationale partners. Zo kan worden afgesproken of data mogen worden gedeeld of alleen kunnen worden ingezien (data visiting).

Rondom het delen van onderzoeksdata kunnen dilemma's ontstaan. Bijvoorbeeld wanneer subsidieverstrekkers eisen dat onderzoeksresultaten conform de principes van open science openbaar worden gemaakt, terwijl subsidieontvangers juist risico's signaleren voor de kennisveiligheid. Om te voorkomen dat instellingen om die reden terughoudend worden bij het indienen van aanvragen, is het van belang dat subsidieverstrekkers vroegtijdig met aanvragers verkennen onder welke voorwaarden publicatie verantwoord en veilig kan plaatsvinden. Door hierover vooraf proportionele en doeltreffende afspraken te maken kunt u voorkomen dat er later in het proces spanning ontstaat tussen het streven naar maximale openheid enerzijds en de legitieme redenen om beschermende maatregelen te treffen anderzijds.

2.4 Ethiek in de wetenschap

De rol van ethiek binnen de nationale aanpak kennisveiligheid beperkt zich tot die risico's die rechtstreeks zijn verbonden aan het gebruik van de betreffende kennis en technologie.

Bij internationale samenwerking kunnen, buiten de context van kennisveiligheid, ook andere ethische dilemma's een rol spelen.

Het is van belang om daar in alle lagen binnen uw instelling alert op te zijn en te blijven, zowel bij het aangaan van samenwerkingen als bij het verdere verloop van de samenwerking. Het is raadzaam om binnen uw instelling structuren voor ethisch beraad in te richten waar onderzoekers ethisch ingewikkelde internationale samenwerkingskwesties kunnen melden en bespreken. De minister van OCW heeft de universiteiten en hogescholen verzocht om bij het maken van ethische afwegingen een aantal uitgangspunten te hanteren. Zie hiervoor de brief die hij in mei 2024 aan de Tweede Kamer heeft gestuurd.[8]

2.5 Inclusiviteit en non-discriminatie

Nederlandse kennisinstellingen zijn verantwoordelijk voor een inclusieve en veilige leer- en werkomgeving voor studenten en medewerkers. Ze horen hun medewerkers, ongeacht hun functie, een veilige werkomgeving te bieden. Voor discriminatie is geen plaats aan Nederlandse kennisinstellingen[9]. Het kabinet werkt aan een wetsvoorstel rond de veiligheid in vervolgonderwijs en onderzoek (mbo, hbo en wo). Daarin wordt nadrukkelijker vastgelegd dat instellingen zorg moeten dragen voor de (sociale) veiligheid en hier ook beleid met een lerende cyclus voor moeten opstellen. Daarnaast zal het wetsvoorstel een aantal verplichtingen bevatten die dit ondersteunen. Denk daarbij aan de monitoring van de ervaren veiligheid op de instelling en de registratie van incidenten. Doel van het beleid is dat er continu aandacht is voor een veilige leer- en werkomgeving en dat hierover actief het gesprek wordt gevoerd, bijvoorbeeld met de medezeggenschap.

---

8 Bijlage bij Kamerbrief Stand van zaken omtrent de veiligheid op universiteiten en hogescholen n.a.v. de protesten over de situatie in Gaza. 31 mei 2024

9 Artikel 1 van de Grondwet

Zorgplicht kennisinstellingen

De zorgplicht voor onderzoekers wordt in de Nederlandse gedragscode wetenschappelijke integriteit als volgt weergegeven: “De instelling zorgt voor een werkomgeving waarbinnen goede onderzoekspraktijken worden bevorderd en gewaarborgd. De instelling zorgt ervoor dat onderzoekers kunnen werken in een veilige, inclusieve en open omgeving, waarin zij zich verantwoordelijk en aanspreekbaar voelen, dilemma’s kunnen delen en gemaakte fouten kunnen bespreken zonder bang te hoeven zijn voor de consequenties (blame-free reporting). De zorgplichten hebben betrekking op training en supervisie, onderzoekscultuur, databeheer, openbaarmaking en verspreiding en ethische normstelling en procedures.”[10]

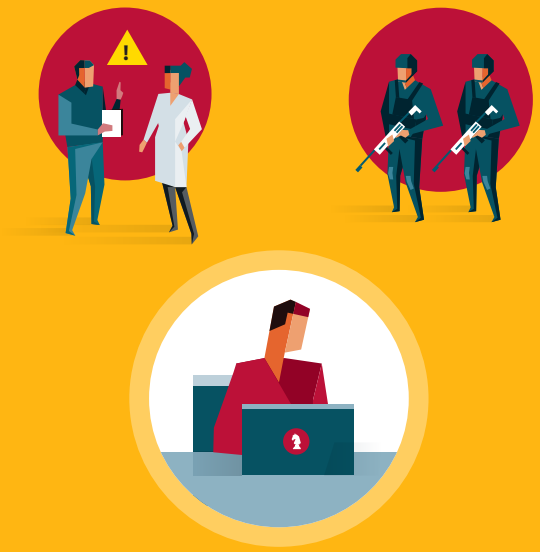
In de beleidsontwikkeling en berichtgeving rondom kennisveiligheid wordt vaak gebruik gemaakt van dreigingsanalyses en risicoprofielen waarin specifieke landen worden genoemd als bron van de dreiging. Hierbij ligt het gevaar op de loer dat het adresseren van kennisveiligheidsrisico’s kan leiden tot vooroordelen, stigmatisering en discriminatie. Dat moet te allen tijde voorkomen worden en vraagt om alertheid en bewustwording. Getroffen maatregelen moeten altijd objectiveerbaar en proportioneel zijn en gerelateerd worden aan een reëel gevaar. Voer hier een open gesprek over binnen uw instelling en neem signalen hierover altijd serieus. Zie ook Nationaal Actieplan voor meer diversiteit en inclusie.[11]

10 In deze versie van de Leidraad wordt verwezen naar de NGWI uit 2018. Ten tijde van schrijven wordt de NGWI herschreven. Bij gebruik van de Leidraad is het raadzaam de laatste versie van de NGWI te raadplegen.

11 Het Nationaal Actieplan DIHOO loopt eind 2026 af. Er wordt gewerkt aan een vervolg.

Hoofdstuk 3

Dreigingsbeeld



Ook Nederlandse kennisinstellingen kunnen doelwit zijn van pogingen om sensitieve kennis en technologie te verwerven.

Diverse statelijke actoren zijn, ook in ons land, actief op zoek naar kennis en technologie, met als doel de eigen militaire, politieke en economische macht te vergroten. Dat brengt risico's voor de Nederlandse nationale veiligheid met zich mee. Bijvoorbeeld omdat die statelijke actoren de overgedragen sensitieve kennis en technologie later inzetten voor doeleinden die direct de nationale veiligheid raken, bijvoorbeeld in de vorm van militair eindgebruik; of voor doeleinden die indruisen tegen onze kernwaarden.

Nederlandse kennisinstellingen en de open wetenschap kunnen hierbij door een statelijke actor als vehikel worden ingezet om dergelijke sensitieve kennis en technologie te verwerven.

In sommige landen wordt de wetenschap meer en meer onderworpen aan de strategische (militaire) belangen van de staat. Wetenschappelijke instellingen en individuele wetenschappers in deze landen werken (vrijwillig of onvrijwillig) samen met staatsprogramma's en krijgen allerlei verplichtingen opgelegd. Dit kan wetenschappelijke kernwaarden, zoals academische vrijheid, openheid en wederkerigheid schaden. Samenwerking met personen of instellingen die banden hebben met dit soort landen, brengt risico's met zich mee. Zeker als hun belangen tegengesteld zijn aan onze nationale veiligheidsbelangen.

Ook wanneer dit de nationale veiligheid niet op korte termijn ernstig schaadt, tast ongewenste overdracht van kennis en technologie op den duur de kennispositie en het innovatievermogen van Nederland aan. Bijvoorbeeld doordat instellingen hun sleutelposities in strategische ontwikkelingsprocessen verliezen. Als Nederland afhankelijk wordt van andere landen voor de toegang tot kennis, onderzoeksinfrastructuur en technologische goederen en diensten, is dat schadelijk voor de wetenschap.

Naast het verwerven van kennis en technologie, houden statelijke actoren zich ook bezig met beïnvloedings- en inmengingsactiviteiten bij kennisinstellingen. Daarbij probeert een actor bijvoorbeeld invloed te verwerven op meningen en publicaties, of worden pogingen gedaan wetenschappelijk onderzoek en onderzoeksresultaten te censureren.

Tot slot bestaat er een risico dat kennis, technologie, of de symbolische waarde van wetenschappelijke samenwerking zelf door statelijke actoren wordt misbruikt voor doelen die Nederlandse en Europese waarden en geldende verdragen schenden of ondermijnen.

Om het inzicht in bestaande dreigingen te verbreden en het bewustzijn te vergroten, wordt in dit hoofdstuk het huidige dreigingsbeeld geschetst. Niet elke dreiging zal voor kennisinstellingen zelf goed waarneembaar zijn. Heimelijke beïnvloeding is bijvoorbeeld vaak lastig te signaleren. Niet elke dreiging zal dan ook direct te adresseren zijn met kennisveiligheidsbeleid, of onder een strikte interpretatie van de definitie vallen. Dat neemt niet weg dat de informatie uit het onderstaande dreigingsbeeld van meerwaarde kan zijn voor het vergroten van het bewustzijn en het uitvoeren van risicoanalyses binnen een instelling.

3.1 Verwerving van kennis en technologie

Openlijke academische samenwerking kan door statelijke actoren worden ingezet om strategische kennis te verwerven die zowel voor civiele als voor militaire doeleinden kan worden gebruikt. Met beurzen en talentenprogramma's creëren zij financiële prikkels en afhankelijkheden. Studenten en wetenschappers worden bijvoorbeeld eerst gestimuleerd bepaalde kennis in het buitenland op te doen, en vervolgens gedwongen deze kennis in te zetten voor de statelijke actor in kwestie. Ook leggen sommige landen wettelijke verplichtingen op aan wetenschappers, waar zij zich tijdens de uitvoering van een samenwerking met een Nederlandse kennisinstelling aan moeten houden.

Associatie met (militair) strategische statelijke programma's

Het komt voor dat buitenlandse kennisinstellingen, studenten en wetenschappers geassocieerd zijn met (militair) strategische statelijke programma's in hun thuisland. Dit is extra waarschijnlijk in landen zoals China, Iran en Rusland, waar onderzoeksinstellingen vaker verweven zijn met het militair-industrieel complex of een bovengemiddeld hoge aansturing door de staat ondervinden. Zie hiervoor ook de meest recente versie van het DBSA. Soms worden kennisinstellingen zelfs direct door de overheid of krijgsmacht bestuurd.

De verwevenheid tussen een samenwerkingspartner en een statelijke actor is niet altijd goed zichtbaar. Kennisinstellingen, stichtingen of bedrijven kunnen deel zijn van een netwerk waarin zich ook staats-aangestuurde entiteiten bevinden. Ook dan bestaat het risico dat sensitieve informatie belandt bij een ongewenste statelijke eindgebruiker, bijvoorbeeld ten behoeve van de ontwikkeling van het militaire apparaat, de verbetering van digitale aanvallen of het gebruik van massasurveillance. Daarnaast kunnen er ook structurele banden bestaan tussen individuele studenten of onderzoekers en hoog-risico-entiteiten in landen van zorg. Deze banden zijn niet altijd onmiddellijk zichtbaar op een CV. In dergelijke gevallen is een directe link richting (militair) strategische statelijke programma's moeilijker te leggen.

Wet- en regelgeving

Sommige statelijke actoren beroepen zich op nationale wet- en regelgeving die onderdanen, organisaties en bedrijven verplicht mee te werken met nationale inlichtingen- en veiligheidsdiensten. Een samenwerking met een kennisinstelling kan betekenen dat de statelijke actor een claim kan leggen op onderzoeksresultaten of intellectueel eigendom. Resultaten of gegevens, afkomstig uit onderzoek dat door de Nederlandse kennisinstelling is opgezet en/of gefinancierd, kunnen in zo'n geval door een statelijke actor worden gekopieerd. Bijvoorbeeld doordat er gebruik wordt gemaakt van gedeelde laboratoria of andere gedeelde (fysieke/digitale) onderzoeksfaciliteiten. De Nederlandse kennisinstelling kan zich dan niet altijd op wettelijke bescherming beroepen, zeker niet als er sprake is van een samenwerking met een statelijke (aangestuurde) partner.

Beurzen en talentenprogramma's

Beursprogramma's kunnen door statelijke actoren worden ingezet om studenten en onderzoekers naar strategisch relevante onderzoeks- en opleidingsposities te sturen. Door voorwaarden op te nemen in zo'n programma creëert de statelijke actor een afhankelijkheid die gebruikt kan worden om een tegenprestatie van de bursaal te verkrijgen. Denk aan een verplichting om over de onderzoeksresultaten aan de statelijke actor te rapporten of om na afronding van het onderzoek een bepaalde baan aan te nemen. Daarin wordt iemand bijvoorbeeld gekoppeld aan defensie-gelieerde entiteiten en zo verplicht bij te dragen aan het realiseren van de militair-technologische ambities van de statelijke actor.

Wetenschappers zijn zich er niet altijd van bewust dat zij de interesse hebben van een statelijke actor. Een tegenprestatie wordt dan als standaardvoorwaarde gezien, of de persoon is simpelweg niet op de hoogte dat het onderzoek relevant is voor een (militair) strategisch statelijk programma.

3.1.1. Verwerving via gerekruteerde personen (insider risk)

Er zijn verschillende manieren waarop statelijke actoren proberen studenten, wetenschappers en andere relevante personen te rekruteren voor (het faciliteren van) kennis- en technologieverwerving. Dit kan op semi-openlijke en -legale manieren gebeuren, zoals door talentrekrutering. Maar er kan ook gebruik gemaakt worden van intimidatie of fêtering, om iemand te rekruteren voor het uitvoeren van aangestuurde handelingen.

Talentrekrutering

Statelijke actoren werven en faciliteren talentvolle studenten en wetenschappers om in hun land te komen studeren of te werken. Talentrekrutering is een normaal fenomeen binnen de wetenschap, maar kan ook een dreiging vormen. Bijvoorbeeld wanneer er sprake is van ondoorzichtige voorwaarden en landen van zorg talent werven voor onderzoek dat kan worden toegepast in (militair) strategische projecten. In landen zoals China en Rusland zijn bepaalde onderzoeksinstellingen verweven met het militair-industrieel complex of ondervinden een bovengemiddeld hoge aansturing door de staat. Dat brengt risico's met zich mee. Wetenschappers kunnen, tijdens of na de samenwerking met Nederland, uiteindelijk gekoppeld worden aan defensie-gelieerde entiteiten en onbedoeld bijdragen aan het realiseren van de militair-technologische ambities van de statelijke actor.

Ook gebeurt het dat studenten-, vak-, en beroepsverenigingen gevestigd in Nederland een rol spelen in het faciliteren van talentrekrutering. Verenigingen organiseren dan bijvoorbeeld evenementen zoals conferenties, lezingen of wedstrijden om talent te rekruteren, soms specifiek gericht op personen afkomstig uit het rekruterende land. Het aanbod om in buitenland te gaan werken wordt aantrekkelijk gemaakt door het verstrekken van beurzen en het creëren van gunstige onderzoeksfaciliteiten met bijvoorbeeld gespecialiseerde grote innovatiecentra. Niet altijd wordt daarbij duidelijk gemaakt dat men gaat werken voor een door de staat aangestuurd project.

Aangestuurde rekrutering

Eenmaal gerekruteerde personen kunnen voor een breed palet aan doeleinden worden ingezet. Soms helpen ze in kaart te brengen wie wat doet op een kennisinstelling, soms worden ze aangezet tot het aansturen van personen voor (het faciliteren van) illegale kennis- en technologieverwerving. Individuen op strategische posities binnen Nederlandse kennisinstellingen, kunnen vanwege hun eigen kennis, of hun toegang tot kennis, technologie of laboratoria, een interessant doelwit voor statelijke actoren vormen. Denk hierbij aan hoogleraren, (hoofd)docenten, post-docs, PhD'rs, studenten of medewerkers. Om deze personen te rekruteren, zetten statelijke actoren werkwijzen in als *social engineering*, financiële compensatie, chantage, intimidatie of fêtering (via statusverhogende of vleiende acties iemand belangrijk laten voelen met als doel een wederdienst te kunnen vragen). Gerekruteerden werken zeker niet altijd bewust, of uit vrije wil mee met een statelijke actor. Soms is iemand zich er zelfs niet van bewust dat hij te maken heeft met een partij die banden heeft met een statelijke actor. Rekrutering kan bovendien zeer geleidelijk plaatsvinden. Het doelwit wordt langzaam 'binnengehaald', over een soms langere periode, tot een moment dat de gerekruteerde geen weg meer terug heeft.

