Awti Adviesraad voor wetenschap, technologie en innovatie

KENNIS IN CONFLICT

VEILIGHEID EN VRIJHEID IN BALANS

Awti Adviesraad voor wetenschap, technologie en innovatie

De Adviesraad voor wetenschap, technologie en innovatie (AWTI) brengt gevraagd en ongevraagd advies uit aan regering en parlement. Zijn onafhankelijke adviezen zijn strategisch van aard en gaan over de hoofdlijnen van wetenschaps-, technologie- en innovatiebeleid. De leden van de AWTI zijn afkomstig uit kennisinstellingen en het bedrijfsleven. De AWTI doet zijn werk vanuit de overtuiging dat het belang van kennis, wetenschap en innovatie voor economie en samenleving groot is en in de toekomst nog verder zal toenemen.

Het secretariaat is gevestigd te:
Prins Willem-Alexanderhof 20
2595 BE Den Haag
t. 070 3110920
e. secretariaat@awti.nl
w. www.awti.nl

ISBN: 978-90-77005-92-7

Kennis in conflict

Veiligheid en vrijheid in balans

november 2022

Colofon

Fotografie	Capuski, via iStock
Ontwerp	2D3D Design; Kate Snow Design
Druk	Quantes
	november 2022
ISBN	978-90-77005-92-7

Alle publicaties zijn gratis te downloaden via www.awti.nl.

Auteursrecht

Inhoud

Samenvatting

In het licht van geopolitieke, technologische en maatschappelijke ontwikkelingen wordt internationale samenwerking voor kennisinstellingen steeds complexer. Het levert veel op, maar er kleven ook risico's aan. De afgelopen jaren hebben overheid en kennisinstellingen een aantal stappen gezet om deze risico's te mitigeren. Nuttige stappen, maar gezien de razendsnelle ontwikkelingen dienen steeds nieuwe uitdagingen zich aan. Daarom stelt de Adviesraad voor wetenschap, technologie en innovatie (AWTI) in dit rapport de vraag:

Hoe moeten we in Nederland omgaan met de risico's van internationale samenwerking bij kennisontwikkeling aan Nederlandse kennisinstellingen, inclusief het hoger onderwijs?

De focus van de analyse en advisering ligt op de Nederlandse (deels) publiek gefinancierde kennisinstellingen, inclusief instellingen voor hoger onderwijs, en hun directe ecosysteem van financiering, regulering en impact. De essentie van onze analyse is dat er voor een juiste aanpak steeds meerdere belangen gewogen moeten worden en simpele conclusies dus niet mogelijk zijn. De dilemma's waar kennisinstellingen voor staan zijn complex en vragen om een genuanceerde benadering. Juist in het omarmen van de nuance ligt volgens de AWTI de voortgang en de vooruitgang van beleid en praktijk rondom kennisveiligheid. Maar binnen de complexiteit van het onderwerp en de oproep tot nuance, ziet de AWTI wel degelijk mogelijkheden om stappen te (blijven) zetten.

Lerende aanpak nodig, met blijvende aandacht voor nuance en meer bewustwording

Om kennisontwikkeling in Nederland veilig én van hoog niveau te houden, is het volgens de AWTI nodig om de effectiviteit van de aanpak rondom kennisveiligheid blijvend te verbeteren. In die aanpak is meer aandacht nodig voor de nuance die de complexe situatie vraagt. Ook moet nog meer gewerkt worden aan bewustwording en ontwikkeling van kennis en kunde rondom kennisveiligheid bij alle betrokkenen.

Uit onze gesprekken en analyses kwam een aantal knelpunten rond het kennisveiligheidsbeleid naar voren. Zo is het denken en doen rondom kennisveiligheid kwetsbaar door een onderontwikkeld begrip en het nog niet geëvalueerde beleid rondom kennisveiligheid. Hoewel de genomen beleidsstappen waardering verdienen, staat de nuance in de toekomstige aanpak onder druk. We zien namelijk een reflex om zo veel mogelijk risico's te voorkomen, vaak aan de hand van vooraf opgestelde, bindende lijsten van kennisgebieden, waartoe sommige statelijke of niet-statelijke entiteiten geen toegang

zouden moeten krijgen. De vraag is of dit beleid effectief is. Dergelijke binaire lijsten zijn inadequaat om met de diversiteit aan factoren die het risico bepalen om te gaan. Ze zijn namelijk ofwel relatief lang, hetgeen tot onnodig veel restricties leidt en schade toebrengt aan de opbrengsten van internationale samenwerking. Of de lijst is vrij kort, waardoor de kennisveiligheid niet wordt vergroot. Het kennisveiligheidsbeleid laat ook verschillende tweede-orde effecten zien, die onvoldoende onderkend en meegewogen worden, zoals de reacties van andere landen op het beleid, opportunistisch gedrag van betrokkenen of een ineffectieve 'afvinkcultuur'.

Daarnaast blijkt uit onze gesprekken en analyses dat er bij verschillende betrokkenen nog onvoldoende aandacht is voor kennisveiligheid, in de context van maatschappelijke, technologische en geopolitieke ontwikkelingen en hun relatie met kennisveiligheid. Dat zijn onderzoekers, bestuurders en de overheid. Men is zich onvoldoende bewust van de toegenomen complexiteit en risico's rond internationale samenwerking, en weet dikwijls niet hoe met die risico's om te gaan. Handelingsperspectieven zijn op veel plekken nog afwezig.

Drie aanbevelingen voor een lerende aanpak rond kennisveiligheid

De AWTI doet drie aanbevelingen om het beleid rondom kennisveiligheid te verbeteren. We geven daarmee een gelaagde invulling aan het advies om te werken aan een lerende aanpak voor kennisveiligheid met blijvende aandacht voor nuance en meer bewustwording. De aanbevelingen sporen aan tot conceptualisatie, differentiatie en realisatie en grijpen in op verschillende plekken in het ecosysteem.

Met een lerende aanpak rondom kennisveiligheid kan Nederland nu en in de toekomst beter omgaan met de complexe uitdagingen van internationale samenwerking bij kennisontwikkeling. Het is onwaarschijnlijk dat het beleid in Nederland in één keer goed is. Dat is niet erg, mits de aanpak zo is ontworpen dat het de lessen kan incorporeren en zich kan aanpassen. Een lerende aanpak is het antwoord op de toenemende complexiteit, zonder onnodig afbreuk te doen aan de waarde van internationale samenwerking. Per definitie vraagt deze aanpak blijvend aandacht.

Het bevorderen van kennisveiligheid is volgens de AWTI voornamelijk een verantwoordelijkheid van de overheid, in samenspel met de kennisinstellingen. Bij de overheid komen de verschillende nationale belangen en perspectieven rondom kennisveiligheid en gerelateerde thema's bijeen, en worden ze afgewogen. Dit advies richt zich dan ook primair op de overheid. Maar het advies spreekt ook de kennisinstellingen aan. Immers, juist daar moet het leerproces rondom kennisveiligheid plaatsvinden. Bovendien is een effectieve en genuanceerde aanpak van de problematiek gebaat bij input en leiderschap vanuit de sector zelf. Het gevaar is dat wanneer deze

lerende aanpak zich onvoldoende ontwikkelt, de druk op de overheid toeneemt om minder genuanceerd, meer restrictief op te treden.

