Indicatoren voor Risico-inschatting Internationale Samenwerkingen Kennisveiligheid

Appendix bij Nationale Leidraad Kennisveiligheid

Voorjaar 2025

Inhoud

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

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.

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 2
  - 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