Van diverse statelijke actoren is bekend dat zij bereid zijn hun geëmigreerde (ex-) landgenoten te intimideren of te dwingen om zich te lenen voor de belangen van de staat. Sommige statelijke actoren (zoals China) beschikken over wet- en regelgeving die onderdanen, organisaties en bedrijven verplicht mee te werken met de nationale inlichtingen- en veiligheidsdiensten. Ook kunnen wetenschappers uit landen van zorg kwetsbaarder zijn voor druk uit hun thuisland, omdat zij daar vaak financiële en persoonlijke belangen hebben. In de praktijk blijken statelijke actoren er niet voor terug te schrikken naasten van het slachtoffer die zich nog in het thuisland bevinden onder druk te zetten en zo medewerking af te dwingen. Als er nog dienstplicht vervult moet worden in het thuisland, kan ook dat worden ingezet als drukmiddel om medewerking met de staat te forceren. Benadrukt moet worden dat niet alleen wetenschappers afkomstig uit landen van zorg een potentieel doelwit zijn. Zoals ook in de vorige paragraaf werd benoemd, kan iedereen die strategisch gepositioneerd is en zich bezighoudt met – of toegang heeft tot – sensitieve kennis en technologie een potentieel doelwit zijn van rekrutering door een statelijk actor.

Kennisverwerving via cybermiddelen

Net als iedereen die beschikt over waardevolle gedigitaliseerde kennis en informatie, kunnen ook studenten, onderzoekers en medewerkers van kennisinstellingen doelwit worden van digitale spionageactiviteiten van een statelijke actor. Van diverse statelijke actoren onderkennen de inlichtingen- en veiligheidsdiensten dat zij een offensief cyberprogramma hebben, dat ook gericht is tegen Nederlandse belangen. Sommige statelijke actoren voeren omvangrijke en structurele spionagecampagnes, gericht op het verkrijgen van hoogwaardige kennis en technologie. Daarbij richten zij zich ook op specifieke onderzoekers en medewerkers van een kennisinstelling, bij wie relevante informatie te vinden is. Met *(spear)phishing*-aanvallen gericht op een concreet doelwit kan dan bijvoorbeeld getracht worden toegang tot systemen en bestanden te krijgen. Het risico kan ook van binnenuit komen. Gerekruteerde personen kunnen een faciliterende rol spelen bij cyberaanvallen, bijvoorbeeld doordat zij een cyberactor toegang kunnen verlenen tot een netwerk. Dit soort mens-ondersteunde cyberaanvallen zijn des te gevaarlijker als er geen netwerksegmentering is en men zich via een onschuldige route toegang kan verschaffen tot sensitieve onderzoeksdata.

3.2 Beïnvloedings- en inmengingsactiviteiten

Sommige statelijke actoren zetten middelen in om invloed uit te kunnen oefenen op de wijze waarop zij internationaal gezien en begrepen worden, of worden geportretteerd. Ook doen bepaalde statelijke actoren pogingen om mondiale legitimatie te zoeken voor hun beleid. Studenten, onderzoekers en medewerkers aan Nederlandse kennisinstellingen kunnen doelwit worden van zulke inmengingsactiviteiten. Met name aan instituten waar onderzoek wordt gedaan naar voor een statelijke actor onwelgevallige onderwerpen, of onderwerpen waarvan de statelijke actor bang is dat er onwelgevallige bevindingen over worden gepubliceerd.

De manier waarop dergelijke invloed wordt uitgeoefend, verschilt. Er kan geprobeerd worden meningen en publicaties te beïnvloeden of wetenschappelijk onderzoek en onderzoeksresultaten te censureren. Het komt voor dat een actor hierbij gebruik maakt van financiële middelen als stimulans of juist als drukmiddel. Ook houden sommige actoren nauwlettend in de gaten of hun landgenoten aan Nederlandse kennisinstellingen geen *dissidente* of onwelgevallige meningen over het thuisland verkondigen, bijvoorbeeld tijdens colleges of congressen.

De druk die statelijke actoren hiermee uitoefenen, kan bij medewerkers aan Nederlandse kennisinstellingen leiden tot gevoelens van onveiligheid, onderling wantrouwen en zelfcensuur. Er zijn gevallen bekend waarbij studenten bang waren door hun medestudenten te worden gerapporteerd aan het herkomstland. Alleen al het idee dat hun herkomstland hen in de gaten kan houden, zorgt voor een gevoel van onveiligheid bij sommige studenten, onderzoekers, docenten en medewerkers. Dit kan leiden tot zelfcensuur, aantasting van de sociale veiligheid en ondermijning van wetenschappelijke kernwaarden. Het kan bovendien grote gevolgen hebben voor het algeheel welbevinden van slachtoffers. Dergelijke inmengingsactiviteiten vormen dan ook een bedreiging voor fundamentele vrijheden en wetenschappelijke integriteit.

Soms spelen dergelijke beïnvloedingsactiviteiten zich op onverwachte plekken af. Zo kunnen internationale studentenverenigingen worden ingezet als instrument voor repressie en monitoring van kritische diaspora en medestudenten.

Bij inmengingsactiviteiten gaat het lang niet altijd om repressie. Wetenschappelijke experts kunnen voor statelijke actoren aantrekkelijk zijn als geloofwaardige spreekbuis. Uit hoofde van hun expertise kunnen ze verleid worden om standpunten uit te dragen die in lijn zijn met de belangen van de actor. Zij worden bijvoorbeeld uitgenodigd om in bepaalde buitenlandse media een stuk te schrijven of om op symposia te spreken.

3.3 Ethische en integriteitschendingen

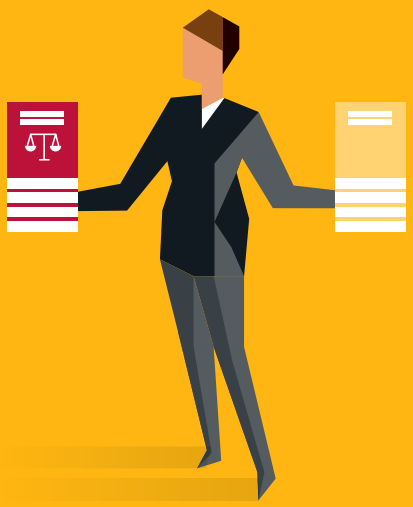
Het risico bestaat dat internationale academische samenwerking leidt tot schending van fundamentele (academische) waarden en verdragen in Nederland of daar buiten. Bijvoorbeeld als het gaat om bescherming van mensenrechten, de bescherming van klimaat en milieu, rechtstatelijke beginselen en andere democratische waarden, inclusie en diversiteit, bescherming van (cultureel) erfgoed, de positie van minderheidsgroepen en cultureel pluralisme.

Kennis en technologie die tijdens de samenwerking wordt verworven, kan door samenwerkingspartners en geaffilieerde (statelijke) actoren bedoeld of onbedoeld worden ingezet voor doelen en belangen die deze fundamentele waarden of verdragen schenden. Dat is niet alleen problematisch voor hen die hier rechtstreeks door getroffen worden, maar verzwakt ook in algemene zin de status en autoriteit en dus de beschermende werking die van deze waarden en verdragen uit gaat.

Het risico om betrokken te raken bij of bij te dragen aan ethische en integriteitsschendingen is groter bij samenwerkingen met partners in landen met een minder sterke rechtstaat, of met een slecht trackrecord op het gebied van mensenrechten, academische vrijheid en democratie. Zie hiervoor ook het overzicht van bronnen in hoofdstuk 5.2.

Hoofdstuk 4

Wettelijke kaders en richtlijnen



Zowel nationaal als internationaal bestaan er wettelijke kaders en richtlijnen die bijdragen aan de veiligheid van Nederland. Iedere instelling is verplicht zich aan de wet- en regelgeving te houden. Het zijn de harde kaders waarbinnen samenwerking met internationale partners dient plaats te vinden.

Dit hoofdstuk gaat in op wettelijke verplichtingen, zoals exportcontrole en sanctieregimes, maar ook op wetgeving die nog in voorbereiding is. Daarnaast is er aandacht voor verschillende gedragscodes die binnen de kennissector zijn uitgewerkt. Deze gedragscodes zijn richtinggevend en kunnen helpen bij het maken van afwegingen.

4.1 Sanctie- en dual-use verordeningen

Twee belangrijke wettelijke systematieken waar kennisinstellingen mee te maken hebben zijn sanctieverordeningen en dual-use verordeningen. Hoewel deze verordeningen onder meer toezien op de ongewenste overdracht van kennis en technologie, verschillen ze fundamenteel van het kennisveiligheidsbeleid. Tegelijkertijd spelen ze zich af in dezelfde context, en zijn in de praktijk vaak dezelfde personen en stafonderdelen betrokken bij de naleving.

De naleving van sanctieverordeningen en dual-use verordeningen is een losstaande opgave, waarbij de verordeningen zelf altijd het juridisch uitgangspunt vormen. In deze leidraad is dan ook geen handleiding voor deze opgave opgenomen. Om toch enig inzicht te geven in de verschillende opgaven en de verplichtingen die daar voor kennisinstellingen uit voortvloeien, worden hieronder een aantal hoofdlijnen geschetst.

Zowel sanctieverordeningen als dual-use verordeningen komen internationaal tot stand, vanuit de EU of de VN. Daarmee zijn ze rechtstreeks op wetenschappers en kennisinstellingen van toepassing zijn, en zijn wetenschappers en kennisinstellingen in principe ook zelf verantwoordelijk zijn voor de naleving van deze verordeningen.

Sanctieverordeningen

Sancties zijn primair bedoeld om het gedrag van de regering in een bepaald land te veranderen. Sanctieverordeningen richten zich op specifieke goederen, diensten, kennis en technologie, en op personen en andere entiteiten binnen een specifiek land. Voor ieder gesanctioneerd land is een eigen verordening van toepassing, waarin specifieke verboden en uitzonderingen staan opgenomen. Een actueel overzicht van geldende sanctieverordeningen kunt u vinden op de *EU Sanctions Map*[12]. Wat er precies gesanctioneerd is vindt u doorgaans terug in de bijlagen van de betreffende verordening.

Ook op specifieke personen en organisaties kunnen sancties van toepassing zijn. Het is belangrijk om dit te checken bij het aannemen of uitnodigen van personen en bij het aangaan van samenwerkingen.

Dual-use verordening

De dual-use verordening dient primair om te voorkomen dat Europese landen bijdragen aan de productie en ontwikkeling van massavernietigingswapens of militaire agressie, waar ook ter wereld. De dual-use verordening werkt op basis van een lijst van goederen en technologie.

12 https://www.sanctionsmap.eu/#/main

Wie onderdelen uit deze verordening uit wil voeren naar landen buiten de EU, dient daar een vergunning voor aan te vragen.

De goederen en technologieën waarvoor een vergunningplicht geldt vindt u in bijlage I en IV van de EU Dual-Use verordening (2021/821).

Technische bijstand

Voor zowel sanctieverordeningen als de dual-use verordening vormt technische bijstand een belangrijk onderdeel van de verboden of vergunningsplicht. Dat betekent dat het ook verboden of vergunningplichtig is om iets te leveren wat bijdraagt aan de installatie, het gebruik, de reparatie of het onderhoud van gesanctioneerde of vergunningsplichtige goederen of technologie.

Technische bijstand is een breed begrip. Het kan gaan om instructies, advies, opleiding, overdracht van praktische kennis, vaardigheden of adviesdiensten, ook in mondelinge vorm. Binnen de kennissector kan dit op allerlei plekken voorkomen. Bij het aanstellen van personeel, het delen van onderzoeksmethodes en resultaten, het opleiden van studenten, uitwisselingen van personeel, het organiseren en bijwonen van conferenties, enzovoort. Het leveren van verboden of vergunning plichtige technische bijstand verdient binnen kennisinstellingen dan ook bijzondere aandacht.

Verscherpt toezicht

Op een klein deel van de gesanctioneerde technologieën is verscherpt toezicht van toepassing. Dit geldt specifiek voor het risico op technische bijstand aan Noord-Korea, Iran, Belarus en Rusland. Voor studenten en onderzoekers die toegang willen tot bepaalde studies en werkzaamheden dient een ontheffing kennisembargo aangevraagd te worden. Voor wie en voor welke studies en werkzaamheden dit nodig is, kunt u vinden op de website van het Loket Kennisembargo[13]. Daar leest u ook hoe u een ontheffing kunt aanvragen.

Verorderingen van landen buiten Europa

Landen buiten Europa hanteren eigen exportcontroleregels. Het is belangrijk te vermelden dat de exportcontroleregels van de Verenigde Staten een extraterritoriale werking hebben. Hierbij worden de Amerikaanse exportcontroleregels niet alleen toegepast op goederen en diensten die in de VS zijn ontwikkeld of geproduceerd, maar ook op goederen en diensten waarin zich Amerikaanse componenten, software of technologie bevinden. Deze regeling wordt ook toegepast als dergelijke goederen en diensten buiten de VS zijn ontwikkeld.

Meer informatie

Met vragen over geldende sanctieregimes kunt u contact opnemen met het Rijksbreed Loket Kennisveiligheid. Let er hierbij wel op dat er door het loket geen onderzoek kan worden gedaan naar personen. Vanwege de strafrechtelijke aard van sanctiewetgeving is het bovendien niet mogelijk om specifieke casuïstiek te toetsen aan sanctieverordeningen en daar eenduidige uitspraken over te doen. Als u wilt weten of iets vergunningsplichtig is of onder een sanctieverordening valt kunt u een indelingsverzoek indienen bij de Centrale Dienst In- en Uitvoer (CDIU) van het ministerie van Buitenlandse Zaken[14].

---

13 https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies

14 https://www.douane.nl/kennisbank/documenten/aanvraag-indelingsverzoek/

4.2 Wet veiligheidstoets investeringen, fusies en overnames (Vifo)

Ook via buitenlandse investeringen, fusies of overnames waarbij Nederlandse bedrijven betrokken zijn, kan een statelijke actor sensitieve kennis bemachtigen. Om risico's voor de

nationale veiligheid te voorkomen, is in 2023 de Wet Veiligheidstoets investeringen, fusies en overnames (Wet Vifo) in werking getreden. Deze wet richt zich op vitale aanbieders en op bedrijven die beschikken over sensitieve technologie[15].

Kennisinstellingen kunnen bij de uitoefening van hun onderzoeks- en onderwijstaken met deze wet te maken krijgen. Bijvoorbeeld als ze een aandelenbelang hebben in startups van (oud-) studenten of medewerkers. Investeringen, fusies of overnames bij deze bedrijven kunnen binnen de reikwijdte van de veiligheidstoets vallen.

4.3 Wetsvoorstel screening kennisveiligheid

Voor de vakgebieden waar de risico's voor de nationale veiligheid het grootst zijn, werkt de Rijksoverheid aan het Wetsvoorstel screening kennisveiligheid. Personen die in Nederland met sensitieve kennis willen werken mogen dat straks pas doen nadat ze gescreend zijn door de overheid.[16] De wet moet ongewenste kennis- en technologieoverdracht via personen voorkomen en daarmee risico's voor de nationale veiligheid verminderen.

Het concept wetsvoorstel is april 2025 ter consultatie gepubliceerd[17]. De memorie van toelichting bevat uitgebreide onderbouwing en uitleg over de beoogde werking van het wetsvoorstel. In het wetsvoorstel is bovendien vastgelegd bij welke kennis- en technologiegebieden de risico's voor onze nationale veiligheid het grootst zijn.

4.4 Aanvullende codes, kaders, modellen en aanbevelingen

Richtlijnen zoals gedragscodes, kaders, modellen en aanbevelingen zijn in de regel niet-bindend, maar wel richtinggevend. Het zijn passende instrumenten voor de kennissector, die zich immers kenmerkt door een hoge mate van autonomie en zelfregulering. De Nederlandse kennissector neemt hierin zelf een proactieve rol, door zowel op eigen initiatief maatregelen te treffen als actief bij te dragen aan gezamenlijke initiatieven met de overheid. Hieronder volgt een aantal belangrijke Nederlandse en Europese richtlijnen.

Uniforme set risico-indicatoren

Een gelijk speelveld tussen kennisinstellingen in Nederland draagt bij aan het versterken van de weerbaarheid van de Nederlandse kennissector als geheel. Om dat te bereiken is het belangrijk dat kennisinstellingen onderling gebruik maken van een gemeenschappelijke basis voor het inschatten van risico's.

15 https://www.rvo.nl/onderwerpen/veilig-weerbaar-ondernemen/wet-vifo

16 Stand van zaken wetsvoorstel: https://wetgevingskalender.overheid.nl/Regeling/WGK025662

17 https://www.internetconsultatie.nl/screeningkennisveiligheid/

In 2025 zijn om deze reden de *Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid*[18] ontwikkeld, ook bekend als de 'set van uniforme risico-indicatoren'. Bestuurders en medewerkers van kennisinstellingen kunnen deze indicatoren gebruiken als referentie bij het inrichten of evalueren van een afwegingskader voor risicobeoordelingen. De indicatoren zijn ontwikkeld in samenwerking tussen de Rijksoverheid en het kennisveld. Ze zijn opgenomen in de bijlage van deze leidraad.