Onze aanbevelingen, die gelijktijdig opgepakt dienen te worden, zijn dan ook:

Aanbeveling 1. Conceptualiseer: verbeter het begrip van kennisveiligheid

Het denken en doen rondom kennisveiligheid staat nog in de kinderschoenen en is daarom vatbaar voor eenzijdige bekritisering vanuit specifieke perspectieven. De overheid heeft een leidende taak bij het verder ontwikkelen en verbeteren van begripsvorming rond kennisveiligheid en het in balans brengen van verschillende waarden en belangen. Hiertoe zijn twee concrete acties van de overheid vereist:

- Actie 1. Bevorder en deel de uitkomsten van het onderzoek naar kennisveiligheid in brede zin
- Actie 2. Stimuleer een brede, genuanceerde discussie over het onderwerp

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

Er is behoefte aan een aanpak van kennisveiligheid, die zowel duidelijkheid verschaft aan onderzoekers over wat wel en niet kan, als differentiatie mogelijk maakt naar type onderzoek, gebruikte data, sociale context en samenwerkingspartners. En die ingrijpt op zowel bewust als onbewust onveilig gedrag. Top-down, binaire, bindende regels miskennen de noodzaak van deze differentiatie. De overheid moet, samen met de kennisinstellingen, aan de slag om de risico's en maatregelen te verduidelijken en daarbij onderkennen dat differentiatie nodig is. We adviseren de volgende concrete acties:

- Actie 1. Ontwikkel een sectorbreed model ter professionalisering van de aanpak van kennisveiligheid
- Actie 2. Verken hoe organisatorische diversiteit van kennisinstellingen in Nederland beter benut kan worden voor kennisveiligheid

Aanbeveling 3. Realiseer: vergroot het bewustzijn en de capaciteit

Kennisinstellingen moeten het bewustzijn, de kennis en de kunde rondom kennisveiligheid verbeteren. De kennissector realiseert zich dat hij zich te verhouden heeft tot maatschappelijke, technologische en geopolitieke ontwikkelingen. Daaruit rijst de noodzaak om kennisveiligheid als onderwerp te erkennen. Kennisinstellingen zullen verder moeten werken aan de bewustwording van de risico's, ontwikkeling van kennis en expertise, en het vergroten van handelingsopties. Daartoe zijn de volgende acties nodig:

- Actie 1. Vergroot in de breedte en de diepte bewustzijn, kennis en kunde bij kennisinstellingen om risico's te mitigeren en kansen te pakken
- Actie 2. Breid de kennisveiligheidsteams bij kennisinstellingen uit

Advies. Gelijktijdig uitvoeren van de drie aanbevelingen door de overheid en de kennisinstellingen leiden gezamenlijk tot een lerende aanpak.

1

Toenemende complexiteit internationale samenwerking vraagt om aandacht

In het licht van geopolitieke, technologische en maatschappelijke ontwikkelingen wordt internationale samenwerking voor kennisinstellingen steeds complexer. Het levert veel op, maar er kleven ook risico's aan.

De afgelopen jaren is door de overheid en door kennisinstellingen een aantal stappen gezet om de risico's van internationale samenwerking te mitigeren. Nuttige stappen, maar gezien de razendsnelle ontwikkelingen dienen zich steeds nieuwe uitdagingen aan. Daarom stelt de AWTI in dit rapport de vraag: hoe moeten we in Nederland omgaan met de risico's van internationale samenwerking bij kennisontwikkeling aan Nederlandse kennisinstellingen, inclusief het hoger onderwijs?

De essentie van onze analyse is dat er geen simpele oplossingen zijn die recht doen aan de conflicterende belangen. De dilemma's waarvoor kennisinstellingen staan zijn complex en vragen om een genuanceerde en lerende benadering. Juist in het omarmen van de nuance ligt volgens de AWTI de voortgang en de vooruitgang van het beleid en de praktijk rondom kennisveiligheid. Ondanks de complexiteit van het onderwerp en de oproep tot nuance, ziet de AWTI wel degelijk mogelijkheden om stappen te (blijven) zetten.

1.1 Internationale samenwerking levert veel op, maar kent ook risico's

Internationale samenwerking is een wezenlijk kenmerk van kennisontwikkeling en in hoger onderwijs. Zowel binnen onderzoek en onderwijs, als bij de maatschappelijke uitwerking van onderzoek is internationale samenwerking sterk ontwikkeld. Dit levert veel op voor Nederland. Denk aan internationale mobiliteit van studenten en onderzoekers en de verrijking van de Nederlandse kennisbasis. Ook draagt internationale samenwerking bij aan het circuleren van kennis, zodat zij sneller toepassing vindt in hoogwaardige producten en diensten. Zo voegt internationale samenwerking waarde toe voor de samenleving, inclusief het innovatie- en verdienvermogen. Ten slotte is kennisuitwisseling van belang voor het aanpakken van mondiale maatschappelijke vraagstukken.

Tegelijkertijd zijn verschillende incidenten en onwenselijke situaties rond internationale samenwerking aan het licht gekomen, zoals ongewenste kennisoverdracht naar het buitenland of heimelijke beïnvloeding van onderzoek in Nederland. Veiligheidsdiensten

zien een toename van de dreiging van statelijke actoren. We geven een aantal voorbeelden.

Onwenselijke situaties bij internationale samenwerking

Er zijn de afgelopen jaren verschillende onderzoeken uitgevoerd waaruit blijkt dat statelijke en niet-statelijke actoren de veiligheid van kennisontwikkeling en hoger onderwijs in Nederland aantasten. In 2020 verstoorde de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) het werk van een Russische inlichtingenofficier. Deze runde een spionagenetwerk met toegang tot hightechbedrijven en een kennisinstelling.[1] Ook blijkt in Nederland sprake te zijn van buitenlandse inmenging in het hoger onderwijs en onderzoek,[2] in de vorm van (zelf)censuur door bedreigingen en beperking van de toegang tot onderzoeksmateriaal. Een internationaal team van onderzoeksjournalisten heeft laten zien dat er wordt samengewerkt tussen Europese universiteiten en aan het Chinese leger gelieerde kennisinstellingen op onderwerpen die militaire relevantie hebben.[3] Naast beïnvloeding en bedreiging kan de integriteit van onderzoek in het geding komen bij internationale samenwerking. Zo trok het tijdschrift Human Genetics in 2019 een onderzoek terug waarbij onderzoekers van de Erasmus Universiteit Rotterdam betrokken waren, omdat onvoldoende duidelijk was of het gebruikte genetische materiaal van Oeigoeren vrijwillig was afgestaan.[4]

Ook buiten Nederland vinden dergelijke incidenten plaats.[5] In het Verenigd Koninkrijk (VK) werden verschillende individuen geïdentificeerd die in dienst waren van het Chinese leger en tegelijkertijd aan Britse universiteiten werkten aan potentiële *dual use*[6] technologie.[7] Onlangs werd in Noorwegen een onderzoeker gearresteerd vanwege verdenking van spionage voor Rusland.[8]

1.2 Samenwerking wordt steeds complexer

Hoewel internationale samenwerking dus enerzijds een wezenlijk onderdeel is van kennisontwikkeling en veel oplevert, leidt het anderzijds tot risico's voor de nationale veiligheid. De balans tussen die kansen en risico's verschilt per situatie. Dat maakt

1 (AIVD, MIVD, en NCTV, 2021)
2 (d'Hooghe en Dekker, 2020)
3 (De Bruijn *e.a.*, 2022)
4 (Kempes en Strijker, 2021)
5 (Nouwens en Legarda, 2018; Long, 2019)
6 *Dual use* of 'tweeërlei gebruik' betreft goederen of kennis die zowel een civiele als militaire toepassing hebben. Een voorbeeld is biomedische kennis over ziekteverwekkers die zowel in de geneeskunde als in biologische oorlogsvoering kan worden gebruikt.
7 (Clark, 2022)
8 (Myklebust, 2022)

internationale samenwerking uiterst complex. We beschrijven hieronder vijf dilemma's die deze complexiteit illustreren. Ze komen voort uit bredere geopolitieke, technologische en maatschappelijke ontwikkelingen en verschillen in ethische standaarden. De dilemma's hebben uiteenlopende implicaties voor kennisinstellingen: zij krijgen met incoherente of zelfs tegenstrijdige signalen en eisen te maken.