UNL kennisveiligheidskader en volwassenheidsmodel

Om universiteiten te ondersteunen bij de besluit- en beleidsvorming rond kennisveiligheid heeft UNL in 2021 op eigen initiatief een Kader Kennisveiligheid voor Universiteiten opgesteld. De tekst vormt een kader waaraan de Nederlandse universiteiten zich committeren en waarbinnen zij zelf invulling geven aan hun instellingsbeleid.

Het kader gaat in op kansen en risico's van internationale samenwerking, op governance en beleidskaders en doet concrete aanbevelingen rond risicomanagement. Daarmee stelt het universiteiten in staat goed geïnformeerde en onderbouwde beslissingen te nemen over internationale samenwerkingen.

In 2024 hebben universiteiten op aanbeveling van het AWTI-rapport 'Kennis in conflict' (2022) zelf een volwassenheidsmodel ontwikkeld. Dit volwassenheidsmodel is in april 2024 opgeleverd en helpt universiteiten bij het ontwikkelen, implementeren en evalueren van hun eigen kennisveiligheidsbeleid. Dit model dient als een intern hulpmiddel, gericht op het continu verbeteren van veiligheidsmaatregelen op academisch en institutioneel niveau.[19]

EU aanbevelingen en guidelines on tackling R&I foreign interference

De Europese Unie heeft een aanbeveling gedaan voor kennisinstellingen over het inrichten van interne compliance procedures. Deze aanbeveling is cruciaal voor het begrip van exportcontrole en dual-use in de context van wetenschappelijk onderzoek en kennisinstellingen.[20]

Bovendien heeft de Europese Raad in 2024 een aanbeveling over research security gepubliceerd[21]. In het document worden aanbevelingen gedaan die de Europese Commissie, de lidstaten en de Europese kennissector moeten ondersteunen in het versterken van hun kennisveiligheidsbeleid. De aanbevelingen kunnen helpen om kennisveiligheidsbeleid van EU-lidstaten op een vergelijkbaar niveau te brengen.

---

18 Zie appendix, maar ook hier: https://www.rijksoverheid.nl/documenten/rapporten/2025/06/13/bijlage-2-uniforme-set-risico-indicatoren-voorjaar-2025

19 https://www.universiteitenvannederland.nl/onderwerpen/onderzoek/kennisveiligheid. Het volwassenheidsmodel dient niet als grondslag van de vervolgmeting kennisveiligheid, waarbij in kaart wordt gebracht in welke mate de leidraad is geimplementeerd.

20 EU-aanbeveling voor kennisinstellingen over het inrichten van interne compliance procedures voor dual-use exportcontrole (2021): https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=-CELEX:32021H1700

21 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202403510

De Europese Commissie heeft ook een '*Staff Working Document Tackling R&I foreign interference*' uitgewerkt, gericht op het tegengaan van buitenlandse inmenging in de Europese kennissector[22]. Dit document is geschreven voor een brede doelgroep: nationale autoriteiten, onderzoeksinstellingen en -organisaties, instellingen voor hoger onderwijs, individuele onderzoekers en ander personeel van kennisinstellingen. Het document omvat vier thema's: waarden, governance, partnerschappen en cyberveiligheid. Per thema wordt een integrale aanpak gepresenteerd, met daarbij voorbeelden van mogelijke maatregelen die genomen kunnen worden.

Kennisveiligheid in andere landen

Ook andere landen nemen maatregelen om kennisveiligheid te verhogen. In diverse landen worden er richtlijnen en checklists ontwikkeld. Net als de Nederlandse Leidraad Kennisveiligheid zijn deze initiatieven bedoeld om inzichtelijk te maken waar op gelet moet worden bij internationale samenwerking en bieden ze handelingsperspectieven. Voorbeelden hiervan zijn: Australië, Duitsland, het Verenigd Koninkrijk, Zweden en Canada.

Het feit dat zowel de EU als individuele partnerlanden dergelijke teksten kennen, maakt het bij samenwerking makkelijker om het gesprek erover te voeren: ook onze partners zijn op zoek naar manieren om binnen het hoger onderwijs en de wetenschap alertheid en weerbaarheid tegen statelijke dreigingen te vergroten.

4.5 Wet open overheid

Iedereen heeft recht op informatie over wat de overheid doet, hoe ze dat doet en waarom. Als die informatie nog niet openbaar beschikbaar is moeten overheidsorganisaties die informatie uit zichzelf geven, of als iemand daarom vraagt (een Woo-verzoek). De informatie wordt dan openbaar. Dat is geregeld in de Wet open overheid (Woo).

Hoewel het verband wellicht niet direct voor de hand ligt, is ook de Wet open overheid relevant voor kennisveiligheid. De Woo is ook van toepassing op publiekrechtelijke kennisinstellingen. Openbare kennisinstellingen vallen zonder twijfel onder de Woo, omdat zij op grond van publiekrecht zijn ingesteld. Bijzondere universiteiten en hogescholen hebben een privaatrechtelijke grondslag. Zij vallen alleen onder de Woo wanneer zij openbaar gezag uitoefenen. Kennisinstellingen zijn zelf verantwoordelijk voor een correcte afhandelingen van Woo verzoeken.

Ook voor documenten over het kennisveiligheidsbeleid geldt openbaarheid als uitgangspunt. De Woo kent wel uitzonderingsgronden. Mocht iemand informatie opvragen die met kennisveiligheid te maken heeft, dan moet op documentniveau - en waar mogelijk op alineaniveau – beoordeeld worden of er uitzonderingsgronden van toepassing zijn. Deze uitzonderingsgronden kunt u vinden in hoofdstuk 5 van de Woo. Hieronder wordt een aantal gronden vermeld die specifiek bij kennisveiligheid relevant kunnen zijn.

Bij het toepassen van een uitzondering moet het algemeen belang van openbaarheid worden afgewogen tegen de belangen die de uitzonderingsgronden beschermen. Kennisinstellingen zijn zelf verantwoordelijk voor het maken van deze afweging.

22 EU guidelines on Tackling R&I foreign interference (2022): https://data.consilium.europa.eu/doc/document/ST-5396-2022-INIT/en/pdf

Voor kennisveiligheid relevante uitzonderingsgronden:

Persoonsgegevens

Persoonsgegevens worden (behoudens uitzonderingen) niet openbaar gemaakt op grond van artikel 5.1, tweede lid onder e van de Woo.

De veiligheid van de Staat, artikel 5.1, eerste lid, onder b van de Woo

Risico's op het gebied van kennisveiligheid, zoals de ongewenste overdracht van kennis en technologie, kunnen negatieve gevolgen hebben voor de veiligheid van de staat. Inzicht in documenten van een kennisinstelling, zoals risicoanalyses, lijsten van sensitieve kennisgebieden of overzichten van risicovolle internationale samenwerkingen, kunnen statelijke actoren daarbij helpen. Wanneer het openbaar maken van bepaalde informatie dit misbruik in de hand werkt en de veiligheid van de staat in het geding brengt, is er reden documenten niet openbaar te maken. Valt informatie onder de veiligheid van de staat, dan vormt dit een absolute weigeringsgrond. Dit betekent dat er geen ruimte is voor een verdere belangenafweging. U mag het stuk dan niet openbaar maken. Het is daarmee ook raadzaam om in dat geval deze weigeringsgrond toe te passen.

Internationale betrekkingen, artikel 5.1, tweede lid, onder a van de Woo

In veel documenten over kennisveiligheid worden relaties met andere landen benoemd. Dit raakt automatisch aan de internationale betrekkingen. Deze kunnen verslechteren wanneer deze landen merken dat Nederland hen bijvoorbeeld als 'risicovol' aanmerkt. Dit kan een reden zijn om bepaalde informatie niet openbaar te maken. Een optie is het betreffende land (of instelling/bedrijf) te 'lakken', maar het kan ook zo zijn dat er meerdere gegevens gelakt moeten worden. Belangrijk is steeds af te wegen of de internationale betrekkingen in het geding komen.

Let er hierbij op dat ook het vragen van zienswijzen aan partijen in andere landen in sommige gevallen kan leiden tot het verslechteren van de internationale betrekkingen.

Goed functioneren van de Staat, artikel 5.1, tweede lid onder i van de Woo

Het is belangrijk dat bestuursorganen veilig over kennisveiligheid kunnen communiceren met andere bestuursorganen. Dat geldt ook voor de communicatie tussen kennisinstellingen en de overheid. Als openbaarmaking er toe leidt dat dit niet langer op een veilige en vertrouwde manier kan plaatsvinden, bijvoorbeeld omdat andere partijen dan niet meer in gesprek willen met een instelling of de overheid, dan kan dit raken aan het goed functioneren van de Staat.

De overige uitzonderingsgronden van de Woo *kunnen* ook van toepassing zijn op stukken binnen het kennisveiligheidsbeleid van kennisinstellingen. Dit is compleet afhankelijk van de inhoud van de documenten. Het is te allen tijde belangrijk dat de beoordeling per document en zelfs op alineaniveau plaatsvindt en er een afweging wordt gemaakt. Uitgangspunt blijft: openbaar, tenzij.

Het kan voor kennisinstellingen lastig zijn om de gevolgen van openbaarmaking voor bijvoorbeeld de nationale veiligheid of de internationale betrekkingen goed in te schatten. Dit kan het moeilijk maken om het belang van openheid goed af te wegen tegen de verschillende uitzonderingsgronden. Voor advies in dit soort vraagstukken kunt u terecht bij het Rijksbreed Loket Kennisveiligheid.

4.6 Cyberveiligheid

Voor een effectieve bestrijding van cyberrisico's, zowel op het gebied van kennisveiligheid als in algemene zin, is samenwerking en continue kennis- en informatiedeling over risico's cruciaal. Voor wie zich met cyberveiligheid bezighoudt, vormen de beveiligingscommunity's van SURF een goed platform voor de uitwisseling van kennis, kaders, standaarden en ervaring. Denk hierbij aan de SURFnet Community of Incident Response Teams (SCIRT) en de SURF Community voor Informatiebeveiliging en Privacy (SCIPR).

Cyberbeveiligingswet

In 2025 heeft het kabinet besloten dat bekostigde hogescholen en universiteiten voortaan onder het toepassingsbereik van de Cyberbeveiligingswet[23] (Cbw) zullen vallen. Het doel van deze wet is om de Europese Network and Information Security directive, of NIS-2 richtlijn[24] in Nederland te implementeren. De NIS2-richtlijn is gericht op het verbeteren van de cyberbeveiliging en de weerbaarheid van essentiële diensten in EU-lidstaten.

Met de wet komt er een zorgplicht om passende en evenredige maatregelen te treffen voor het beheersen van de risico's rond de beveiliging van netwerk- en informatiesystemen. Onderdelen van de wet zijn verder: een meldplicht voor significante incidenten, recht op bijstand en advies van een Computer Incident Response Team (CSIRT) bij dreigingen en incidenten, een registratieplicht, en onafhankelijk extern toezicht op de naleving van genoemde plichten.

4.7 ABRO: Algemene Beveiligingseisen Rijksoverheid Opdrachten

Sinds 1 januari 2026 zijn de *Algemene Beveiligingseisen voor Rijksoverheidsopdrachten* (ABRO) ingevoerd. De ABRO bouwt voort op de ABDO (Algemene Beveiligingseisen voor Defensieopdrachten) uit 2019. Net als de ABDO is de ABRO een werkwijze en een uitgebreide set van veiligheidseisen. De ABRO is van toepassing op opdrachten voor de Rijksoverheid die raken aan de nationale veiligheid. Ook kennisinstellingen kunnen hier dus mee te maken krijgen.

Het Nationaal Bureau Industrieveiligheid (NBIV) controleert of een bedrijf of instelling zich houdt aan de in de ABRO gestelde eisen.

De kennisinstellingen die met ABDO of ABRO te maken hebben, hebben zeer robuuste risicomanagementprocessen moeten inrichten. Daardoor kunnen zij een inspiratiebron vormen voor kennisinstellingen die zelf geen defensieopdrachten uitvoeren, maar wel hun interne procedures en processen willen verstevigen.

23 https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie

24 https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/

Hoofdstuk 5

Het inschatten van risico's

Dit hoofdstuk biedt een aantal handvatten voor het in kaart brengen van risico's voor ongewenste kennisoverdracht. Hierbij spelen drie factoren een belangrijke rol:

- de inhoud van het onderzoek;
- de samenwerkingspartner;
- de samenwerkingsvorm.

Deze factoren hangen met elkaar samen. Bij het inventariseren van risico's dienen ze dan ook integraal bekeken te worden.

In 2025 hebben de Rijksoverheid en de kennissector gezamenlijk een set van indicatoren opgesteld voor het maken van risicoschattingen op het gebied van kennisveiligheid bij internationale samenwerkingen. Deze indicatoren vormen een concretisering van de aandachtspunten die worden beschreven in de leidraad. Ze vormen een minimale gemeenschappelijke basis, met als inzet het creëren van een gelijk speelveld in het Nederlandse hoger onderwijs en de wetenschap en het versterken van de weerbaarheid van de Nederlandse kennissector als geheel. De indicatoren zijn online te vinden en als appendix aan deze leidraad toegevoegd.[25]

5.1 Welke kennisgebieden binnen uw instelling hebben een verhoogd risico?

Het is van belang om binnen uw instelling nauwkeurig te identificeren op welke kennisgebieden er kennisveiligheidsrisico's van toepassing zijn.

Het risico op ongewenste overdracht van sensitieve kennis en technologie speelt met name voor kennis die specifiek voor militaire toepassingen, of voor dual-use technologieën ontwikkeld wordt (zie paragraaf 4.1). Het ministerie van OCW werkt aan een wetsvoorstel voor de invoering van een screeningsplicht, waarin een specifiekere lijst van sensitieve technologie is opgenomen. Instellingen kunnen hier alvast kennis van nemen via openbare internetconsultatie. Vanuit het perspectief van ongewenste kennis- en technologieoverdracht is deze lijst leidend. Hoewel het wetsvoorstel toeziet op de screening van personen, is deze lijst evenwel bruikbaar in de context van internationale samenwerkingen met organisaties. De lijst kan gedurende het wetstraject onderhevig zijn aan wijzigingen.

Risico's op de kwaadwillige invloed op onderzoek en onderwijs, zijn over het algemeen aan de orde bij onderwerpen die van invloed zijn op internationale beeldvorming rond bepaalde statelijke actoren, of onderwerpen waarbij statelijke actoren willen toezien op de loyaliteit van landgenoten. Zie daarvoor ook Hoofdstuk 3.2.

Tot slot kan voor sommige kennisgebieden sprake zijn van een verhoogd risico op onethische toepassing van onderzoeksresultaten, of op het risico dat in de onderzoekssamenwerking gebruik gemaakt wordt van onethische praktijken.

25 https://www.rijksoverheid.nl/documenten/rapporten/2025/06/13/bijlage-2-uniforme-set-risico-indicatoren-voorjaar-2025

Al deze risico's zijn nog groter op gebieden waarop Nederland of uw eigen instelling een unieke kennispositie heeft. Dit betreft bijvoorbeeld kennisgebieden waarop uw instelling een reputatie heeft opgebouwd en waarin onderzoek wordt verricht dat internationaal geldt als toonaangevend of excellent.

Kennisveiligheidsrisico's kunnen overlappen met dreigingen op het gebied van economische veiligheid als onderdeel van de nationale veiligheid (zie hiervoor ook hoofdstuk 1). Denk bijvoorbeeld aan kennisgebieden waarin gewerkt wordt met kennis en technologie die raakt aan de continuïteit van vitale processen waar Nederland van afhankelijk is, of wanneer kritieke kennis en technologie gebruikt kunnen worden als politiek drukmiddel. Het gaat daarbij voor kennisinstellingen dus niet om de bescherming van het verdienvermogen van Nederland.

U kunt per sensitief kennisgebied een korte risicoanalyse uitvoeren, niet alleen vanwege de nationale veiligheid, maar ook om de veiligheid van uw medewerkers, de wetenschappelijke kernwaarden en de reputatie van uw instelling te waarborgen. Stel uzelf daarbij een aantal vragen:

- Waar binnen uw instelling bevindt zich unieke, gevoelige kennis?
- Welke dreigingen spelen er?
- Welke maatregelen kunt u nemen om deze dreigingen af te wenden?

Bedenk daarbij dat kennis en technologie in de loop van de tijd meer of minder sensitief kan worden. Het is daarom raadzaam om te werken met een dynamische lijst met sensitieve kennisgebieden, die periodiek wordt herzien. Zie voor het inrichten van uw risicobeheer en mogelijke maatregelen voor verschillende dreigingen ook hoofdstuk 6.

5.2 Welke landen hebben een verhoogd risico?

Het is verstandig uit te gaan van een risicomanagementbeleid dat gericht is op dreigingen, ongeacht uit welk land ze komen. Richt u uw beleid uitsluitend op enkele 'risicolanden', dan ziet u mogelijk dreigingen over het hoofd. Dreigingen kunnen ook vanuit minder voor de hand liggende landen komen. Het is bovendien verstandig ervoor te waken dat niet alles wat aan 'risicolanden' verbonden is, op voorhand verdacht wordt gemaakt. Dat is slecht voor de wetenschap en in strijd met het non-discriminatie beginsel.