Samenwerken met topwetenschappers

Het is van groot strategisch belang om samen te werken met onderzoekers die vooroplopen in belangrijke kennisdomeinen. Als Nederland achterblijft in de internationale strijd om kennis en technologisch leiderschap[9], remt dit onze innovatieve kracht en brengt dit strategische risico's met zich mee, bijvoorbeeld vanwege eenzijdige afhankelijkheden.[10] Voorheen vond het gros van het toponderzoek in 'bevriende' landen plaats, maar vandaag de dag doen steeds meer opkomende landen mee in de voorhoede van de wetenschap.[11] Samenwerking met topwetenschappers uit die landen is belangrijk om onze kennispositie te behouden, maar tegelijkertijd kan samenwerking nieuwe rivalen vooruithelpen in hun strijd om het technologisch leiderschap.[12]

Aanpakken van mondiale uitdagingen

Een ander dilemma treedt op bij kennisontwikkeling op het gebied van mondiale vraagstukken.[13] Onderzoekers worden gewaarschuwd om niet samen te werken met landen waar grondrechten niet gerespecteerd worden en waar andere waarden worden nageleefd dan in Nederland. Een dergelijke samenwerking kan afbreuk doen aan de wetenschappelijke integriteit van onderzoek. Tegelijkertijd is het voor de aanpak van mondiale uitdagingen als armoede, ongelijkheid, klimaatverandering en gezondheid juist nodig om samen te werken met landen waar een belangrijk deel van de oplossing ligt. Voor maximale impact van onze kennis is vaak maximale verspreiding en benutting nodig. Ook al wordt daar waar die problemen spelen soms vanuit andere normen en waarden gewerkt. Mogelijk kan samenwerking de onderzoekers in die landen zelfs helpen in hun moeizame relatie met de plaatselijke autoriteiten, afhankelijk van hoe deze onderzoekers zich opstellen en welke ruimte er bestaat. Samenwerken met (onderzoekers uit) landen waar andere waarden gelden levert dus enerzijds risico's op

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

voor wetenschappelijke integriteit, maar is een onmisbaar onderdeel in het aanpakken van wereldproblemen.

Open science en veiligheid

De trend naar meer *open science* leidt tot ingewikkelde dilemma's in relatie tot het vergroten van kennisveiligheid. *Open science* is gebaseerd op de overtuiging dat wetenschap een mondiaal publiek goed is en meer openheid, transparantie en samenwerking nodig is in de relatie tussen samenleving en wetenschap.[14] Dit krijgt vorm door datasets en ander onderzoeksmateriaal beter beschikbaar te maken voor buitenstaanders en door onderzoeksuitkomsten publiekelijk beschikbaar te maken en actief te delen. Het past bovendien bij *open science* om samen te werken met niet-wetenschappelijke stakeholders, zoals burgers en praktijkexperts. Echter, openheid, vrije toegang en transparantie maken het onderzoek kwetsbaar voor inmenging en spionage door partijen met kwade bedoelingen. Het afsluiten van onderzoek daarentegen, met als doel de veiligheid te vergroten, bemoeilijkt juist de *open science*-beweging.

Hoge verwachtingen en veel voorwaarden

In het licht van maatschappelijke uitdagingen, economische groei en nationale veiligheid stelt de samenleving hoge verwachtingen aan kennisinstellingen in Nederland. Denk bijvoorbeeld aan oplossingen voor maatschappelijke problemen en hoogwaardige kennis ten behoeve van het innovatieve bedrijfsleven.[15] Er is sprake van een toename van vragen aan kennisinstellingen en individuele onderzoekers. Meer vragen leiden ook tot een toename van de eisen en voorwaarden. Daar komen ook de zorgen bij op het gebied van integriteit en veiligheid. Dit zijn belangrijke aspecten die zorgen voor extra werk in de kennissector waar de werkdruk al hoog is. Het wordt daardoor mogelijk een nóg grotere uitdaging om talent aan te trekken en te behouden, waardoor de werkdruk op diegenen die in het onderzoek actief zijn verder toeneemt. En dat maakt het nóg moeilijker om aan de verwachtingen te voldoen.

WTI-diplomatie

De rol van wetenschap, technologie en innovatie in diplomatie[16] leidt tot een andersoortig dilemma. Er is een neiging om de economische en wetenschappelijke samenwerking tussen rivaliserende landen of machtsblokken te verbreken.[17] In termen van handel en andere vormen van samenwerking is dit vaak onontkoombaar. Maar in de wetenschap is

14 (Boulton, 2021)
15 (KNAW, 2019, 2021)
16 (AWTI, 2017b; Fägersten, 2022)
17 (Hudson *e.a.*, 2022)

enige vorm van samenwerking dikwijls wenselijk[18], omdat deze juist een opening biedt in conflicten en leidt tot wederzijds begrip.[19] Bovendien kan dit soort samenwerking leiden tot inzichten in de achterliggende oorzaken en belangen in het conflict.

Dilemma's. Internationale samenwerking wordt steeds complexer.

 **Samenwerking met topweten-schap(pers)** is belangrijk om onze goede kennispositie te behouden.	Kan nieuwe rivalen vooruithelpen in hun strijd om technologisch leiderschap.
 **Internationale samenwerking** cruciaal voor het aanpakken van mondiale uitdagingen.	Samenwerkingspartners met andere waarden vormen een risico voor wetenschappelijke integriteit.
 ***Open science*** is een belangrijke ontwikkeling voor de relatie tussen samenleving en wetenschap.	Vergroot kwetsbaarheden voor buiten-landse inmenging en spionage.
 **Hoge verwachtingen** van kennisinstellingen resulteert in veel vragen en voorwaarden.	Afname aantrekkelijkheid van onderzoek maakt het lastiger om verwachtingen waar te maken.
 **WTI diplomatie** biedt opening in conflict en leidt tot wederzijds begrip.	Rivaliserende landen neigen weten-schappelijke samenwerking te verbreken.

Bovenstaande dilemma's illustreren de uitdaging om de opbrengsten van internationale samenwerking op het gebied van kennisontwikkeling en hoger onderwijs te waarderen en tegelijkertijd het hoofd te bieden aan de toegenomen risico's en dreigingen. Als we dat niet op de juiste manier doen, dreigen kwaliteit, integriteit en impact van

18 (Fägersten, 2022), zie ook https://www.nwo.nl/en/science-diplomacy
19 (Kissinger, 1995)

kennisontwikkeling en hoger onderwijs te worden aangetast. En dat heeft gevolgen voor het welzijn, de veiligheid en het concurrentievermogen van Nederland.

1.3 Adviesvraag: Hoe gaan we om met de risico's bij internationale samenwerking?

In veel westerse landen is men zich bewust van de risico's bij internationale samenwerking. Als gevolg hiervan is de afgelopen jaren in rap tempo een nieuw beleidsterrein ontstaan. Dit kennisveiligheidsbeleid[20] betreft het beschermen of beveiligen van kennisontwikkeling en hoger onderwijs in relatie tot internationale ontwikkelingen. Kennisveiligheidsbeleid raakt aan wetenschapsbeleid, hogeronderwijsbeleid, onderzoeksbeleid, economisch beleid, buitenlandbeleid en binnenlands veiligheidsbeleid. Nederland bevindt zich internationaal gezien – achter enkele Angelsaksische landen en samen met een aantal Scandinavische landen – in de voorhoede wat betreft het nemen van maatregelen op dit gebied.[21]

Toch is het niet zo dat hiermee de problemen zijn opgelost. De ontwikkelingen gaan razendsnel, zowel op het gebied van wetenschap, technologie en innovatie, als in geopolitiek en -economisch opzicht.[22] Mondiale onderzoekssamenwerking is de afgelopen jaren juist enorm toegenomen.[23] De complexiteit neemt als gevolg van de genoemde ontwikkelingen naar verwachting alleen maar toe en het doel van het beleidsterrein kennisveiligheid moet daarop steeds worden aangepast. In het licht van het huidige geopolitieke tumult wordt het maatschappelijke debat rondom kennisveiligheid bovendien scherp aangezet. Dat leidt tot verhitte discussies en een scherpe stellingname van verschillende betrokkenen.[24]

---

20 Er worden overigens verschillende labels gebruikt, zoals *research security* (OECD, 2022), *tackling foreign interference* (European Commission. Directorate General for Research and Innovation, 2022), *trusted research* (UKRI, 2021) en *knowledge security* (Rathenau Instituut, 2021). Bovendien wordt in de beschrijving gerefereerd aan (*open*) *strategic autonomy*, research integrity en anti-coercion. In hoofdstuk 2 gaan we dieper in op deze uiteenlopende terminologie.