Als u een inschatting wilt maken van het risicoprofiel van een land, kunt u gebruikmaken van openbaar beschikbare dreigingsinformatie. Zo stellen de NCTV, AIVD en MIVD periodiek een gezamenlijk 'Dreigingsbeeld Statelijke Actoren' op. Ook de jaarverslagen van AIVD en MIVD bevatten actuele dreigingsinformatie. En kijk bijvoorbeeld op www.sanctionsmap.eu om te zien tegen welke landen er sancties gelden (zie ook paragraaf 4.2).

Daarnaast kunt u relevante internationale ranglijsten en indices van ngo's, onderzoeksinstituten en internationale organisaties raadplegen. Deze geven inzicht in de mate van academische vrijheid, vrijheid in het algemeen, de staat van de democratie en de rechtsstaat. Ze kunnen helpen bij het maken van een bredere afweging.

Scoort een land slecht op dergelijke ranglijsten, dan betekent dat niet zonder meer dat u niet kunt samenwerken met instellingen uit dit land. Ook met onderzoekers uit dergelijke landen kan in principe worden samengewerkt, mits u de juiste voorzorgsmaatregelen treft en u zich rekenschap geeft van de context waarbinnen de beoogde partner opereert. Zie hoofdstuk 6 voor meer informatie over risicomanagement.

In de 'Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid'[26] is een overzicht van relevante bronnen opgenomen. Deze indicatoren zijn als bijlage bij deze leidraad opgenomen.

5.3 Ken uw samenwerkingspartners, opdrachtgevers en financiers

Gaat u een nieuwe overeenkomst aan, of wordt een samenwerking verlengd? Dan is het van belang dat de betrokken onderzoeker of projectleider zich verdiept in de achtergrond van de buitenlandse partnerorganisatie of opdrachtgever. *Due diligence* is de term die daar internationaal voor gebruikt wordt. Wat is de wetenschappelijke reputatie van de instelling? Wie zijn er precies bij het project betrokken? Wie is de *ultimate beneficial owner* (UBO)? Hoe zit het met de kosten? Het is van belang dat u daarbij óók stilstaat bij kennisveiligheid.

Goed beschouwd is het altijd relevant om daar op te letten, maar het is pure noodzaak bij instellingen of bedrijven afkomstig uit landen met een hoog risicoprofiel (zie paragraaf 5.2) en bij samenwerkingen op sensitieve kennisgebieden (zie paragraaf 5.1). Ook hier is het raadzaam instellingen of bedrijven niet op voorhand categorisch uit te sluiten. Het gaat erom dat de betrokken medewerkers zich bewust zijn van de risico's en dreigingen en bewust maatregelen treffen om deze te beheersen.

Daarvoor hoeft diegene geen veiligheidsexpert te zijn: met alertheid en open bronnen kan men al een eind komen. Let daarbij scherp op signalen die erop kunnen wijzen dat er iets niet in de haak is. Bijvoorbeeld een samenwerkingspartner die bij niemand bekend is of waarover nauwelijks informatie te vinden is op internet. Is de beoogde partner wel bekend binnen uw organisatie of bij collega's van andere instellingen, dan kan navraag gedaan worden. Welke ervaringen hebben zij? Zijn er incidenten geweest? De veiligheidscoördinator van uw instelling kan helpen dit soort informatie boven tafel te krijgen. Waar u bijvoorbeeld op kunt letten:

- Is de partner verbonden aan de overheid? Denk bijvoorbeeld aan staatsgeleide bedrijven of instellingen.
- Is de partner verbonden aan het leger of aan de defensie-industrie?
- Zijn er sancties op de partner van toepassing?[27]
- Heeft de instelling een aantoonbare reputatie op het vakgebied waar het om gaat? Als expertise ontbreekt of onduidelijk is hoe de beoogde samenwerking aansluit op de normale activiteiten van de partner, is dat een reden tot alertheid.
- Wat voor onderzoek doen de bij de samenwerking betrokken onderzoekers nog meer? Zijn zij verbonden aan meerdere instellingen/organisaties?
- Hoe en met wie verloopt het contact over de samenwerking? Loopt het contact via een andere entiteit (andere naam, ander adres) dan de partnerorganisatie zelf, of verandert dit gaande het proces?
- Is duidelijk wat de voorwaarden zijn en hoe het onderzoek zal worden toegepast? Geeft de partner onduidelijke antwoorden op vragen over de beoogde toepassing van de onderzoeksuitkomsten? Maakt de partner om onduidelijke redenen bezwaar tegen gebruikelijke bepalingen in de overeenkomst of stelt de partner excessieve geheimhoudingsbepalingen voor?

26 https://www.rijksoverheid.nl/documenten/rapporten/2025/06/13/bijlage-2-uniforme-set-risico-indicatoren-voorjaar-2025

27 Het toezicht hierop is niet optioneel, maar een wettelijke verplichting. Zie hier over ook Hoofdstuk 4.

Er zijn gespecialiseerde onderzoeksbureaus actief, die veiligheidsgerelateerde analyses maken of due dilligence onderzoek kunnen doen. Let daarbij goed op hoe actueel en betrouwbaar de gegevens in de gemaakte analyses en gebruikte bronnen zijn.

Bij opdrachtgevers en onderzoeksfinanciers geldt iets vergelijkbaars als bij onderzoekspartners. Daarbij maakt het in beginsel niet uit om wat voor soort financier het gaat; het kan bijvoorbeeld ook gaan om schenkingen van donateurs. Begin met basale vragen als: waar komt het geld dat de partner wil investeren vandaan en wat zouden de motieven van de partner kunnen zijn om het onderzoek te financieren? Heeft de financier economische of politieke belangen bij een bepaalde uitkomst van het onderzoek? Een aantal signalen waar u bijvoorbeeld op kunt letten:

- Er is weinig tot geen informatie te vinden over de opdrachtgever of financier (geen website etc.).
- Er wordt gebruik gemaakt van een entiteit die atypisch is voor dit soort onderzoeksfinanciering.
- De opdrachtgever of financier stelt uitzonderlijk grote bedragen beschikbaar of stelt bijzonder gunstige financieringsvoorwaarden voor en vraagt daar amper iets voor terug.
- De opdrachtgever of financier wil niet dat resultaten worden gepubliceerd, stelt uitzonderlijk strenge intellectuele eigendomseisen of bedingt geheimhouding t.a.v. eindgebruikers en specificaties.

Bedenk daarbij dat u ook stap voor stap in een situatie van financiële of wetenschappelijke afhankelijkheid terecht kunt komen. Met de projecten en activiteiten afzonderlijk is dan weinig mis, maar bij elkaar opgeteld geven ze de financier een positie die hem in staat stelt de samenwerking en de inhoud ervan te sturen. De financier kan uw instelling en/of de betrokken onderzoekers persoonlijk onder druk zetten via zowel positieve prikkels (in het vooruitzicht stellen van beloningen) als via negatieve prikkels (bedreigingen).

Als u inschat dat aan de beoogde samenwerkingspartner, opdrachtgever of financier veiligheidsrisico's verbonden zijn, is het van belang de veiligheidscoördinator van uw organisatie te betrekken. Samen met hem/haar kunnen vervolgstappen worden overwogen. De uiteindelijke beslissing over het aangaan van de samenwerking, valt onder de verantwoordelijkheid van het centrale gezag van uw organisatie. Bij dat besluit worden veiligheidsrisico's expliciet meegewogen, als onderdeel van het partneracceptatiebeleid van de instelling.

5.4 Waar u op moet letten bij het aangaan van een samenwerking

Binnen het risicomanagement van uw kennisinstelling verdienen overeenkomsten met buitenlandse partners bijzondere aandacht. Door aan de voorkant duidelijke afspraken te maken, kunt u bepaalde risico's mitigeren én heeft u iets om op terug te vallen in gevallen dat het toch mis dreigt te gaan. Ook aan inkopen en aanbesteden kunnen risico's rond kennisveiligheid kleven. Risico's waar u -mits u ze tijdig signaleert- maatregelen tegen kunt nemen.

Samenwerking met buitenlandse instellingen of bedrijven kan op allerlei manieren ontstaan. Soms gaat dit heel vrijblijvend, via persoonlijke contacten van onderzoekers. Hoe een samenwerking ook tot stand komt, op het moment dat er inhoudelijke of financiële toezeggingen worden gedaan, is het belangrijk de afspraken wel in een overeenkomst vast te leggen.

Samenwerkingsovereenkomsten vormen een goed aangrijpingspunt voor het afwegen van kansen en risico's. Het sluiten of verlengen van een overeenkomst of het aanvaarden van een opdracht is bij uitstek een geschikt moment om een risicoanalyse uit te voeren en eventuele risico's te mitigeren. We hebben het hier over alle vormen van samenwerking, van breed tot specifiek.

Gaat uw instelling, of een onderdeel daarvan, een samenwerking aan met een buitenlandse kennisinstelling of een buitenlands bedrijf? Dan is het allereerst van belang grondig te onderzoeken met wie u precies in zee gaat (zie paragraaf 5.3). Vervolgens is het zaak duidelijke afspraken te maken, die de kennisveiligheidsrisico's zoveel mogelijk voorkomen. Doen zich gedurende de looptijd van de samenwerking onwenselijke ontwikkelingen voor, dan kunt u uw samenwerkingspartner erop aanspreken. Blijven de risico's voortbestaan, dan kunt u de samenwerking vroegtijdig beëindigen (exit strategie).

Formats en standaardovereenkomsten bieden een zekere basisbescherming tegen de meest voorkomende juridische en financiële risico's. Heeft u vastgesteld dat dit gaat om een samenwerking in een kennisgebied met een verhoogd risico? Dan zijn alleen juridische standaard-bepalingen in veel gevallen niet genoeg. En soms kunnen ook een grondige overeenkomst en andere mitigerende maatregelen niet voorkomen dat de restrisico's onacceptabel blijven voor de verantwoordelijke risico-eigenaar (veelal het college van bestuur). In dat geval is samenwerking niet mogelijk.

De Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid[28]kunnen u helpen om te bepalen op welke specifieke zaken u moet letten. Deze indicatoren zijn het product van samenwerking tussen de Rijksoverheid en de kennissector. De indicatoren zijn ook te vinden als appendix bij deze leidraad.

Is de overeenkomst eenmaal gesloten, dan komt het erop aan de gemaakte afspraken leidend te laten zijn. Dat vergt regelmatig overleg met de samenwerkingspartner, waarbij er niet alleen aandacht is voor de inhoudelijke voortgang, maar ook voor de *manier waarop* de samenwerking vorm krijgt. Knelpunten en incidenten moeten daarbij vroegtijdig worden aangekaart en geadresseerd. Het verdient aanbeveling om periodieke evaluaties van de samenwerking in te bouwen en vooraf af te spreken op welke onderwerpen er zal worden geëvalueerd.

Samenwerkingsovereenkomsten lopen na de initiële looptijd vaak stilzwijgend door. Wanneer de samenwerking zonder grote problemen is verlopen, is de neiging om geen aandacht te besteden aan zo'n verlengingsmoment. Bij samenwerkingen met een verhoogd risico is dat onverstandig. Het is raadzaam uw interne organisatie zó in te richten dat u ruim voor het verlengmoment een seintje krijgt en de samenwerking nog eens kritisch tegen het licht kunt houden. Mogelijk hebben zich sinds het afsluiten van de overeenkomst ontwikkelingen voorgedaan die extra mitigerende maatregelen of scherpere afbakeningen nodig maken.

28 Zie appendix.

5.5 Kennisveiligheid bij inkopen en aanbesteden

Aan sommige inkoopprocedures en aanbestedingen zijn veiligheidsrisico's verbonden. Dit hangt af van het type product of dienst dat wordt geleverd, van de opdrachtgever en van het bedrijf aan wie de opdracht wordt gegund. Denk bijvoorbeeld aan de aanbesteding van uw digitale infrastructuur, onderzoeksapparatuur, clouddiensten en software of de vervanging van systemen waar veel persoonsgegevens op staan. Daarnaast is voor sommige inkoopopdrachten fysieke toegang tot gevoelige locaties nodig, waarbij het goed is om beschermende maatregelen te treffen.

Bij een aanbesteding is het daarom zaak om eerst in kaart te brengen of dit soort risico's aanwezig zijn. Risico's kunnen gesignaleerd worden met behulp van de quickscan nationale veiligheid bij inkoop en aanbesteden. Dit instrument is ontwikkeld voor de Rijksoverheid en de vitale sector maar dient ook ter inspiratie voor andere sectoren. De quickscan bestaat uit een aantal vragen om snel te kunnen bepalen of er met de opdracht risico's ontstaan voor de nationale veiligheid of dat er eventueel nader onderzoek nodig is om dit te bepalen.

Te denken valt aan de volgende vragen:

- Is de te contracteren opdrachtnemer ingericht op de informatie waar hij mee moet werken?
- Weet de opdrachtnemer wat hij moet doen als beveiligingsincidenten zich voordoen en voldoen ook de onderaannemers aan de beveiligingseisen voor de opdracht?
- Kan er met de samenwerking of overeenkomst met een dergelijk bedrijf een strategische afhankelijkheid ontstaan?
- Kan er gevoelige informatie (zoals persoonsgegevens) weglekken?
- Kan de continuïteit van de levering in gevaar komen en wat zou dit voor gevolgen hebben?
- Komt personeel in aanraking met gevoelige informatie?
- Wat gebeurt er met de informatie na beëindiging van het contract?

Wanneer er een beeld is geschetst van de potentiële risico's van een opdracht kunnen er maatregelen worden getroffen. Te denken valt aan het stellen van aanvullende contracteisen of andere maatregelen gericht op risicomanagement (zie hoofdstuk 6) en het verhogen van de digitale weerbaarheid.

Hoofdstuk 6

Risicomanagement

Kennisveiligheid doet een groot beroep op de verantwoordelijkheid die kennisinstellingen op grond van hun institutionele autonomie hebben. Binnen de instelling is risicomanagement een gezamenlijke opgave, waar de hele organisatie zich verantwoordelijk voor moet voelen. Het doel is steeds ervoor te zorgen dat het kennisveiligheidsbewustzijn tot in de haarvaten van uw instelling doordringt. In dit hoofdstuk komen verschillende aspecten aan de orde die bijdragen aan een veiligheidscultuur en daarmee aan de weerbaarheid van uw organisatie.

Binnen een kennisinstelling is het bestuur eindverantwoordelijk voor risicomanagement. Dat geldt ook voor de risico's die samenhangen met kennisveiligheid. Kennisinstellingen dienen daarom interne procedures en protocollen te hebben, zodat zij risico's tijdig kunnen signaleren en adresseren.

Deze leidraad moet nadrukkelijk niet gelezen moet worden als oproep om alle risico's uit de weg te gaan. Het is echter wel essentieel om een goed begrip te hebben van de bestaande dreigingen en risico's en om deze op een effectieve manier te beheersen. Dit hoofdstuk biedt een aantal handvatten voor het inrichten van de governance en interne procedures.

6.1 Organiseer risicomanagement binnen uw organisatie

Kennisinstellingen kenmerken zich vaak door een gelaagde bestuursstructuur. Zowel op centraal instellingsniveau als op decentraal niveau is actie nodig om de kennisveiligheid te borgen. Duidelijke afspraken over wie waarvoor verantwoordelijk is, zijn dan ook belangrijk. Vanuit het uitgangspunt dat het bestuur van de kennisinstelling eindverantwoordelijkheid draagt, betekent dit dat het bestuur beslisbevoegdheden mandateert. Het is aan te raden om dergelijke mandatering formeel vast te leggen. In geval van incidenten of onregelmatigheden kan dan snel worden geschakeld.

Het kennisveiligheidsbeleid staat niet los van de andere elementen binnen de veiligheids-opgave van kennisinstellingen. Het is daarom van belang de benodigde processen in te richten in samenhang met andere (veiligheids)processen, op alle relevante niveaus binnen de organisatie.

Aan de hand van de informatie in deze leidraad, kan elke instelling een eigen uitwerking geven aan deze processen. Het is zaak al deze factoren en overwegingen om te zetten in werkwijzen, processen en structuren die rekening houden met de specifieke kenmerken van uw organisatie. Risicomanagement is maatwerk. Hoe hoger het risiconiveau, hoe strikter de benodigde risicoanalyses en controles, en hoe hoger en op centraler niveau de beslissingsbevoegdheid binnen de organisatie komt te liggen.

Bij het uitwerken van kennisveiligheidsmaatregelen is proportionaliteit essentieel. Er moet een gezonde verhouding zijn tussen de dreiging en risico's enerzijds en de getroffen maatregelen anderzijds. Dat het nemen van te weinig maatregelen onwenselijk is, spreekt voor zich. Maar ook het treffen van te veel, verkeerde of te ingrijpende maatregelen kan nadelig uitpakken. Denk aan bureaucratie door een overdaad aan controle en wantrouwen. Maar ook aan het belemmeren van kansen en mogelijkheden en de aantasting van uw academische reputatie als openheid en toegankelijkheid al te zeer worden beperkt. Het adagium 'open waar mogelijk, beschermen waar nodig' vat het belang van proportionaliteit goed samen.