21 Zie bijvoorbeeld het OESO-portal over *research security* https://stip.oecd.org/stip/research-security-portal, waar Nederland tot het beperkte aantal landen behoort dat hiermee bezig is.

22 Zie bovendien de waarschuwing voor *normalcy bias* door de WRR: de psychologische reflex om een potentiële dreiging te bagatelliseren (Van der Dool, 2022).

23 Ruim tien jaar geleden bracht de AWT een advies uit getiteld 'De Chinese handschoen'. Dat advies signaleerde de groeiende relevantie van China als land voor wetenschap, technologie en innovatie. Hoewel in dit advies veel aandacht was voor de kansen – de AWT adviseerde om samenwerking te intensiveren – werden ook de nadelen en risico's benoemd. De AWT constateerde toen ook al de bezorgdheid over het weglekken van kennis en spoorde de regering aan om zich te beraden op welke kennis cruciaal is en hoe we deze kunnen behouden (AWT, 2012, p. 5).

24 Zie bijvoorbeeld het Tweeminutendebat van 14 september 2022 over Kennisveiligheid Nederlandse kennisinstellingen in de Tweede Kamer hierover en het gesprek bij het programma Op1 op 14 oktober 2022 over afhankelijkheden van China.

De AWTI stelt zich dan ook de volgende vraag: ***Hoe moeten we in Nederland omgaan met de risico's van internationale samenwerking bij kennisontwikkeling aan Nederlandse kennisinstellingen, inclusief het hoger onderwijs?*** Bij de beantwoording van deze vraag focussen we op de Nederlandse (deels) publiek gefinancierde kennisinstellingen, inclusief instellingen voor hoger onderwijs, en hun directe ecosysteem van financiering en impact. Hoewel we erkennen dat ook bij bedrijven en maatschappelijke organisaties uitdagingen bestaan op het gebied van buitenlandse inmenging, spionage of sabotage, vormen deze geen onderdeel van dit advies. Cybersecurity is weliswaar een gerelateerd thema, maar ook daar leggen we in dit advies niet de nadruk op, anders dan waar het onderdeel is van kennisveiligheid. Cybersecurity krijgt als onderwerp al langer aandacht en past beter bij de taak en expertise van andere instanties.[25]

Totstandkoming advies

Dit advies is in een aantal stappen tot stand gekomen (zie Bijlage 1). Ter verkenning van het onderwerp hebben we gesproken met verschillende experts en stakeholders (zie Bijlage 2). Ook zijn inzichten verzameld aan de hand van een aantal deelanalyses en casestudies (zie bijvoorbeeld Bijlage 3 en Bijlage 4). Het LeidenAsiaCentre heeft bovendien een internationale vergelijking gedaan naar maatregelen voor kennisveiligheid in twaalf landen.[26] De deelanalyses zijn besproken tijdens de raadsvergaderingen om tot een advieslijn te komen, met aanbevelingen. Deze advieslijn is vervolgens besproken met verschillende stakeholders en experts. We danken alle gesprekspartners voor hun tijd, openheid en inzichten.

Projectgroep

Dit advies is voorbereid door een projectgroep bestaande uit de raadsleden Chokri Mousaoui, Ellen Moors, Sjoukje Heimovaara en Koenraad Debackere, en stafleden Chris Eveleens, Bart Gulden, Tara van Viegen en Sabine Jaegers.

Boodschap en structuur van dit adviesrapport

Hoofdstuk 2 bespreekt de resultaten van de analyses. Onze belangrijkste conclusie is dat een lerende aanpak nodig is, met blijvende aandacht voor nuance en meer bewustwording. We zien namelijk dat het beleid rondom kennisveiligheid kwetsbaar is, de

25 Zoals de Cyber Security Raad, het National Cyber Security Centre. Zie ook (Bertuzzi, 2022)
26 (d'Hooghe en Lammertink, 2022). Beschikbaar op www.awti.nl

nuance onder druk staat, de risico's onvoldoende zijn doorgedrongen tot de belanghebbenden, en de handelingsperspectieven ontbreken.

Hoofdstuk 3 bevat vervolgens drie aanbevelingen om de huidige aanpak te verbeteren. Ondanks de complexiteit van het onderwerp en de oproep tot nuance, ziet de AWTI wel degelijk mogelijkheden om stappen te (blijven) zetten. Met de drie aanbevelingen en onderliggende acties willen we bijdragen aan een verbetering van het begrip, het beleid en de praktijk rondom kennisveiligheid in Nederland.

2

Lerende aanpak nodig, met aandacht voor nuance en meer bewustwording

Om kennisontwikkeling in Nederland veilig én van hoog niveau te houden, is het volgens de AWTI nodig om de effectiviteit van de aanpak rondom kennisveiligheid blijvend te verbeteren. In die aanpak is aandacht nodig voor de nuance die de complexe situatie vraagt. Ook moet nog meer gewerkt worden aan bewustwording en aan het ontwikkelen van kennis en kunde rondom kennisveiligheid bij alle betrokkenen.

Uit onze gesprekken en analyses kwam een aantal knelpunten rond het kennisveiligheidsbeleid naar boven. Zo is het denken en doen rondom kennisveiligheid kwetsbaar door een onderontwikkeld begrip ervan en het nog niet geëvalueerde beleid (paragraaf 2.1). De stappen die zijn gezet verdienen waardering, maar de nuance in de aanpak staat onder druk (paragraaf 2.2). De ontwikkelingen vragen aandacht van alle betrokkenen: onderzoekers, bestuurders en de overheid. Men is zich echter onvoldoende bewust van de toegenomen complexiteit en risico's. Handelingsperspectieven zijn bovendien onvoldoende aanwezig (paragraaf 2.3). In dit hoofdstuk werken we deze knelpunten verder uit. In hoofdstuk 3 doen we concrete aanbevelingen om de aanpak rondom kennisveiligheid te verbeteren.

2.1 Denken en doen rondom kennisveiligheid kwetsbaar

Kennisveiligheid gaat in algemene zin om het voorkomen of mitigeren van een aantal risico's en dreigingen die voortkomen uit internationale verhoudingen of samenwerking. Het belang ervan wordt onderkend en de bekendheid groeit. Toch is het denken en doen rondom kennisveiligheid kwetsbaar.

Die kwetsbaarheid heeft een aantal redenen. De conceptualisatie van kennisveiligheid is nog onderontwikkeld en zal zowel een bewegend als bewegelijk doel blijven. Verschillende perspectieven op kennisveiligheid, zoals een academisch perspectief, een veiligheidsperspectief en een economisch perspectief, trekken de discussie bovendien snel in extremen. Daarnaast zijn de maatregelen in het kader van kennisveiligheid, nationaal en internationaal, nog relatief nieuw, waardoor evaluaties van het functioneren en de effectiviteit van het beleid nog niet zijn uitgevoerd.

Beschrijving kennisveiligheid bruikbaar, maar conceptualisatie nog onderontwikkeld

Er bestaat in Nederland een breed gedragen beschrijving van kennisveiligheid, die wordt gehanteerd door de overheid en kennisinstellingen.[27] Deze stelt dat kennisveiligheid gaat om het voorkomen of tenminste mitigeren van een aantal risico's en dreigingen die voortkomen uit internationale verhoudingen en samenwerking. Volgens de beschrijving in de leidraad kennisveiligheid gaat het grofweg om drie soorten risico's (zie het kader hieronder): a) ongewenste overdracht van kennis en technologie met negatieve gevolgen voor nationale veiligheid of innovatiekracht, b) ongewenste beïnvloedings- en inmengingsactiviteiten in hoger onderwijs en wetenschap en c) problematische ethische kwesties.