6.2 Organisatorische maatregelen

Uiteindelijk is het doel te komen tot een integraal veiligheidsbeleid op instellingsniveau; een beleid waarin de verschillende elementen van veiligheid in samenhang georganiseerd zijn. Het Platform Integrale Veiligheid Hoger Onderwijs[29] biedt veel aanknopingspunten en mogelijkheden voor de ontwikkeling van integrale veiligheid binnen het hoger onderwijs.

Kennisveiligheid heeft een strategisch en geopolitiek karakter en is meer dan een bedrijfsvoeringskwestie. Het vergt aandacht op bestuursniveau. Het inrichten van kennisveiligheidsbeleid begint dan ook concreet met het aanwijzen van een bestuurlijke trekker of portefeuillehouder voor het thema kennisveiligheid. Deze portefeuillehouder kan de inrichting en uitvoering van het kennisveiligheidsbeleid op strategisch niveau van sturing voorzien.

De exacte wijze waarop een instelling vervolgens invulling geeft aan het kennisveiligheidsbeleid, is aan de instelling zelf. Er kunnen verschillen bestaan tussen instellingen, afhankelijk van hoe instellingen ingericht en georganiseerd zijn. Ook de manier waarop risicoanalyses zijn ingericht, kunnen tussen instellingen verschillende eisen stellen aan doelmatig en effectief kennisveiligheidsbeleid. Het beleid dient wel zo te zijn ingericht, dat het de instelling in staat stelt adequaat om te gaan met de verschillende kennisveiligheidsrisico's.

Aanbevolen wordt dat de bestuurlijke portefeuillehouder kennisveiligheid wordt bijgestaan en geadviseerd door een intern Adviesteam Kennisveiligheid; een team van deskundigen met uiteenlopende expertises. In de kern kan gedacht worden aan: (1) de kennisveiligheidscoördinator, (2) de veiligheidscoördinator of adviseur integrale veiligheid; (3) een expert op het gebied van informatiebeveiliging, bijvoorbeeld de Chief Information Security Officer (CISO); en (4) een deskundige op het gebied van internationalisering/ internationale samenwerking. Afhankelijk van de casuïstiek kan daar andere expertise aan worden toegevoegd, zoals een HR-adviseur. Dit adviesteam heeft bij voorkeur een formeel mandaat om het bestuur gevraagd en ongevraagd te informeren en adviseren over kennisveiligheidsissues. Met name voor kleinere kennisinstellingen kan het interessant zijn om bepaalde expertise, bijvoorbeeld met betrekking tot bepaalde landen of kennisvelden, te bundelen en te werken met een *shared service*.

Het is van belang dat er binnen uw organisatie een open veiligheidscultuur bestaat (zie hierna, paragraaf 6.5). In aanvulling daarop is het aan te raden te werken met vertrouwenspersonen of ombudsfunctionarissen en om over een goede klokkenluidersregeling te beschikken. Dit regelt dat medewerkers vermoedens van illegale of onethische praktijken binnen de instelling (anoniem en in vertrouwen) kunnen melden. Medewerkers die zorgen hebben over kennisveiligheid, bijvoorbeeld bij ernstige twijfels over de risicobeoordeling van een samenwerkingsovereenkomst, moeten weten dat zij bij een vertrouwenspersoon of ombudsfuctionaris terecht kunnen om die zorgen te bespreken. Het is raadzaam dat de vertrouwenspersonen en ombudsfunctionarissen zelf goed op de hoogte zijn van risico's rond kennisveiligheid en hun kennis hierover periodiek bijspijkeren.

Het is uiteraard ook verstandig om er voor te zorgen dat medewerkers van de instelling terecht kunnen bij kennisveiligheidsadviesteams of -coördinatoren zelf wanneer er geen noodzaak is voor vertrouwelijkheid, of voor de tussenkomst van een onafhankelijke partij.

29 https://integraalveilig-ho.nl/

6.3 Zorg voor een accurate feitenbasis voor besluitvorming

Omdat bestuurders binnen kennisinstellingen eindverantwoordelijk zijn voor het risicomanagement van de gehele instelling, is het belangrijk dat zij beschikken over de juiste informatie. Daarom wordt aanbevolen dat bestuurders minimaal eens per jaar een actueel en compleet overzicht krijgen van risicovolle internationale partnerschappen die betrekking hebben op onderzoek en onderwijs. Dit geldt voor alle relevante typen kennisveiligheidsrisico's, dus zowel voor ongewenste overdracht van kennis en technologie, als kwaadwillige invloed op onderzoek en ethische en integriteitsschendingen. Bestuurders kunnen het overzicht tussentijds altijd raadplegen. De instellingen waarborgen de actualiteit en de vertrouwelijkheid van de overzichten.

Zoals gezegd kennen kennisinstellingen op grond van hun institutionele autonomie veel vrijheid en eigen verantwoordelijkheid bij de inrichting van hun risicomanagement. De precieze vorm van een dergelijk overzicht, en de precieze rol die dat overzicht speelt binnen het risicomanagement, kan dan ook verschillen. Dit is afhankelijk van de behoeften en vereisten die voortvloeien uit de aard van de instelling en de wijze waarop het risicomanagement binnen die instelling is ingericht. Een overzicht van risicovolle samenwerkingen is geen verantwoordingsinstrument en is niet bedoeld voor openbaarmaking. Zo kan een instelling vertrouwelijke informatie opnemen in het overzicht, die van belang kan zijn voor de risicobeheersing. Zie Hoofdstuk 4.6 voor meer informatie over de omgang met vertrouwelijke informatie binnen het kennisveiligheidsbeleid.

Binnen deze vrijheid is het de bedoeling dat het overzicht een bestuurder ten minste in staat stelt om periodiek een inschatting te maken van de cumulatieve risico's die voortkomen uit het geheel van lopende en voorgenomen samenwerkingen. Bijvoorbeeld als het gaat om ongewenste afhankelijkheid van buitenlandse kennis, infrastructuur of investeringen.

Het is dan ook raadzaam om in het overzicht ten minste alle lopende meerjarige samenwerkingen op te nemen tussen organisaties of organisatieonderdelen op het gebied van de geïdentificeerde risicovolle vakgebieden binnen de instelling (zie hoofdstuk 5). Daarbij moet sprake zijn van één of meerdere partners van buiten de Europese Unie en van een vastgestelde overeenkomst of een investering (in bijvoorbeeld financiering, personeel of materieel) van één of beide partners.

De hierboven genoemde aanbevelingen bieden houvast, maar vragen ook veel verantwoordelijkheid van kennisinstellingen voor een eigen afweging. Een gedegen overzicht vraagt om een context-afhankelijke invulling van kennisinstellingen ten aanzien van:

1. **Omvang van de risico's.**
   Er is geen eenduidig onderscheid tussen relevante en irrelevante risico's. Of een risico groot genoeg is om van belang te zijn voor de risicobeheersing kan bijvoorbeeld verschillen tussen instellingen, vakgebieden en type risico's.
2. **Aard van de samenwerking.**
   Binnen de wetenschap bestaat er een grote variëteit aan manieren om samen te werken. Welke typen van samenwerking precies relevant zijn voor de risicobeheersing kan verschillen tussen instellingen, vakgebieden en type risico's.
3. **Aard van het buitenlands belang.**
   Naast volledig buitenlandse instellingen kan er ook op andere manieren sprake zijn van een buitenlands belang bij samenwerkingspartners. Denk daarbij bijvoorbeeld ook aan de samenwerking met bedrijven met gedeelde eigendoms- en aandeelhoudersstructuren. De mate waarin een buitenlands belang relevant is voor de risicobeheersing kan dan ook verschillen tussen vakgebieden en typen risico's.

6.4 Veiligheidsbevorderende maatregelen

Fysieke en digitale beschermingsmaatregelen

Naast organisatorische en administratieve maatregelen kunnen ook fysieke en digitale beschermingsmaatregelen effectief zijn. Welke gebouwen zijn vrij toegankelijk en voor welke verdiepingen of ruimtes geldt een restrictief toegangsbeleid? Zorg dat plekken waar sensitief onderzoek wordt gedaan, zoals labs, alleen toegankelijk zijn voor diegenen die bij het onderzoek betrokken zijn.

Dat geldt evenzeer voor onderzoeksgegevens. Wie heeft er binnen het systeem toegang toe? Welke gegevens en resultaten moeten worden afgeschermd voor vakgenoten en collega's die niet bij het onderzoek betrokken zijn? Het (digitaal) afschermen van gegevens en het beperken van de toegang tot personen die geautoriseerd zijn, is een effectieve en relatief eenvoudige manier om ongewenst weglekken te voorkomen.

Heeft u binnen uw instelling te maken met zeer sensitieve onderzoeksdata of -resultaten? Dan valt te overwegen om te werken met rubricering van documenten. Dat betekent dat documenten worden ingedeeld in een gevoeligheidsklasse, zoals 'vertrouwelijk' of 'geheim'. Door het aanbrengen van rubriceringen op documenten kent iedere medewerker de gevoeligheid van de informatie en de daaraan gekoppelde maatregelen. Het zorgt dat iedereen binnen de organisatie dezelfde taal spreekt als het gaat om vertrouwelijkheid van informatie en verkleint zo de kans dat gevoelige kennis weglekt.

Het verhogen van de weerbaarheid tegen ongewenste overdracht van kennis en technologie, vraagt om volwassenheid op het gebied van informatiebeveiliging binnen kennisinstellingen. Specifiek bij organisatieonderdelen waar kennis of technologie wordt ontwikkeld die voor een statelijke actor van waarde kan zijn.

Informatiebeveiliging kent verschillende niveaus van weerbaarheid. Hier bestaan diverse volwassenheidsmodellen voor. Om voldoende weerbaar te zijn tegen de intensievere dreiging van dit moment, is de inschatting dat kennisinstellingen of losse organisatieonderdelen minimaal dienen te voldoen aan volwassenheidsniveau 3 van het NIST Framework of volwassenheidsniveau 4 van het NBA Volwassenheidsmodel Informatiebeveiliging. De lagere volwassenheidsniveaus bieden onvoldoende weerstand tegen een gerichte statelijke dreiging.

Algemene maatregelen bij het aangaan van samenwerkingen

Bij het aangaan van samenwerkingen kunt u een aantal maatregelen nemen om de specifieke risico's te beheersen. Zie paragraaf 5.4 voor meer informatie over waar u op kunt letten bij het aangaan van samenwerkingen.

- Beding dat het onderzoek wordt uitgevoerd in overeenstemming met internationaal aanvaarde normen van wetenschappelijk handelen, zoals neergelegd in (inter)nationale gedragscodes, zoals de Nederlandse Gedragscode Wetenschappelijke Integriteit (zie paragraaf 2.1).

- Zorg dat de overeenkomst duidelijk geformuleerde ontbindende voorwaarden bevat. Deze bepalingen geven u het recht de samenwerking vroegtijdig te beëindigen als zich zaken voordoen die voor u niet door de beugel kunnen. Ook een bepaling over geschillenbeslechting (dispute settlement), kan daarin handig zijn.

- Bepaal vooraf gezamenlijk welke toegang wenselijk is voor de partner. Tot welke gebouwen, informatie of interne netwerken krijgt de partner toegang? Wat wordt met de partner gedeeld? Wordt toegang gegeven tot een volledig product of tot een 'light' versie zonder gevoeligheden? Het is verstandig hier vooraf duidelijke afspraken over te maken. Leg ze zo nodig vast.

- Ga na of de samenwerking betrekking heeft op dual-use-technologie (zie paragraaf 4.1). Is dat het geval, dan is een eindgebruikersverklaring wenselijk. Dit is een door de eindgebruiker ondertekend document waarin diegene verklaart dat hij/zij de goederen niet anders dan voor civiele doeleinden zal gebruiken. De eindgebruikersverklaring wordt ook wel een *End User Statement* (EUS) genoemd.

Maatregelen kwaadwillige invloed onderzoek en onderwijs

Het tegengaan van kwaadwillige invloed op onderzoek en onderwijs kan voor kennisinstellingen lastig zijn. Statelijke actoren kunnen individuele wetenschappers op verschillende manieren onder druk zetten of verleiden. Het is niet vanzelfsprekend dat een doelwit van heimelijke beïnvloeding daarbij steun vanuit de Nederlandse instelling wenst, of de stap daartoe durft te zetten. Evenmin kan worden aangenomen dat kennisinstellingen in staat zijn om de dreiging vanuit de statelijke actor weg te nemen.

Bewustwording binnen risicogebieden kan helpen voorkomen dat slachtoffers door druk of verleiding worden beïnvloed. Bovendien zijn er gevallen bekend van onder druk gezette slachtoffers die zich wèl melden en op zoek gaan naar steun en begeleiding vanuit de instelling. Daarom, maar ook voor het uitvoeren van risicoanalyses, is het nuttig dat instellingen enig inzicht te hebben in de problematiek, daar waar die wel aan het oppervlak komt.

Hoewel dit de dreiging zelf niet weg kan nemen, kan zo wel een bijdrage worden geleverd aan de (sociale) veiligheid van wetenschappers en studenten en aan het vergroten van de weerbaarheid tegen de kwaadwillige invloed van statelijke actoren op onderzoek en onderwijs. De Rijksoverheid en de koepels werken met elkaar aan meer bewustwording en handelingsperspectieven op dit thema, in het kader van de aanpak kennisveiligheid.

Maatregelen ethische kwesties en integriteitsschendingen

Om de weerbaarheid te vergroten tegen het risico op de schending van fundamentele waarden en verdragen kunt u aantal maatregelen overwegen. Net als bij de andere risico's is het ook hier van belang dat onderzoekers en docenten zich bewust zijn en dat er duidelijke processen en afspraken zijn over het signaleren en adresseren van deze risico's. Hiervoor kunt u denken aan trainingen, campagnes en de beschikbaarheid van toegankelijke informatie.

In paragraaf 2.3 is een van de concrete handelingsperspectieven beschreven: binnen uw instelling structuren inrichten voor ethisch beraad. Zo'n beraad kan adviseren over kwesties die samenhangen met het risico dat landen onderzoeksresultaten toepassen op een manier die mogelijk indruist tegen fundamentele normen en waarden, zoals mensenrechten.

6.5 Veiligheidscultuur: bewustwording en alertheid

Het creëren van een open veiligheidscultuur binnen uw organisatie is essentieel als het gaat om bewustzijn (incident- en risicodetectie) en weerbaarheid. Mensen moeten open en in vertrouwen met elkaar over mogelijke risico's kunnen spreken en ervan doordrongen zijn dat interne veiligheidsprocedures er niet voor niks zijn. Bied ruimte voor het uiten van zorgen en denk actief mee over wat er kan worden verbeterd. Veiligheid mag niet iets zijn waar alleen de bestuurders en de kennisveiligheidscoördinator het over hebben.

Campagnes kunnen een nuttige bijdrage leveren aan het vergroten van het bewustzijn. Zo kunt u ervoor zorgen dat de boodschap van deze leidraad wordt overgebracht op een manier die aansluit bij de behoeften van uw organisatie.

Bewustwording is echter nooit een eenmalige exercitie: doorlopende aandacht is nodig om iedereen scherp te houden en ook nieuwe medewerkers mee te krijgen. Ook is kennisveiligheid -en het denken daarover- volop in beweging. Het is dus belangrijk kennis up-to-date te houden.

Daarbij kunt u gebruikmaken van input en expertise die binnen de Rijksoverheid en organisaties als UNL en de TO2-federatie voorhanden is. Zij kunnen bijvoorbeeld een platform bieden waar u van ervaringen binnen andere kennisinstellingen kunt leren en waarvan u wellicht nuttige instrumenten en checklists kunt overnemen. Het Loket Kennisveiligheid speelt hierin een centrale rol.

Naast de adviezen die het loket geeft over algemene vraagstukken en concrete casuïstiek, beheert het loket ook een 'learning community'. Doel van de learning community is om expertise vanuit de Rijksoverheid te delen met kennisinstellingen en met specifieke doelgroepen daarbinnen, bijvoorbeeld juristen of HR-medewerkers van kennisinstellingen. Daarnaast is de learning community bedoeld om expertise van kennisinstellingen te delen en samen te brengen. Op het beveiligde platform van de learning community is een uitgebreide kennisbank te vinden. Daarin wordt veel relevante informatie gedeeld, maar zijn ook good practices van kennisinstellingen te vinden. De learning community organiseert tevens thema-bijeenkomsten en webinars en ontwikkelt materialen als campagnes, e-learnings en interactieve workshops die door kennisinstellingen vrij te gebruiken zijn.

Zorg er bij een bewustwordingscampagne altijd voor dat deze is toegesneden op de beoogde doelen en doelgroepen (onderzoekers, projectleiders, ondersteunende diensten, etc.). Sluit zo veel mogelijk aan bij hun belevingswereld. Een effectieve campagne gebruikt meerdere kanalen en ingangen. Denk bijvoorbeeld aan informeren via posts op intranet, e-mails en e-learning modules en interactieve bijeenkomsten en teamsessies. Ook simulaties, waar (fictieve) casuïstiek wordt doorlopen, zijn zeer geschikt om houdings- en gedragsaspecten te trainen.

Denk ook na over wie de boodschap binnen de organisatie overbrengt. Essentieel is dat het management het goede voorbeeld geeft en uitstraalt kennisveiligheid belangrijk te vinden. In aanvulling daarop kunnen bijvoorbeeld ambassadeurs binnen de organisatie worden aangewezen die de boodschap actief verder verspreiden. Tot slot kunnen er vanuit de Rijksoverheid briefings verzorgd worden. Afhankelijk van de insteek kan gedacht worden aan experts van OCW, EZ, BZ, NCTV, AIVD of MIVD. Voor meer informatie kunt op contact opnemen met het Loket Kennisveiligheid van de Rijksoverheid.

Hoofdstuk 7

Gastonderzoekers- en personeelsbeleid

Onderwijs, onderzoek en wetenschap is mensenwerk. Voor de beheersing van alle relevante typen kennisveiligheidsrisico's (zie hoofdstuk 1) is het daarom van belang dat instellingen bewust en verantwoord omgaan met personeelsgebonden risico's.

Kennisinstellingen hebben, op grond van hun institutionele autonomie, veel vrijheid en eigen verantwoordelijkheid bij de inrichting en uitvoering van hun personeelsbeleid. Ze maken hun eigen risicoanalyse en bepalen zelf instelling-specifieke risico's. Met inachtneming van landelijke en gezamenlijke kaders en criteria kunnen ze vervolgens hun personeelsbeleid zo vormgeven dat geïdentificeerde risico's effectief èn passend bij de aard van de instelling beheerst worden.

Om effectief invulling te kunnen geven aan deze verantwoordelijkheid moet voor kennisinstellingen helder zijn wat er van hen op basis van de relevante wetgeving wordt verwacht en welke richting de leidraad daarbij verder biedt. Dit hoofdstuk gaat in op overwegingen die horen bij verschillende fases in de aanstelling van personeel, het ontvangen van gastonderzoekers, interne mobiliteit, dienstreizen, uitdiensttredingen en het personeelsbeleid in algemene zin.

7.1 Kennisveiligheid bij werving en selectie

Bij de werving en selectie van nieuw personeel is veiligheidsbewustzijn van groot belang. Dan wordt immers bepaald wie en in welke hoedanigheid toegang krijgt tot (gevoelige) kennis en technologie. Dat begint al bij de uitgangspunten en werkprocessen van het personeelsbeleid. Het is raadzaam al bij de start van de werving risicoanalyses in te bouwen en mogelijke veiligheidsvraagstukken te delen met interne betrokkenen en belanghebbenden. Stel in een zo vroeg mogelijk stadium vast of er specifieke risico's aan een vacature of aan andere posities zijn verbonden. Bij de selectie, achterliggende processen en besluitvorming kan dan vervolgens gerichte aandacht zijn voor de beheersing daarvan. Dit helpt ook om bijzonderheden ten aanzien van de functie meteen in de vacature te benoemen en bij sollicitatiegesprekken te betrekken en voor de indiensttreding afspraken te maken over eventuele aanvullende maatregelen.

Een belangrijk aandachtspunt hierbij is dat het beleid, de procedures en de besluiten rondom werving en selectie niet discriminerend mogen zijn. Dit verdient specifieke aandacht, omdat dit risico zich juist gemakkelijk voordoet bij het nemen van besluiten over personen in de context van kennisveiligheidsrisico's en sanctienaleving. Er bestaat een risico op het doen van ongefundeerde aannames en het ontstaan van vooroordelen. In het licht van artikel 1 van de Nederlandse grondwet en artikel 21 van het Handvest voor de Grondrechten van de Europese Unie is nationaliteit in zichzelf nooit een afdoende grond voor het aannemen of afwijzen van nieuw personeel.

Zoals in de inleiding beschreven, verschilt de precieze inrichting van het personeelsbeleid per kennisinstelling. Het is daarom vooral belangrijk dat binnen de kennisinstelling duidelijk is wie betrokken zijn bij verschillende personeelszaken en dat iedereen weet wat hun rollen en verantwoordelijkheden zijn in de werkprocessen en het kennisveiligheidsbeleid.

Een kennisveilig personeelsbeleid moet de relevante risico's effectief beheersen. Tegelijkertijd moet het ook uitvoerbaar zijn en moeten de inspanningen in verhouding staan tot de geïdentificeerde risico's. Met andere woorden: wanneer doet u genoeg? *Due diligence* is een centraal begrip in dit dilemma. Wanneer u voldoet aan de 'gepaste zorgvuldigheid' waar due diligence om vraagt, hangt af van de risico's, en dient binnen het personeelsbeleid van de instelling per geval of risico bepaald te worden.

Hoeveel zorgvuldigheid vereist is, hangt af van allerlei factoren, zoals de omvang, de aard en de waarschijnlijkheid van de geïdentificeerde risico's. Hoe openbare – en mogelijk risicovolle – affiliaties van een kandidaat worden afgewogen, is bijvoorbeeld sterk afhankelijk van of de functie directe toegang tot sensitieve kennis biedt. Voorziet de instelling geen noemenswaardige kennisveiligheidsrisico's, bijvoorbeeld omdat er geen sprake is van toegang tot sensitieve kennis, dan zijn in de werving en selectie misschien helemaal geen specifieke zorgvuldigheidsmaatregelen nodig. Worden er wel kennisveiligheidsrisico's geïdentificeerd, dan is het van belang dat instellingen een bewuste inzet plegen.

Van kennisinstellingen wordt niet het onmogelijke of het ontoelaatbare gevraagd. Kennisinstellingen zijn onderworpen aan onvermijdelijke beperkingen; bijvoorbeeld in de informatie en de bevoegdheden waar zij over kunnen beschikken. Daarnaast dienen ook kennisinstellingen zich te allen tijde aan relevante wetgeving te houden. Dat betekent dat *due diligence* zich beperkt tot het mogelijke en het toelaatbare.

Het is belangrijk dat kennisinstellingen de relevante autoriteiten inschakelen, wanneer ze vaststellen dat ze specifieke risico's zelf onvoldoende kunnen beheersen. In dat geval kunnen kennisinstellingen terecht bij het Loket Kennisveiligheid voor advies. Het loket is het centrale aanspreekpunt voor alle vragen over kennisveiligheid. Het onderhoudt contact met de relevante overheidsinstanties om instellingen van passend advies te voorzien. Hierbij horen onder andere de relevante afdelingen van verschillende ministeries en veiligheidsdiensten.

Voor de HR-opgave van kennisinstellingen zijn op twee verschillende niveaus zorgvuldigheden te formuleren en te beschrijven: (1) Verplichte zorgvuldigheid en (2) Aanvullende zorgvuldigheid.

1. **Verplichte zorgvuldigheid.**
   Elke kennisinstelling heeft wettelijk verplichte verantwoordelijkheden ten aanzien van de selectie van personeel. Zie hiervoor ook hoofdstuk 4 van deze leidraad. Dit gaat bijvoorbeeld over:
   a. Naleving van sancties: De kennisinstelling dient na te gaan of: (1) er persoonlijke sancties van toepassing zijn op beoogde kandidaten, gastonderzoekers of -docenten, en (2) er aanleiding is om aan te nemen dat er een risico is op verboden of vergunningsplichtige[30] technische bijstand op het gebied van specifiek kennis en technologie aan gesanctioneerde landen. Het is raadzaam dat kennisinstellingen risico's op sanctieovertreding meenemen in hun algehele risicoanalyse, om te identificeren voor welke kennis er binnen de instelling aandacht dient te zijn binnen het HR-proces.
   Om inzicht te krijgen in de verschillende EU- en VN-sancties kunnen instellingen gebruikmaken van de EU Sanction Map[31]. Daarin zijn alle actuele sancties terug te vinden en te doorzoeken op gesanctioneerde regimes, personen en entiteiten.
   b. Naleving van verscherpt toezicht: De kennisinstelling dient na te gaan of de beoogde kandidaat, gastonderzoeker of -docent een ontheffing kennisembargo nodig heeft. Dit volgt uit de nationale sanctieregelingen en is na vaststelling terug te vinden in de lijst van vakgebieden die onder het kennisembargo vallen.[32]

30 EU 2021/821 artikel 8 met aanvullend artikel 2.9, artikel 2.10c en artikel 4.1.

31 www.sanctionsmap.eu

32 https://www.Rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies

2. **Aanvullende zorgvuldigheid.**
   Dit gaat om verantwoordelijkheden die niet wettelijk zijn vastgelegd, maar die op basis van de aanpak van bewustwording en zelfregulering door de sector wel van groot belang zijn. Vanuit het perspectief van kennisveiligheid is deze zorgvuldigheid gewenst wanneer er personeelsgebonden risico's zijn bij een vacature.
   a. Openbare affiliaties: De kennisinstelling gaat na of er sprake is van duidelijke kennisveiligheidsrisico's. Bijvoorbeeld omdat kandidaten, gastonderzoekers of -docenten:
      i. Recentelijk hebben gewerkt aan instellingen in landen met een verhoogd risico,
      ii. en of zij daar bijvoorbeeld aan militair toepasbare technologie of strategische machtsmiddelen hebben gewerkt,
      iii. of actuele (neven)functies hebben op dergelijke onderwerpen of instellingen.

      Voor informatie over instellingen, vakgebieden en landen kunnen kennisinstellingen terecht bij het Loket Kennisveiligheid.
   b. Volledigheid en navolgbaarheid: De kennisinstelling gaat na of CV, brief en gesprek aan het einde van het proces een transparant en geloofwaardig geheel vormen, en geen problematische onverklaarbare gaten of tegenstrijdigheden bevatten of heimelijk gedrag suggereren.
   c. Verdiepend achtergrondonderzoek: Kennisinstellingen kunnen een grondiger onderzoek uitvoeren naar het verleden of netwerk van kandidaten op basis van het aangeleverde CV. Dit kan bijvoorbeeld inhouden dat wordt gekeken naar eerdere activiteiten en samenwerkingen, zoals co-auteurs met wie de kandidaat onderzoek heeft gepubliceerd.
   d. Integriteitsassessment: een kennisinstelling kan ervoor kiezen om van kandidaten medewerking te vragen aan een integriteitsassessment. Een dergelijk assessment kan helpen om een indicatie te geven van de eerlijkheid en oprechtheid van beoogde kandidaten.

Voordat bovenstaande of andere maatregelen worden geïmplementeerd, is het belangrijk om een gedegen risicoanalyse te maken, om te bepalen wat de maatregelen opleveren. Zodra een instelling kiest voor bepaalde maatregelen ontstaat de verantwoordelijkheid om die in lijn met geldende wetgeving uit te voeren.

Rol van de Rijksoverheid

Hoewel de Rijksoverheid zelf geen uitvoering kan geven aan het personeelsbeleid van kennisinstellingen, biedt zij wel een aantal voorzieningen die kennisinstellingen kunnen helpen bij de totstandkoming en de uitvoering van het personeelsbeleid. Dit gaat allereerst om het Loket Kennisveiligheid. Hoewel het Loket Kennisveiligheid geen onderzoek doet naar personen, kunnen instellingen het loket wel om advies vragen. Specifiek bij het beoordelen van risico's die horen bij specifieke organisaties, landen, vakgebieden of financiering; maar ook over vragen rondom sanctienaleving. Let op dat er in de adviesverzoeken geen tot personen herleidbare informatie mag worden gedeeld. De afgegeven adviezen kunnen vervolgens worden betrokken bij de interne besluitvorming van de instelling.

7.2 Opleiding en training

Opleidingen en trainingen kunnen helpen om alle betrokkenen binnen een kennisinstelling in staat te stellen de verantwoordelijkheden die horen bij het personeelsbeleid goed uit te voeren. Hierbij kunt u bijvoorbeeld denken aan:

- Nieuwe medewerkers een welkomstpakket aanbieden met relevante informatie en regelingen over kennisveiligheid

- Een module of briefing over kennisveiligheid aanbieden aan nieuwe medewerkers die met risico's op het gebied van kennisveiligheid te maken kunnen krijgen. Hiervoor kan ook de basis e-learning kennisveiligheid en de e-learning kennisveiligheid voor onderzoekers worden gebruikt. Deze e-learnings zijn zowel in het Nederlands als Engels beschikbaar op het online platform van het Loket Kennisveiligheid. De e-learnings van het Loket Kennisveiligheid zijn ook beschikbaar in een formaat dat gebruikt kan worden in de eigen leeromgeving van een instelling;
- Het aanbieden van opfrismodules aan het begin van een nieuw onderzoeksproject om te zorgen dat het bewustzijn van de projectleden op peil is;
- Het inrichten van een platform op het intranet waar medewerkers informatie kunnen vinden en waar zij hun kennis en alertheid kunnen testen (self assessment).
- Het opzetten van een speciaal trainingsprogramma voor onderzoekers en studenten gericht op enculturatie en inbedding in de academische gemeenschap, en de bijbehorende principes van wetenschappelijke integriteit en wetenschappelijke kernwaarden.

7.3 Risico op stigmatisering en ongewenst gedrag

Het thema kennisveiligheid leeft breed in de samenleving. Er zijn geregeld voorbeelden in het nieuws en ook de inlichtingen- en veiligheidsdiensten maken er geen geheim van bij welke landen zij de grootste risico's voor de nationale veiligheid zien. Uitgangspunt is echter dat kennisveiligheidsbeleid landenneutraal en non-discriminatoir is. Dit om te voorkomen dat wetenschappers met een specifieke achtergrond of nationaliteit worden geraakt, zonder dat zij persoonlijk een risico vormen.

De ervaring leert dat het voor personeel en studenten onderling niet altijd eenvoudig is om dat onderscheid goed te maken. Het is daarom voor kennisinstellingen belangrijk om in het kader van sociale veiligheid en inclusie oog te hebben voor het risico op stigmatisering en uitsluiting van collega's op basis van afkomst. Het uitgangspunt is hierbij dat personeel en gasten zich welkom en sociaal veilig voelen; zowel tijdens de sollicitatie en het besluitvormingsprocedures als tijdens de rest van hun aanstelling of verblijf.

Het helpt bijvoorbeeld als de nuances van het kennisveiligheidsbeleid binnen de kennisinstelling breed bekend zijn bij personeel en studenten. Zo begrijpt personeel en studenten dat er zorgvuldig en deskundig wordt omgegaan met risico's bij sollicitaties, en dat je daar als wetenschapper of student in algemene zin op mag vertrouwen. En dat het bijvoorbeeld bij relevante risico's ook niet om nationaliteit draait, maar om inhoudelijke affiliaties met risicovolle instellingen, bedrijven of overheidspartijen.

7.4 Interne functiewisselingen en onderzoeksprogrammering

Toegang tot sensitieve kennis en technologie ontstaat niet alleen in het proces van werving en selectie, maar kan ook optreden als gevolg van interne functiewisselingen of verschuivingen in de onderzoeksprogrammering van vakgroepen. Bestaande medewerkers en masterstudenten kunnen door zo'n verandering onderdeel worden van vakgroepen of onderzoekslijnen waarvoor er binnen de instelling risico's zijn geïdentificeerd. Om hier grip op te houden is het belangrijk om een brede bewustwording binnen de instelling te bevorderen. Ook is het raadzaam om duidelijke afspraken en processen in te richten om functiewisselingen en verschuivingen in de onderzoeksprogrammering tijdig te signaleren en waar nodig veiligheidsbevorderende maatregelen te treffen.

In bredere zin vestigt dit thema aandacht op de risico's die aan zittend personeel en (in sommige gevallen) masterstudenten verbonden kunnen zijn. Dit wordt in veiligheidsjargon ook wel *insider risk* genoemd. Voor handvatten ten aanzien van de veelal digitale beheersing van dergelijke risico's kunnen kennisinstellingen terecht bij het Digital Trust Center van het ministerie van EZK[33]. Daar worden concrete handvatten gepubliceerd ten behoeve van de omgang met (digitale) insider risico's.

7.5 Toelating bezoekers, gastonderzoekers, gastdocenten en externe inhuur

Niet alleen personeel met een arbeidsrelatie kan toegang hebben tot specifieke kennis en technologie binnen kennisinstellingen. Ook voor bezoek en voor specifieke werkzaamheden kan toegang worden verleend.

Dat kan gaan om deelnemers aan conferenties, werkbezoeken, vertegenwoordigers van bedrijven, gastdocenten, gastonderzoekers, facilitair personeel, externe inhuur, cateraars, enzovoort. Omdat er geen sprake is van een arbeidsrelatie, is er in die gevallen vaak ook geen sprake van een sollicitatieprocedure. Toch kunnen kennisinstellingen wel beleid maken rond de toelating van gasten en de besluitvorming, randvoorwaarden en voorzieningen die daarvoor nodig zijn. Net als voor de werving en selectie van personeel. Veel van de onder 7.1 beschreven aandachtspunten zijn ook van toepassing op de toelating van bezoekers.