Beschrijving kennisveiligheid

Kennisveiligheid wordt door kennisinstellingen en de overheid doorgaans als volgt omschreven:

"Bij kennisveiligheid gaat het in de eerste plaats om het voorkomen van ongewenste overdracht van gevoelige kennis en technologie. Van ongewenste overdracht is sprake als onze nationale veiligheid in het geding komt. Kennisveiligheid richt zich daarnaast op heimelijke beïnvloeding van onderwijs en onderzoek door andere staten. Die inmenging brengt de academische vrijheid en sociale veiligheid in gevaar. Kennisveiligheid gaat verder over ethische kwesties die een rol kunnen spelen bij samenwerking met landen die de grondrechten niet respecteren."[28]

De beschrijving van kennisveiligheid is volgens verschillende gesprekspartners nadrukkelijk niet bedoeld als formele definitie.

Hoewel bovenstaande beschrijving van kennisveiligheid bruikbaar is gebleken bij het beter begrijpen van de uitdagingen en het gezamenlijk interveniëren daarop, is ze niet onproblematisch.[29] Allereerst bestaat er aanzienlijke ruimte voor interpretatie. Zo zijn de grenzen van wat wel en niet onder kennisveiligheid past vaag. Wat is precies onwenselijk en volgens wie? Bij het tegengaan van klimaatverandering bijvoorbeeld kan de uitwisseling van duurzame technologische kennis tussen kennisinstellingen van groot

27 Snetselaar (2022) laat zien hoe de term kennisveiligheid werd geïntroduceerd om een gezamenlijke probleemdefinitie te hebben van een complex sociale wereld ('rendering'). Het bracht een set aan problemen die opkwamen onder een label. Door de risico's en de oorzaken te benoemen, kon actie worden ondernomen.

28 (Universiteiten van Nederland *e.a.*, 2022, pp. 9–10)

29 Dit volgt uit de discussies die we over het begrip voerden, als raad en met verschillende stakeholders. Het blijkt dat verschillende kennisinstellingen de nadruk of afbakening anders leggen als het gaat om wat zij onder kennisveiligheid verstaan. Zie ook Snetselaar (2022, p. 11).

belang zijn. Maar vanuit commercieel oogpunt is het wellicht wenselijk om die kennis door te ontwikkelen tot innovatieve toepassingen, waaraan naast maatschappelijke baten ook economische baten zitten. Ook zijn de causale verbanden tussen beslissingen in de onderzoekspraktijk en de uiteindelijke, eventuele negatieve, gevolgen onzeker. Hoewel onderzoekers een verantwoordelijkheid hebben voor welke kennis zij ontwikkelen, is het uiteindelijke gebruik vaak niet op voorhand te bepalen. Dit is niet alleen afhankelijk van het onderwerp waarop kennis ontwikkeld wordt en de directe samenwerkingspartners, maar ook van de bredere sociale en politieke context waarbinnen die kennis wordt opgedaan en zich verspreidt.

In de beschrijving valt verder op dat de verschillende risico's breed geformuleerd zijn. Zo wordt er geen onderscheid gemaakt tussen bewust genomen risico's en (onbewuste) naïviteit (zie kader hieronder). Ongewenste kennisoverdracht kan bovendien op legale en illegale wijze plaatsvinden; beide vormen vallen onder de beschrijving. De ethische dimensie van kennisveiligheid heeft betrekking op de integriteit van het onderzoek zelf (*ethics dumping*), maar ook op wat er later met de uitkomsten wordt gedaan (*misuse*). Kortom, het is lang niet altijd duidelijk of een situatie een risico vormt voor de kennisveiligheid hetgeen ingrijpen bemoeilijkt. Anders gezegd: het ontbreken van een heldere conceptualisatie staat een effectieve aanpak in de weg.[30]

Bewust en onbewust gedrag

In relatie tot kennisveiligheid onderscheiden we onbewust en bewust gedrag. Onbewuste aantasting van kennisveiligheid gebeurt vaak vanuit een zekere naïviteit. Bijvoorbeeld als iemand bij een bezoek aan het buitenland de computer of telefoon onvoldoende beschermt of online kennis deelt die in het buitenland misbruikt kan worden. Ook kan een onderzoeker ongemerkt gevoed worden met misinformatie of heimelijk beïnvloed worden.

Bewust gedrag dat tot aantasting van kennisveiligheid leidt, vindt bijvoorbeeld plaats als onderzoekers uit Nederland een aantrekkelijk buitenlands aanbod krijgen om samen te werken op onderwerpen waarvan bekend is dat deze sensitief zijn. Ook wanneer een onderzoeker meerdere affiliaties heeft, waaronder in het buitenland, maar deze bewust niet opgeeft bij Nederlandse instellingen of onderzoeksfinanciers, is de kennisveiligheid in het geding.

30 (Gort, 2011)

De Nederlandse beschrijving van kennisveiligheid is in lijn met, maar niet gelijk aan de beschrijvingen die in het internationale discours worden gebruikt.[31] Dat is *a priori* geen probleem, maar zeker wanneer gepleit wordt voor internationale afstemming of zelfs een gecoördineerde aanpak, is het goed om de verschillen te onderkennen. Bovendien reflecteert de gehanteerde terminologie in (groepen) landen de specifieke focus en aanpak aldaar.[32] De Organisatie voor Economische Samenwerking en Ontwikkeling (OESO), bijvoorbeeld, gebruikt de term *research security*.[33] Onder *research security* verstaat men het voorkomen van ongewenste buitenlandse statelijke of niet-statelijke inmenging in de onderzoekspraktijk, met als doel het veiligstellen van het onderzoeks-ecosysteem en de nationale en economische belangen die daarmee samenhangen.[34] De nadruk ligt bij de OESO dus meer op de praktijk en processen van onderzoek doen, en in mindere mate op de kennis zelf. In de Verenigde Staten (VS) ligt de nadruk in het beleid voornamelijk op technologische en economische dominantie.[35] De Europese Commissie (EC) gebruikt de term *foreign interference in research and innovation*.[36] Foreign interference, ofwel buitenlandse inmenging, betekent volgens de EC 'dwingende, heimelijke, bedrieglijke of corrumperende activiteiten van statelijke actoren die ingaan tegen de soevereiniteit, waarden of belangen van de Europese Unie'.[37] Deze definitie komt dus met name overeen met het tweede aspect in de Nederlandse beschrijving van kennisveiligheid, die gaat om het voorkomen van heimelijke beïnvloeding van onderzoek en onderwijs. De G7 gebruikt ook de term *research security*. De nadruk ligt hier op het beschermen van de onderzoeksgemeenschap en hangt ook samen met sociale veiligheid. Door de G7 wordt *research security* consistent in combinatie gebruikt met de term wetenschappelijke integriteit (*scientific integrity* of *research integrity*).[38] Onder wetenschappelijke integriteit verstaat men het naleven van professionele waarden, principes en praktijken die leiden tot de validiteit, maatschappelijke relevantie,

31 Zie voor een uitgebreidere bespreking van de verschillen en overeenkomsten (d'Hooghe en Lammertink, 2022)
32 Het internationaal vergelijkende onderzoek van het LeidenAsiaCentre brengt helder in kaart hoe de gekozen terminologie in verschillende landen samenhangt met de nationale context en gekozen aanpak (d'Hooghe en Lammertink, 2022). Het maakt dus uit welke woorden worden gebruikt.
33 (OECD, 2022)
34 "Research security is about preventing undesirable foreign state or non-state interference with research. The main goal of research security is to protect the research ecosystem and thus protect legitimate national and economic interests." (OECD, 2022)
35 (National Security Commission on Artificial Intelligence, 2021)
36 (European Commission. Directorate General for Research and Innovation, 2022)
37 "Foreign interference are activities that are carried out by, or on behalf of, a foreign state-level actor, which are coercive, covert, deceptive, or corrupting and are contrary to the sovereignty, values, and interests of the European Union (EU)."(European Commission. Directorate General for Research and Innovation., 2022)
38 (G7, 2022; Scientific integrity fast-track action committee, 2022)

verantwoordelijkheid en kwaliteit van onderzoek.[39] De beschrijving bevat een interne component (over de validiteit en kwaliteit van onderzoek) en een externe component (relevantie en verantwoordelijkheid). De interne component zien we niet zo zeer terug in de Nederlandse beschrijving van kennisveiligheid; de externe component zien we wel terug in het onderdeel over ethische kwesties.

Verschillende perspectieven op kennisveiligheid trekken discussie in extremen

Kennisveiligheid kan benaderd worden vanuit tenminste drie perspectieven[40]: een veiligheidsperspectief, een academisch perspectief en een economisch perspectief. De verschillende standpunten en argumenten in de discussie over internationale samenwerking in kennisontwikkeling zijn vaak terug te voeren op deze perspectieven (zie ook Bijlage 4). Elk perspectief biedt immers een eigen blik op de waarden die gehanteerd worden in de discussie rondom kennisveiligheid. Het aanpakken van kennisveiligheid vraagt om het afwegen van deze waarden. Er zijn zowel raakvlakken als verschillen.

Binnen het veiligheidsperspectief spelen stabiliteit en soevereiniteit een belangrijke rol. Die waarden zien we ook terug bij het economische en academische perspectief, voornamelijk onder de noemer van autonomie. Zo is er op economisch gebied het belang van (open) strategische autonomie, waarmee grofweg het vermogen om zelfstandig te besluiten en handelen, en zelfvoorzienend en -redzaam te zijn wat betreft industrie, technologie en diplomatie wordt bedoeld.[41] Op academisch gebied is er de kernwaarde van institutionele autonomie, waarmee de garantie van academische vrijheid voor wetenschappelijke instellingen wordt bedoeld.[42] Bij het tegengaan van ongewenste inmenging zijn er raakvlakken tussen deze perspectieven.

Maar er zijn ook verschillen. Het veiligheidsperspectief wordt namelijk gekenmerkt door het willen ‘behouden’ of ‘beschermen’ van onze manier van werken en leven, terwijl het economische en academische perspectief zich eerder laten kenmerken door ‘verbeteren’ of ‘veranderen’. In economische zin uit zich dat in het vrije verkeer van goederen, diensten en personen om het economisch potentieel te verbeteren. In academische zin uit zich dat in het vrije verkeer van personen, data, onderzoekssamenwerkingen en -resultaten om zo de maatschappelijke impact van wetenschap te vergroten. Deze tegenstrijdigheden in de verschillende perspectieven verklaren de zoektocht naar en het belang van een balans tussen openheid en geslotenheid. Vanuit het

39 “Research integrity is the adherence to the professional values, principles, and best practices that ensure and uphold the validity, social relevance, responsibility, and quality of research.” (G7, 2022, p. 7)
40 Deze perspectieven zijn duidelijk terug te vinden in documenten en de gesprekken die we voerden. In Bijlage 4 beschrijven en vergelijken we de drie perspectieven uitgebreider.
41 Zie bijvoorbeeld De Jager e.a. (zonder datum)
42 (KNAW, 2021)

veiligheidsperspectief neigt men naar een gesloten positie, terwijl het economische en academische perspectief juist overwegend vragen om openheid.

Het is daarom van belang om te duiden welk perspectief de toon van de discussie bepaalt en beïnvloedt. Als vanuit een academisch perspectief de waarden van academische vrijheid of institutionele autonomie tot in het absolute worden nagestreefd, maakt dit inbreuk op waarden als veiligheid en stabiliteit, die dominant zijn vanuit een veiligheidsperspectief. Als strategische autonomie, vanuit een veiligheidsperspectief, te ver wordt doorgevoerd, ontstaat een spanning met openheid, een belangrijke waarde (en waarde-creërende dimensie) vanuit het academische en economische perspectief. Om recht te doen aan de verschillende waarden, kan geen ervan dus absoluut worden gesteld. Bij het ontwikkelen van kennisveiligheidsbeleid moet dus continue een afweging worden gemaakt tussen de verschillende waarden.

Wanneer de waarden uit een bepaald perspectief dominant worden en de discussie in het extreme wordt getrokken, belemmert dit beleidsontwikkeling. Zonder consensus zijn legitimiteit en haalbaarheid van beleidsmaatregelen immers beperkt en dat bemoeilijkt implementatie. Vormt een extreme positie het uitgangspunt voor beleid en maatregelen, dan zien we in de praktijk een aantasting van andere waarden. Daar wordt vervolgens op gecorrigeerd en zo ontstaat ‘zwalkend’ beleid, dat internationale samenwerking bemoeilijkt en kwaliteit van onderzoek negatief beïnvloedt.

Relatief nieuw beleidsterrein bemoeilijkt effectbepaling

Een herkenbaar startpunt voor het kennisveiligheidsbeleid in Nederland was de kamerbrief van eind 2020.[43] Het beleid dat daarmee vorm kreeg, strekt zich uit over verschillende ministeries. Tegen een achtergrond van al bestaande, wettelijke maatregelen (zoals exportregelgeving en kennisembargo’s tegen Iran en Noord-Korea) en niet-wettelijke maatregelen (zoals de gedragscode wetenschappelijke integriteit) zijn de afgelopen twee jaar nieuwe maatregelen getroffen die moeten bijdragen aan kennisveiligheid.[44] De kern van het beleid bestaat uit maatregelen genomen door de ministeries van Onderwijs, Cultuur en Wetenschap, van Economische Zaken en Klimaat, en van Justitie en Veiligheid. Die maatregelen zijn bijvoorbeeld een nationale leidraad en kennisveiligheidsloket, bestuurlijke afspraken en een systematische risicoanalyse bij

43 We markeren de brief ‘Kennisveiligheid hoger onderwijs en wetenschap’ als start van het beleid (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020). Uiteraard ontstond dit beleid niet uit het niets en zijn er andere relevante activiteiten aan te wijzen. Die eerdere activiteiten zijn meegenomen in de beleidsanalyse (zie Bijlage 3).

44 Bijlage 3 bevat een geannoteerd overzicht van een groot aantal maatregelen (beleidsinstrumenten, gedragscodes, wetgeving, et cetera) die gerelateerd zijn aan kennisveiligheid.

kennisinstellingen.[45] Het doel van het kennisveiligheidsbeleid is om "*internationale samenwerking op een veilige manier te laten plaatsvinden, met oog voor zowel de kansen als de risico's die ermee samenhangen.*"[46] Het ministerie van Onderwijs, Cultuur en Wetenschap heeft een leidende en coördinerende rol. Andere ministeries zijn leidend in een aantal gerelateerde maatregelen zoals de 'Wet veiligheidstoets, investeringen, fusies en overnames' (Wet vifo)[47] en de aangescherpte spionagewetgeving.[48] Daarnaast werken de veiligheids- en inlichtingdiensten aan kennisveiligheid. Zij vallen onder het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het ministerie van Defensie, en hebben als doel om de nationale veiligheid te beschermen.[49] Tot slot heeft ook het ministerie van Buitenlandse Zaken beleid dat raakt aan het kennisveiligheidsbeleid, bijvoorbeeld via het postennetwerk en de China-strategie.[50] Zo ontvouwt zich een vrij nieuw en divers pakket aan maatregelen, ontwikkeld en geïmplementeerd vanuit verschillende ministeries, dat antwoord moet geven op de ontwikkelingen in de wereld.

Ook in andere landen is het beleid sterk in ontwikkeling. Het onderzoek dat het LeidenAsiaCentre (LAC) in opdracht van de AWTI uitvoerde, brengt dit diepgravend en overzichtelijk in beeld.[51] De studie laat bijvoorbeeld zien dat er een brede variatie aan aanpakken bestaat, in termen van structuur (*governance*) en maatregelen. Een van de dimensies waarop deze variatie tot uiting komt is of de aanpak meer *top-down* is, zoals in Japan en Frankrijk, of meer *bottom-up* zoals in Finland en Duitsland.[52] Ook een combinatie van top-down wetgevende maatregelen met bottom-up initiatieven komt voor, zoals bijvoorbeeld in Australië en het Verenigd Koninkrijk. Een andere dimensie is de mate van dwang of handhaving binnen de maatregelen. Sommige landen hebben een meer dwingende, juridische aanpak, met bijvoorbeeld verplichte registratie van samenwerking (Australië), openbaarmaking van onderzoeksfinanciering (in de VS en het VK) of verplichte screening voor contracten (Frankrijk). In het Verenigd Koninkrijk en Australië bijvoorbeeld voeren officiële instanties de controle hierop uit.[53] In de andere landen kiest men niet voor dergelijke dwingende, juridische maatregelen.