Het is bijvoorbeeld raadzaam een bezoekersprotocol uit te werken voor buitenlands bezoek in het algemeen. Met daarin aandacht voor specifieke locaties binnen de instelling, en voor bezoekers vanuit instellingen met een verhoogd risicoprofiel in het bijzonder. Bezoekersbeleid heeft alleen nut als er daarnaast ook fysieke en digitale maatregelen worden getroffen om de locaties te beschermen.

Good practice

Voorbeelden van bouwstenen voor een bezoekersprotocol

- Laat bezoekers en delegaties uit het buitenland altijd vóóraf aanmelden door de medewerkers die deze bezoekers willen ontvangen. Zonder aanmelding vooraf geen toegang. Zorg er daarnaast voor dat alle bezoekers zich bij binnenkomst identificeren en registreren en vanaf een elders gelegen punt, zoals een receptie, worden opgehaald.
- Weet waar bepaalde bezoekers wel mogen rondlopen en waar niet, zodat van tevoren kan worden beoordeeld of een bezoek op een bepaalde plek kan doorgaan.
- Kondig bezoek in gevoelige ruimtes vooraf aan bij collega's, zodat zij hier rekening mee kunnen houden.
- Laat uw bezoekers nooit alleen, vooral niet op sensitieve plekken. Begeleid hen te allen tijde op uw locaties.
- Maak duidelijk dat het niet is toegestaan om foto's of video's te maken op locatie zonder uw toestemming of zorg dat alle apparatuur op sensitieve locaties opgeborgen is (bijvoorbeeld in een kluis).
- Stel van te voren vast wat u wel en niet met de bezoeker gaat (en mag) delen en vermijd tijdens het bezoek en in uw gesprekken met gasten onderwerpen die met de beveiliging van informatie of locaties te maken hebben.
- Op zeer gevoelige onderzoeken/plekken/locaties is het beter geen bezoekers te ontvangen, of om bezoekers van landen met een verhoogd risicoprofiel uit te sluiten.

33 https://www.digitaltrustcenter.nl/informatie-advies/wat-zijn-insider-threats

7.6 Dienstreizen naar het buitenland

Het is raadzaam om ook beleid te hebben rondom het beheersen van de risico's die verbonden zijn aan uitgaande reizen, waarbij medewerkers van uw kennisinstelling een ander land bezoeken. Zeker als het om een land gaat met een verhoogd risicoprofiel op het gebied van kennisveiligheid, vergt dat de nodige bewustwording, voorbereiding en alertheid.

Good practice
Voorbeelden van bouwstenen voor een protocol bij dienstreizen naar landen met een verhoogd risicoprofiel

Voordat u vertrekt
Zorg dat u een minimale hoeveelheid (vertrouwelijke) gegevens bij u heeft.
Bedenk vooraf wat er op de gegevensdragers staat die u meeneemt. Bevat uw laptop bestanden met gevoelige informatie, terwijl u deze niet nodig heeft tijdens uw reis? Verplaats deze bestanden dan naar een andere computer voor u vertrekt of laat deze laptop thuis en neem een andere (reis) laptop mee.

Idem voor uw mobiele telefoon. Wis de belgeschiedenis van uw telefoon voor vertrek of laat deze telefoon thuis en neem een (reis)telefoon mee.
Gebruik wachtwoorden en/of toegangscodes voor uw devices en schakel devices waar mogelijk uit: wanneer devices aanstaan, bent u extra kwetsbaar.

Als u onderweg bent
Schakel de bluetooth functie van uw telefoon en laptop altijd uit.
Neem vertrouwelijke informatie en gegevensdragers altijd mee in uw handbagage en niet in uw ruimbagage (denk aan usb-sticks, telefoons).
Wees voorzichtig met vertrouwelijke gesprekken aan boord van een vliegtuig, trein of in andere publieke ruimten. Niet alleen medepassagiers kunnen meeluisteren; sommige (vliegtuig) maatschappijen hebben bijvoorbeeld nauwe banden met inlichtingen- en veiligheidsdiensten.

Op de plek van bestemming
Bescherm vertrouwelijke informatie. Laat geen vertrouwelijke gegevens achter op een plaats waar anderen ze kunnen inzien. Dit geldt ook voor uw hotelkamer of hotelkluis.
Geef uw laptop of telefoon niet zomaar af en zorg ervoor dat u altijd kunt controleren of iemand uw informatie heeft ingekeken.

Verstrek selectief informatie. Ga bij contacten uit van het need-to-know-principe: vertel uw gesprekspartner niet meer dan noodzakelijk. Dit geldt ook voor congressen of bijeenkomsten waar u bent uitgenodigd als spreker.
Wees voorzichtig met verkregen (gratis) USB's op congressen of evenementen. Dit is een makkelijke manier om malware te installeren op uw laptop.

Zie ook de AIVD-brochure 'Op reis naar het buitenland – Veiligheidsrisico's onderweg

Voor wie werkzaam is op een kennisgebied dat zeer sensitief is en/of regelmatig landen met een verhoogd risicoprofiel bezoekt, kan het verstandig zijn een HEAT-training (Hostile Environment Awareness Training) te volgen en voorafgaand aan een bezoek actuele informatie over de veiligheidssituatie te raadplegen.

7.7 Beëindiging arbeidsrelatie

Tot slot is het raadzaam ook bij uitdiensttreding van personeel alert te zijn op bepaalde risico's. Dat is uiteraard lastig, omdat het voor kennisinstellingen niet mogelijk is om in contact te blijven met iedereen die ooit aan de instelling verbonden is geweest.

Tegelijkertijd zijn er wel een aantal zaken die er aan bij kunnen dragen dat de bijbehorende risico's zo goed mogelijk gemitigeerd worden.

Zo kunnen kennisinstellingen in het geval van sensitieve vakgebieden of heel waardevolle kennis gebruik te maken van de geheimhoudingsverklaring zoals geregeld in de CAO. Het is daarbij wel belangrijk dat dit bij het aangaan van de arbeidsrelatie al wordt vastgelegd. De geheimhoudingsverklaring kan dan tot een aantal jaar na uitdiensttreding werkzaam blijven. Het is raadzaam om bij het opstellen van deze geheimhoudingsverklaringen juridische expertise te betrekken.

Het is tevens belangrijk om goede afspraken te maken over en toe te zien op het beëindigen van de toegang tot sensitieve kennis en technologie. Dit gaat om het beëindigen van concrete toegangsrechten tot fysieke faciliteiten van de instelling, maar ook om toegang tot de digitale infrastructuur van de kennisinstelling en de soms eigen infrastructuur van onderzoekgroepen en laboratoria.

Voor universiteiten en onderzoeksinstituten is het raadzaam om specifieke aandacht te hebben voor de processen en het beleid rondom de overgang naar het emeritaat, en de bijbehorende digitale en fysieke toegangsrechten.

Appendix

Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid

Appendix bij
Nationale Leidraad Kennisveiligheid

Voorjaar 2025

Inleiding

Internationale samenwerking en open kennisuitwisseling zijn essentieel voor de wetenschap. In een tijd van gespannen verschuivende geopolitieke verhoudingen brengt dit internationale karakter echter ook risico's met zich mee. Bij het aangaan van internationale samenwerkingen maken Nederlandse kennisinstellingen daarom een zorgvuldige en weloverwogen afweging tussen kansen en risico's. Zij doen dit met het oog op kennisveiligheid.

Kennisveiligheid

Kennisveiligheid is het anticiperen op en beheren van risico's in verband met:

a. de ongewenste overdracht van sensitieve kennis en technologie die van invloed kan zijn op de nationale veiligheid en/of de wetenschappelijke positie van instellingen;
b. 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 aan te zetten tot zelfcensuur onder studenten en onderzoekers, waarmee inbreuk wordt gemaakt op de academische vrijheid en de integriteit van onderzoek en onderwijs in Nederland; en
c. ethische of integriteitsschendingen, wanneer kennis en technologie door statelijke actoren worden gebruikt om Nederlandse en Europese waarden en geldende verdragen te schenden of te ondermijnen.

Deze publicatie bevat een set van uniforme indicatoren die kennisinstellingen kunnen gebruiken bij het inschatten van de risico's. De set is tot stand gekomen aan de hand van verschillende indicatoren en procedures die kennisinstellingen hanteren. Deze indicatoren dienen als een minimale gemeenschappelijke basis, met als inzet het creëren een gelijk speelveld in het Nederlandse hoger onderwijs en de wetenschap en het versterken van de weerbaarheid van de Nederlandse kennissector als geheel.

➔ **Wanneer kennisinstellingen soortgelijke indicatoren hanteren bij het inschatten van risico's, versterkt dit de weerbaarheid van de Nederlandse kennissector als geheel.**

De kennisinstellingen en de Rijksoverheid hebben deze indicatoren gezamenlijk ontwikkeld. Ze vormen een concretisering van aandachtspunten beschreven in de Nationale Leidraad Kennisveiligheid. In die geest moet dit document opgevat worden. De indicatoren zijn niet-bindend, staan ten dienste van de kennisinstellingen, en zijn een uitdrukking van onze gezamenlijke ambitie om het hoger onderwijs en de wetenschap weerbaarder te maken tegen statelijke dreigingen. Zo zorgen we ervoor dat internationale wetenschappelijke samenwerking veilig kan plaatsvinden, met een goede balans tussen de kansen en risico's en met inachtneming van onze academische kernwaarden.

Voor wie?

Deze publicatie is in eerste instantie bedoeld voor bestuurders en medewerkers die verantwoordelijk zijn voor kennisveiligheid binnen een Nederlandse kennisinstelling. Zij kunnen deze bijvoorbeeld als referentie gebruiken bij het inrichten of evalueren van een afwegingskader voor risicobeoordelingen. Ook voor anderen kan deze set indicatoren nuttig zijn, zoals onderzoekers, decanen, docenten of projectleiders, wanneer de instelling geen eigen afwegingskader heeft vastgesteld en om het veiligheidsbewustzijn te verhogen.

Reikwijdte

De indicatoren hebben betrekking op nieuwe internationale samenwerkingen. Met **internationale samenwerkingen** wordt in dit document bedoeld: samenwerkingen met organisaties of organisatieonderdelen, met een wetenschappelijke of onderwijsdoelstelling, waarbij sprake is van een overeenkomst of investering (bijvoorbeeld financiering, personeel of materieel). Een onderdeel kan een onderzoeksproject, onderzoekslijn, programmalijn, vakgroep, onderzoeksgroep, team, laboratorium, opleiding, of technologiegebied zijn. Ook beursprogramma's en (wetenschappelijke) gastvrijheid worden gerekend tot samenwerking. Individuen vallen niet binnen de reikwijdte van dit document, tenzij het de wettelijke kaders uit hoofdstuk 1 betreft.

Bij **risico's** gaat het om de mogelijkheid van overdracht van sensitieve kennis en technologie naar statelijke actoren, die deze vervolgens inzetten op een manier die schade aanbrengt aan de nationale veiligheid. Bijvoorbeeld via militaire toepassingen of door verstoring van vitale processen. Ook gaat het om de kans op buitenlandse inmenging en heimelijke beïnvloeding, en de impact die dit heeft op de integriteit van hoger onderwijs en wetenschap of op het welzijn van medewerkers en studenten. Daarnaast gaat het om de mogelijkheid dat sensitieve kennis, technologie of onderzoeksmethoden door statelijke actoren worden misbruikt, waarbij Nederlandse of Europese waarden en verdragen worden ondermijnd. In de Nationale Leidraad Kennisveiligheid zijn deze risico's nader beschreven.

De **indicatoren** betreffen aandachtspunten en vragen die gesteld moeten worden voordat een samenwerking tot stand komt. In enkele gevallen zijn daarbij ook specifieke **normen** opgenomen of **stappen** die ondernomen kunnen worden. Ook is opgenomen welke **bronnen** instellingen doorgaans raadplegen.

Toepassing

Een risico dat geïdentificeerd wordt op basis van deze indicatoren betekent niet per sé dat de samenwerking ontoelaatbaar is.[34] Een opstapeling van risico's kan echter een aanwijzing zijn dat de samenwerking onwenselijk is in het kader van kennisveiligheid. Het maken van een afweging is hierbij van belang, waarbij kansen en risico's tegenover elkaar worden gezet. Daarbij speelt ook mee of een aantal randvoorwaarden op orde zijn, die de risico's kunnen beperken, zoals toegangsbeleid en cybersecuritybeleid. Mitigerende maatregelen kunnen helpen bij het beheersen van aanwezige risico's. Het Loket Kennisveiligheid kan adviseren over het inschatten van risico's en het treffen van mitigerende maatregelen.

1. Wettelijke kaders

Een eerste vraag bij een internationale samenwerking is of de samenwerking ***juridisch*** is toegestaan. De volgende vragen dienen doorlopen te worden:

➔ **Staat de organisatie of de persoon waarmee de samenwerking wordt aangegaan op een sanctielijst van de EU of de VN?**

Nederlandse kennisinstellingen werken niet internationaal samen met organisaties of personen die voorkomen op de EU- of VN-sanctielijst. Het overdragen van goederen, technologie en/of het verlenen van diensten ('technische bijstand') aan organisaties of personen op de sanctielijst is niet toegestaan. Het overtreden van een sanctie is een strafbaar feit.

34 Tenzij de samenwerking uitdrukkelijk in strijd met de wet is – zie hoofdstuk 1.

Alle landen waarop EU-sancties van toepassing zijn, zijn te vinden op www.sanctionsmap.eu. Momenteel (begin 2025) staan er instellingen en personen op uit landen zoals Belarus, Iran, Noord-Korea, Rusland en Syrië. Kennisinstellingen zijn ook alert op het risico van indirecte overtredingen van de sancties en dit risico te beperken. Een indirecte overtreding van sancties vindt plaats wanneer iemand opzettelijk of met nalatigheid bijdraagt aan het ontduiken of omzeilen van sancties. Dit gebeurt meestal via tussenpersonen, omwegen of constructies waardoor gesanctioneerde personen of entiteiten alsnog toegang krijgen tot goederen, diensten of kapitaal.

➔ **Valt het onderzoeksgebied onder internationale sancties?**

Nederland is als lidstaat verplicht om de verboden uit EU-sanctieverordening na te leven. Ook kennisinstellingen zijn rechtstreeks gebonden aan deze verboden. De Rijksoverheid ondersteunt kennisinstellingen sinds 2019 bij de naleving van een deel van deze verboden met de Taskforce Ongewenste Kennisoverdracht (Verscherpt Toezicht). Specifiek als het gaat om het overdragen van bepaalde kennis en technologie naar Noord-Korea, Iran en Rusland.

De Rijksoverheid heeft via deze link in maart 2025 een update gegeven van alle sanctieregelingen waar Nederland zich aan heeft gecommitteerd. Nieuwe updates zijn raadpleegbaar via deze link. Met behulp van deze link kan men vinden voor welke onderzoeksgebieden of vakgroepen een ontheffing moet worden aangevraagd bij de Taskforce Ongewenste Kennisoverdracht.

➔ **Valt het onderzoek onder de Dual-use Verordening?**

Nederland wil voorkomen dat bepaalde strategische goederen, technologieën en diensten geëxporteerd worden om redenen van nationale veiligheid. Strategische goederen zijn militaire goederen, dual-use-goederen en diensten, en sanctiegoederen. Om ongewenst eindgebruik tegen te gaan, geldt een vergunningplicht voor de uitvoer hiervan. Is sprake van een onderzoek dat betrekking heeft op dual-use of militaire goederen, producten, programmatuur of technologie, dan mag dit onderzoek alleen worden geëxporteerd met een vergunning van de Centrale Dienst voor In- en Uitvoer (CDIU) van de Douane. In bijlage I van de Dual-use verordening (EU-verordening 2021/821) staat uitgewerkt wat vergunningplichtig is.

Het begrip *uitvoer of export* is in deze context veelomvattend; in feite gaat het om alle vormen van overdracht, ongeacht het middel. Het betreft dus ook de overdracht via e-mail of clouddiensten. Het is mogelijk dat ook producten en technieken hieronder vallen waarvan men dat in eerste instantie niet verwacht. Het is daarom belangrijk te controleren of een product, programma, technologie of dienst op de lijst van dual-use goederen voorkomt.

2. Affiliaties en type organisatie

Voor de inschatting van kennisveiligheidsrisico's is het essentieel om verder te kijken dan alleen wet- en regelgeving. Organisaties kunnen banden hebben met of overgenomen zijn door statelijke actoren die door middel van inmenging, spionageactiviteiten of heimelijke beïnvloeding de nationale veiligheid kunnen bedreigen. In deze stap wordt er goed gekeken naar de affiliaties van een organisatie.