45 Het ministerie van OCW heeft over het algemeen een leidende rol in het kennisveiligheidsbeleid (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020; Minister van OCW, 2022b, 2022a; Minister van OCW, Minister van EZK, en Minister van J&V, 2022)..
46 (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020, p. 1)
47 (Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, 2022b)
48 (Ministerie van Justitie en Veiligheid, 2022)
49 Zie bijvoorbeeld de openbare jaarverslagen van de AIVD (AIVD, 2022) en MIVD (MIVD, 2022), en het dreigingsbeeld statelijke actoren (AIVD, MIVD, en NCTV, 2021).
50 (Ministerie van Buitenlandse Zaken, 2019; Minister van Buitenlandse Zaken, 2021)
51 (d'Hooghe en Lammertink, 2022)
52 (d'Hooghe en Lammertink, 2022, pp. 49–50)
53 (d'Hooghe en Lammertink, 2022, p. 50)

De OESO heeft onderzoek gedaan naar onderzoeksintegriteit en -veiligheid.[54] Het rapport bevat – naast een inventarisatie van de risico's – een overzicht van beleidsinitiatieven en -activiteiten in de OESO-landen. Veel van de casuïstiek komt uit Angelsaksische landen, maar ook instrumenten uit Duitsland, Zweden en Nederland worden beschreven. De onderzoekers concluderen dat de verantwoordelijkheden voor onderzoeksintegriteit en onderzoeksveiligheid verdeeld zijn over verschillende actoren, zoals nationale overheden, onderzoeksfinanciers en instellingen. Om kennis over maatregelen te vergroten, is de OESO een zogenaamd *research security portal* gestart.[55]

Het kennisveiligheidsbeleid is niet alleen nieuw en divers, maar ook nog nauwelijks geëvalueerd. Dat maakt het vooralsnog lastig vast te stellen wat het effect van het beleid is. Bij het schrijven van dit advies was van de 120 maatregelen die in het OESO-portal zijn opgenomen er nog geen één formeel geëvalueerd. In Australië en Finland zijn wel parlementaire onderzoeken gedaan naar het kennisveiligheidsbeleid; ook de interviews en analyses van de LAC-studie bieden inzicht.[56] Deze analyses suggereren dat de bewustwordingscampagnes in Australië, Duitsland, Finland, het VK en de VS effectief waren. De LAC-studie laat een verband zien tussen enerzijds de effectiviteit en anderzijds de uitgebreidheid, coherentie en het pragmatisme van het beleid en de mate van afstemming tussen overheid en kennisinstellingen. Toch is meer onderzoek nodig. De OESO-onderzoekers pleiten ervoor dat overheden, organisaties voor onderzoeksfinanciering, onderzoeksinstellingen en hogeronderwijsinstellingen met regelmaat bepalen in hoeverre hun veiligheidsstrategie voldoende volwassen is. En, om indien nodig hun beleid aan te passen om de effectiviteit te vergroten en onbedoelde consequenties te monitoren.

2.2 Er zijn goede stappen gezet, maar nuance in de aanpak staat onder druk

De stappen die zijn gezet voor het vergroten van kennisveiligheid verdienen waardering. Er is echter wel een balans nodig tussen openheid en vrijheid enerzijds, en geslotenheid en regulering anderzijds. Die balans is niet overal gelijk, maar hangt onder andere af van het onderzoeksgebied, toepassingsmogelijkheden en samenwerkingslanden. We constateren dat de nuance bij het zoeken van die balans onder druk staat, vanwege extreme posities in het debat en de reflex om risico's te minimaliseren. Dit komt de effectiviteit van de aanpak niet ten goede.

54 (OECD, 2022)
55 https://stip.oecd.org/stip/research-security-portal
56 (d'Hooghe en Lammertink, 2022, p. 51)

Het recent ontwikkelde kennisveiligheidsbeleid bouwt voort op een bestaande mix van beleid (zie Bijlage 3 voor een geannoteerd overzicht van zowel bestaand als nieuw beleid). De overheid en de kennisinstellingen hebben belangrijke stappen gezet en dat verdient waardering. De beleidsontwikkelingen houden rekening met belangrijke waarden voor kennisontwikkeling en benutten de overlegcultuur en -structuren rondom wetenschap, technologie en innovatie. We constateren bovendien dat Nederland een van de landen is die een internationale voorbeeldfunctie heeft.

Uit woord en daad van de minister van Onderwijs, Cultuur en Wetenschap blijkt dat beleidsmakers in Den Haag zijn doordrongen van de gevoeligheid van het ingrijpen in de wetenschap ten behoeve van kennisveiligheid.[57] Het door hen ontwikkelde beleid bestaat dan ook uit een aantal elementen. Zo draagt de leidraad kennisveiligheid bij aan het verhogen van begrip, kennis en bewustwording rondom kennisveiligheid. Het kennisveiligheidsloket verzamelt en bundelt informatie vanuit de overheid en voorziet kennisinstellingen van advies. Op aandringen van de Kamer heeft de overheid bovendien alle kennisinstellingen in Nederland gevraagd om een risicoanalyse kennisveiligheid uit te voeren. De risicoanalyse van universiteiten wordt getoetst via een externe audit.[58] Daarnaast is een toetsingskader individuen in voorbereiding, dat later in deze paragraaf wordt besproken. Het beleid is tot nu toe grotendeels uitgegaan van zelfregulering. De aangekondigde audits gaan echter een stap verder en hebben een meer top-down karakter. Door de introductie van het toetsingskader individuen verandert de relatie tussen de overheid en kennisinstellingen als het gaat om het aantrekken van onderzoekers uit bepaalde landen.

In de aanpak wordt over het algemeen goed gebruikgemaakt van de overlegstructuren in de sector.[59] Zo is de nationale leidraad kennisveiligheid opgesteld door een brede groep organisaties, te weten UNL, KNAW, Vereniging Hogescholen, NFU, TO2-federatie, NWO en de Rijksoverheid.[60] Er wordt veel waarde gehecht aan de dialoog; de minister van OCW heeft bestuurlijke afspraken gemaakt met de kennisinstellingen en er vindt regelmatig overleg plaats tussen instellingen en de minister over het kennisveiligheidsbeleid.[61] Er zijn een portefeuillehouder op bestuursniveau en een ‘adviesteam kennisveiligheid’ benoemd.[62] In de praktijk hebben instellingen een

57 Commissiedebat Internationalisering en Kennisveiligheid van 9 februari 2022 (https://debatgemist.tweedekamer.nl/debatten/internationalisering-en-kennisveiligheid) en (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020)
58 (Van der Woude en Van der Molen, 2022)
59 (van der Meulen en Rip, 1998)
60 (Universiteiten van Nederland *e.a.*, 2022). De leidraad bouwde voort op een kader kennisveiligheid universiteiten, ontwikkeld door de VSNU, de voorloper van UNL (VSNU, 2021).
61 Zie bijvoorbeeld (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020) en (Minister van OCW, 2022a)
62 (Minister van OCW, 2022b, p. 1)

‘beleidsadviseur’, ‘project-‘ of ‘programmamanager’ kennisveiligheid, die al dan niet voltijds bezig is met ontwikkeling, implementatie en monitoring van het beleid rondom kennisveiligheid. Zij voeren onder andere de eerdergenoemde risicoanalyse kennisveiligheid uit, op verzoek van de minister.[63]