Statelijke actoren gebruiken verschillende manieren om kennis te bemachtigen. De intenties van statelijke actoren, zoals beschreven in het DSBA II, zijn om een technologische grootmacht te worden, afhankelijkheden te verminderen en technologie in te zetten als strategisch machtsmiddel. Deze intenties, gecombineerd met geconstateerde offensieve (cyber)programma's of dreigingen, maken dat instellingen zich bewust moeten zijn van hoe statelijke actoren kennis proberen te bemachtigen en van de mogelijke omzeilingsroutes die zij daarbij inzetten. Affiliaties bieden hiervoor een goed aanknopingspunt in de context van internationale samenwerkingen. Ook de omzeilingsroutes, waarbij statelijke actoren gebruik maken van (organisaties in) bevriende staten om via een omweg toch toegang te krijgen tot kennis en technologie, kunnen hiermee in kaart worden gebracht.

Affiliaties verwijzen naar (in)formele banden, verbanden of lidmaatschappen die organisaties hebben met andere organisaties. Dit kunnen organisatorische, professionele, politieke of sociale affiliaties zijn. Affiliaties zijn relevant omdat ze inzicht geven in netwerken, belangen, waarden en invloedssferen waartoe iemand of een organisatie behoort. Indicatoren hiervoor zijn onder andere of een beoogd partner verbonden is aan een overheid. Dit is extra relevant indien het een statelijke actor betreft waar een dreiging vanuit gaat. Staatsgeleide bedrijven of instellingen, gebleken militaire toepassingen van vreedzaam bedoelde onderzoeksuitkomsten, een niet-aantoonbare reputatie of onwenselijke geheimhoudingsbepalingen in contracten kunnen indicatoren zijn voor mogelijke risico's. Deze opsomming is niet uitputtend.

Instellingen stellen daarbij in elk geval deze vragen:

- ➔ **Betreft het een samenwerking met een partner uit een land met een offensief (cyber) programma tegen Nederland en westerse belangen?**
- ➔ **Is de partner verbonden (geweest) aan een organisatie buiten de EU met militaire banden waar dreiging van het land of organisatie uitgaat?**

De affiliatiecheck is onderdeel van de due diligence en wordt uitgevoerd *voor* het aangaan van een samenwerking. Voor affiliaties wordt gekeken zowel naar directe (militaire) als indirecte (civiele) affiliaties. Het kan voorkomen dat organisaties in het verleden verbonden zijn geweest aan een organisatie of persoon die op een sanctielijst staat, of dat de organisatie zelf gesanctioneerd is geweest.

Een samenwerking met een organisatie uit een land van buiten de EU/NAVO waar een dreiging van uitgaat kan risicovol zijn, zeker als er sprake is van militaire affiliaties. In de risicobeoordeling van affiliaties wordt in elk geval specifiek gekeken naar de landen die door de AIVD en MIVD vermeld worden in het Dreigingsbeeld Statelijke Actoren (DBSA) en het Dreigingsbeeld Hybride en Militaire Dreigingsbeelden, vanwege het risico op ongewenste kennisoverdracht. Dit zijn China, Iran, Noord-Korea en Rusland. Als door geopolitieke veranderingen het dreigingslandschap verandert kunnen andere landen, na publicatie in het DBSA, worden toegevoegd.

Instellingen hebben oog voor geopolitieke verschuivingen, maar sluiten zelf niet op voorhand alle samenwerkingen met een specifiek land uit. Waar het samenwerking met gehele landen betreft, doet de overheid daar richtinggevende uitspraken over.

Daarnaast raadplegen instellingen ook andere bronnen om een breder beeld te krijgen van de risico's met betrekking tot ongewenste kennisoverdracht, buitenlandse inmenging en ethische kwesties. Bijgevoegd is een overzicht van bruikbare bronnen.

- ➔ **Instellingen raadplegen, waar dit van toepassing is, in elk geval bronnen uit de bijlage in dit document.**
- ➔ **Voor affiliaties kijken kennisinstellingen in elk geval naar de afgelopen vijf jaar. Indien daar aanleiding toe is, kijken zij in sommige gevallen naar de afgelopen tien jaar.**

Het beoordelen van een organisatie of affiliatie levert een eerste risico-inschatting op, die naast inhoudelijke aspecten van het onderzoek, project of samenwerking wordt gelegd (zie volgend hoofdstuk). De combinatie van affiliaties en expertise of interessegebieden van de entiteit met de sensitiviteit van het onderzoek of technologie maakt dat een samenwerking in deze stap al als risicovol kan worden beschouwd, zeker als er een dreiging uitgaat van de statelijke actor waar de organisatie aan verbonden is.

3. Vakgebied en type onderzoek

Sensitieve kennis en technologie

Samenwerkingen met betrekking tot bepaalde kennis en technologie kunnen een verhoogd risico met zich meebrengen voor de nationale veiligheid; omdat ze kunnen leiden tot ongewenst eindgebruik (zoals bepaalde militaire toepassingen) of het ontstaan van risicovolle strategische afhankelijkheden (waarbij kennis of technologie als machtsmiddel worden ingezet). In die gevallen is er sprake van sensitieve kennis en technologie. Voorbeelden zijn kunstmatige intelligentie, kwantumonderzoek, biotechnologie en rakettechnologie.

Het ministerie van OCW werkt aan een wetsvoorstel voor de invoering van een screeningsplicht, waarin een specifiekere lijst van sensitieve technologie is opgenomen. Instellingen kunnen hier alvast kennis van nemen via openbare internetconsultatie. Vanuit het perspectief van ongewenste kennis- en technologieoverdracht is deze lijst leidend. Hoewel het wetsvoorstel toeziet op de screening van personen, is deze lijst evenwel bruikbaar in de context van internationale samenwerkingen met organisaties. De lijst kan gedurende het wetstraject onderhevig zijn aan wijzigingen.

- ➔ **Wordt er onderzoek gedaan naar of met sensitieve technologie die niet reeds openbaar toegankelijk is?**
- ➔ **Is het doel van het onderzoek om toepassingen te ontwikkelen, te onderzoeken of te produceren binnen het militaire-, politie-, inlichtingen en veiligheidsdomein?**
- ➔ **Wordt het onderzoek gekenmerkt door een breed toepassingsbereik binnen vitale infrastructuur of vitale processen?**

De NCTV heeft een beschrijving gepubliceerd van de vitale infrastructuur en processen, zie link.

De mate van sensitiviteit van een technologie kan lager zijn als er sprake is van fundamenteel onderzoek, maar ook dan kunnen er risico's zijn, bijvoorbeeld als een specifiek risicovolle toepassing is voorzien, of er sprake is van samenwerking met een externe financier.

4. Afhankelijkheid en beïnvloeding

Voor het inschatten van risico's bij internationale samenwerkingen hebben de kennisinstellingen ook oog voor buitenlandse inmenging en financieringsstromen.

Buitenlandse inmenging

Statelijke actoren kunnen proberen om onderzoek en onderwijs te beïnvloeden. Mogelijke willen zij de manier veranderen waarop de actor internationaal gezien en begrepen wordt. Daarbij willen statelijke actoren soms ook controle en zicht houden op hun landgenoten, bijvoorbeeld door te voorkomen dat zij dissidente of negatieve standpunten uiten over het herkomstland. Ook kunnen wetenschappelijke experts ingezet worden door statelijke actoren als geloofwaardige spreekbuis, vooral wanneer deze experts standpunten uitdragen die in lijn zijn met de belangen van de staat. Tot slot kan inmenging ook ingezet worden voor ongewenste kennisoverdracht.
Hiervoor kan een statelijke actor gebruik maken van (financiële) middelen die worden ingezet als stimulans (beloning) of juist als drukmiddel (bedreiging). Het is ook mogelijk dat er sprake is van financiële afhankelijkheid voor een wetenschapper of student. De druk die hiervan uitgaat kan leiden tot zelfcensuur, waarbij individuen en groepen zich niet altijd openlijk kritisch uit durven laten. Ook kunnen academici worden gehinderd om onderzoeksresultaten te publiceren wanneer deze niet in lijn zijn hetgeen de statelijke actor graag zou willen. Hierdoor komt de sociale veiligheid van de wetenschapper of student in het gedrang. Het is daarom cruciaal dat onderzoekers en studenten binnen een veilige omgeving kunnen spreken over ervaringen of gesignaleerde kennisveiligheidsrisico's, zonder dat zij daar consequenties van ondervinden.

Om risico's ten aanzien van buitenlandse inmenging in te schatten, beoordelen kennisinstellingen de bron van financiering bij een samenwerking, en het mogelijke doel van de financiering. Daarbij stellen zij in elk geval deze vragen:

- ➔ **Is sprake van (grotendeels) eenzijdige externe financiering bij de samenwerking of bij inkomende (gast)medewerkers?**
- ➔ **Wat zijn redenen voor de partner om het onderzoek, de samenwerking of betrokken personen te financieren?**
- ➔ **Wat is de herkomst van de financiering?**
- ➔ **Wordt de samenwerking (mede) gefinancierd door een buitenlandse (overheids)bron verbonden aan een statelijke actor waar dreiging van uitgaat of waarvan bekend is dat het onderzoek misbruikt kan worden?**

Beursprogramma's

Samenwerkingen kunnen buitenlandse beursprogramma's betreffen. Sommige statelijke actoren financieren internationale beursprogramma's met inmenging of het bemachtigen van sensitieve kennis als doel. Financiële inbreng maakt het voor veel Nederlandse instellingen aantrekkelijk om wetenschappelijk talent in huis te halen, zonder hoge kosten te maken. Statelijke actoren weten dit en streven actief naar een dergelijke afhankelijkheidsrelatie. De kennisinstellingen zijn hier alert op. Voor beursprogramma's gefinancierd door organisaties in risicovolle landen stellen de kennisinstellingen de volgende vragen:

- ➔ **Gaat het om bursalen voor korter dan twee jaar met een onderwerp en begeleiding afkomstig uit het thuisland?**
- ➔ **Doen de bursalen onderzoek naar of met sensitieve technologie die niet reeds openbaar toegankelijk is?**
- ➔ **Zijn de bursalen afkomstig van een universiteit met militaire banden uit een land waar dreiging van uitgaat?**

5. Ethiek en integriteit

Ethisch onverantwoorde praktijken

Voordat kennisinstellingen de ethische aspecten van de samenwerking met buitenlandse partijen beoordelen, is het van belang dat onderzoekers zorgen dat hun eigen werk voldoet aan de Nederlandse gedragscode wetenschappelijke integriteit, en dat de kennisinstellingen de zorgplichten op het gebied van ethische normstelling- en procedures naleven.

Bepaalde onderzoeken kunnen leiden tot mensenrechtenschendingen, misbruik van kennis of onveilige situaties voor onderzoekers en respondenten. Bijvoorbeeld wanneer data in handen komen van andere statelijke actoren of wanneer onderzoeksdata over gemarginaliseerde groepen in handen vallen van een repressieve overheid. Dit kan leiden tot represailles voor de betrokken onderzoekers of respondenten. Om deze kennisveiligheidsrisico's in te perken is het van belang alert te zijn op aanwijzingen van deze ongewenste praktijken en dat academische waarden door de samenwerkingspartner worden erkend en nageleefd.

Instellingen stellen daarbij in elk geval deze vragen:

- ➔ **Bestaat er een risico dat de vrijheden van de onderzoeker(s) onder druk komt te staan?**
- ➔ **Zijn er bij de samenwerking landen betrokken waarin de academische vrijheid sterk ingeperkt wordt?**
- ➔ **Kunnen de onderzoeksresultaten en/of data gebruikt worden voor doeleinden die op gespannen voet staan met het respecteren van mensenrechten?**

Een manier om dergelijke aanwijzingen te achterhalen is door due diligence uit te voeren. Hiermee kan bijvoorbeeld worden onderzocht of er negatieve berichtgeving is in betrouwbare en onafhankelijke media. Dergelijke bronnen kunnen inzicht geven in de reputatie van een zakelijke relatie. Mogelijk is er nieuws over betrokkenheid bij mensenrechtenschendingen of recente schandalen rond omkoping en corruptie. Daarnaast kunnen instellingen ook tools aanschaffen voor due diligence-onderzoek. Deze tools controleren onder andere op strafbare feiten, negatieve media, sanctielijsten, staatsbedrijven en door de staat gefinancierde ondernemingen. Ook gedurende het onderzoek kan due diligence worden uitgevoerd om mogelijke onethische toepassingen van het onderzoek te traceren.

Het beoordelen en wegen van ethische kwesties bij internationale samenwerking kan een lastig en gevoelig proces zijn. Dit vraagt om zorgvuldige afwegingen. Kennisinstellingen hebben daarom eigen criteria en bepaalde processtappen om hiermee om te gaan, zodat de afwegingen hierover navolgbaar zijn.

Bronnen

Voor het beoordelen van risico's bij het aangaan van internationale samenwerkingen raadplegen kennisinstellingen verschillende bronnen. Bronnen zien op verschillende risico-indicatoren en zijn niet voor elk type samenwerking even geschikt. In dit overzicht zijn bronnen opgenomen die de overheid en de instellingen betrouwbaar en nuttig achten.

Algemeen

Medewerkers en bestuurders hebben adviesteams, commissies en/of functionarissen tot hun beschikking, die geraadpleegd kunnen worden over risico's ten aanzien van kennisveiligheid. Bij een vermoeden van grote risico's vindt altijd overleg plaats.

Het Rijksbreed Loket Kennisveiligheid biedt informatie en advies bij vragen over risico's en te nemen maatregelen rondom internationale samenwerking in hoger onderwijs en wetenschap.

- Loket Kennisveiligheid

Wettelijke kaders

Vanuit de overheid worden de volgende bronnen aangereikt om te bepalen of, en onder welke voorwaarden, een samenwerking juridisch is toegestaan:

- Rijksoverheid - Internationale sancties
    - Sanctieregelingen - stand van zaken 20 maart 2025 | Regeling | Rijksoverheid.nl
- EU Sanctions Map
- United Nations Security Council Consolidated List
- Ontheffing voor Kennisembargo
    - Sanctieregeling Noord-Korea 2017
    - Sanctieregeling Iran 2012
    - Sanctieregeling territoriale integriteit Oekraïne 2014
- EU Dual-Use Verordening

Affiliaties en type organisatie

Door de Nederlandse inlichtingen- en veiligheidsdiensten worden dreigingsbeelden uitgebracht. In deze dreigingsbeelden komen China, Iran, Noord-Korea en Rusland naar voren als landen met een offensief (cyber)programma tegen Nederland en westerse belangen. In alle internationale samenwerkingen representeren deze landen een risicofactor. Met name bij sensitief technologisch onderzoek is er een groot risico op ongewenste kennis- en technologieoverdracht.

- Nationaal Coördinator Terrorismebestrijding en Veiligheid - Statelijke dreigingen
    - Dreigingsbeeld Statelijke Actoren 2025
    - Dreigingsbeeld Hybride en Militaire Dreigingen
    - Fenomeenanalyse Over de Grens

Instellingen maken daarnaast gebruik van verschillende online tools om risicobeoordelingen te maken. Onderstaande tools zijn behulpzaam bij het inschatten van militaire relaties en affiliaties met statelijke actoren voor verschillende landen:

- ASPI Defence University Tracker
- Named Research Organizations
- CSET

Vakgebied, type onderzoek en financiering

Het ministerie van OCW werkt aan een wetsvoorstel voor de invoering van een screeningsplicht, waarin een specifieke lijst sensitieve technologieën is opgenomen. Voor de beoordeling van sensitieve kennis en technologie raadplegen instellingen in elk geval deze lijst.

- Wetsvoorstel screening kennisveiligheid: Bijlage 2 van het wetsvoorstel en hoofdstuk III van de memorie van toelichting

Eerder hanteerden instellingen de lijst sleuteltechnologieën van NWO. Deze is nog steeds bruikbaar, maar wel breder dan de lijst uit het wetsvoorstel.

- Sleuteltechnologieën | NWO

Risico's op buitenlandse inmenging, heimelijke beïnvloeding en ethische kwesties zijn groter bij samenwerkingen waarin landen met beperkte academische vrijheid betrokken zijn. Deze bronnen zijn bruikbaar voor een eerste indicatie of er sprake is van risico's bij samenwerking. Bij landen met een score van 0.4 of lager op de Academic Freedom Index, of met een score van 5 of lager op de Democracy Index, zijn kennisinstellingen extra alert.

- Academic Freedom Index
- Democracy Index
- Freedom in the World
- World Justice Project Rule of Law

Ethiek en integriteit

Bij het aangaan van internationale samenwerkingen betrekken de instellingen de vijf principes zoals vastgelegd in de Nederlandse gedragscode wetenschappelijke integriteit.

- Nederlandse gedragscode wetenschappelijke integriteit

Contactgegevens

Rijksbreed Loket Kennisveiligheid

Telefoon: 088 042 42 42
E-mail: info@loketkennisveiligheid.nl
Website: www.loketkennisveiligheid.nl

Exportcontrole - Centrale Dienst voor In- en Uitvoer (CDIU)

Telefoon: 088 151 21 22
Website: www.douane.nl/onderwerpen/vgem/cdiu/Aanvraagformulier indelingsverzoek.