Internationaal kijkt men naar Nederland als een van de landen die vrij ver is in het ontwikkelen van een aanpak kennisveiligheid.[64] We zijn weliswaar minder ver dan de Angelsaksische landen, maar toch is er in korte tijd behoorlijk veel kennis en expertise over kennisveiligheid opgebouwd. De inbreng van Nederlandse experts en beleidsmakers wordt internationaal dan ook gewaardeerd. Vooral het kennisveiligheidsloket valt daarbij op. Hoewel evaluatie nog niet heeft plaatsgevonden, wordt het loket door veel van onze gesprekspartners in binnen- en buitenland als *good practice* aangemerkt.[65]

Balans en differentiatie cruciaal

Velen, waaronder de minister van Onderwijs, Cultuur en Wetenschap, hebben het belang van proportionaliteit benadrukt in de aanpak van kennisveiligheid.[66] Het gaat om het vinden van een balans tussen *securitization* (het doorslaan in veiligheid) en naïviteit. Beide uitersten leiden tot gevaren en verliezen. Immers, bij een naïeve aanpak kan misbruik worden gemaakt van de openheid en transparantie bij kennisontwikkeling en in hoger onderwijs, teneinde deze te beïnvloeden of zich de ontwikkelde kennis toe te eigenen. Maar ook bij over-regulatie of een doorslaan in veiligheid ontstaat een onwenselijke situatie.[67] In het bijzonder zien we het risico op stigmatisering van mensen uit bepaalde landen[68], aantasting van de positieve gevolgen wetenschap inzetten als zachte kracht voor diplomatie[69], en beperking van competitiviteit en vooruitgang.[70]

---

63 (Minister van OCW, 2022b)
64 Dit blijkt uit de gesprekken die we hebben gevoerd met gesprekspartners buiten Nederland.
65 Bijvoorbeeld in de Mutual Learning Exercise van de Europese Commissie. Ook in het EU-Knowledge Network on China (EU-KNOC) wordt de Nederlandse inbreng gewaardeerd, aldus onze internationale gesprekspartners.
66 Zie bijvoorbeeld de Kamerbrief ‘Kennisveiligheid in hoger onderwijs en wetenschap’ waarin staat “Het motto ‘open waar mogelijk, beschermen waar nodig’ blijft het uitgangspunt: het draait steeds om proportionaliteit en maatwerk.” (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020, p. 3). Vanuit de G7 stelt men zich ook de vraag “How to keep science open, but also secure?” (Hudson, 2022).
67 Zelfs, of juist, in de meest gevoelige sociale of geopolitieke situaties, is in het verleden gepleit voor openheid en vrijheid (Stone *e.a.*, 2022). Deze waarden bleken en bleven een wezenlijk onderdeel van het (wetenschappelijke) onderzoekssysteem.
68 Zie bijvoorbeeld (Ellis en Gluckman, 2019; Fischer, 2021, 2022b). En er is een versterkte re-migratie naar China zichtbaar van onderzoekers uit de VS. (Xie *e.a.*, 2022).
69 (AWTI, 2017b; Fägersten, 2022; Hudson *e.a.*, 2022)
70 (Baker, 2022)

Dergelijke tweede-orde effecten van het beleid zijn van significante betekenis en moeten meegewogen worden voorafgaand aan en bij evaluatie van het beleid.

De juiste balans in de aanpak hangt af van de context waarin kennisontwikkeling plaatsvindt. Iedereen begrijpt dat bij defensieonderzoek striktere voorwaarden gelden dan gemiddeld. Ook biomedische onderzoeksgebieden kennen relatief veel veiligheidsmaatregelen. In toenemende mate zien we die maatregelen ook bij technologisch onderzoek zoals kwantumcomputers en encryptietechnologie. Maar de context kent meer aspecten dan de sector waarin de kennis landt.[71] Denk daarbij aan het kennisveld of de discipline, het type onderzoeksorganisatie, het type data waarmee gewerkt wordt, de technologie die gebruikt wordt, de 'toepassingsgereedheid' van de kennis, de aard van de samenwerkingspartners, het land waarmee wordt samengewerkt en het type financiering.[72] Bovendien vinden onderzoeksprojecten en -programma's niet in isolatie plaats. Ze zijn doorgaans onderdeel van een breder, vaak internationaal systeem van actoren (bijvoorbeeld onderzoekers, bedrijven, maatschappelijke partijen) en instituties (wet en regelgeving).[73] Ingrijpen in dit systeem heeft directe en indirecte effecten. Daarom is een gedifferentieerde aanpak, waarin rekening wordt gehouden met de context van het onderzoek, van groot belang.[74]

Signalen dat de nuance onder druk staat

In de beleidsontwikkelingen, de maatregelen en het discours rondom kennisveiligheid is nuance dus van belang. We constateren echter dat de nuance op dit moment onder druk staat, op basis van vier observaties.

Allereerst blijkt uit onze gesprekken en openbare bronnen[75] dat er een zeker wantrouwen heerst tussen verschillende actoren. We zien niet alleen een verhit debat in Nederland[76], maar ook internationaal.[77] Dit leidt tot extreme posities en voorstellen voor vergaande, ongenuanceerde maatregelen, met ongewenste effecten. Zo zijn er in de VS voorbeelden bekend van onderzoekers die – naar het bleek ten onrechte – zijn vervolgd vanwege

71 Let wel, de uiteindelijke toepassing van kennis is vaak onbekend en onzeker op het moment waarop die kennis ontwikkeld wordt, laat staan wanneer de onderzoeksvoorstellen worden geschreven (zie Van der Meulen in (Graaf, de, Rinnooy Kan en Molenaar, 2017)). Bovendien zijn er signalen dat de scheidslijn tussen militaire- en civiele toepassing steeds vager wordt (Diercks, Deuten en Diederen, 2019).
72 (Wellerstein, 2021).
73 Zie ook (Fransman *e.a.*, 2021).
74 (Committee on Protecting Critical Technologies for National Security in an Era of Openness and Competition *e.a.*, 2022)
75 Zie ook (Snetselaar, 2022)
76 Zie bijvoorbeeld (ScienceGuide, 2022a, 2022b)
77 Zie bijvoorbeeld (Baker, 2022) en (Foy, 2022)

vermeende onwenselijke banden met China.[78] Dit heeft een negatieve uitwerking op de sociale veiligheid van onderzoekers en draagt bij aan de remigratie van onderzoekers.

Ten tweede ontstaat er een reflex bij sommige betrokkenen om zo veel mogelijk van de risico's te voorkomen. Zo wordt nu gewerkt aan een aantal instrumenten dat probeert grip te krijgen op eerder beschreven risico's. Het belangrijkste instrument is het aangekondigde toetsingskader, dat naar verwachting een aantal sensitieve kennisgebieden bevat waartoe individuen uit bepaalde landen geen toegang krijgen.[79] Er is dan vooraf toestemming nodig vanuit de overheid als mensen uit specifieke landen aan het werk willen gaan in bepaalde kennisgebieden of met bepaalde technologieën. Een ander instrument is het 'besluit toepassingsbereik sensitieve technologie' voor de 'Wet vifo',[80] waarin aan de hand van lijsten van technologieën wordt bepaald wat niet-sensitief, sensitief of zeer sensitief is.[81] Investeringen in bedrijven die sensitieve technologie bezitten, moeten eerst worden goedgekeurd door het ministerie. Dit soort lijsten zijn verleidelijk en bieden ogenschijnlijk duidelijkheid, maar kennen een aantal tweede-orde problemen. Ze lopen allereerst per definitie achter op wetenschappelijke en technologische ontwikkelingen. Daardoor ontstaat de verleiding om ze 'ruim' op te stellen, zodat toekomstige ontwikkelingen ook binnen de categorieën passen.[82] Daarmee wordt onderzoek mogelijk onnodig ingeperkt. Een tweede probleem is dat dergelijke lijsten kunnen leiden tot een soort 'afvinkcultuur' (zie ook het kader hieronder): in plaats van het erkennen van de complexiteit wordt de situatie versimpeld tot landen en kenniscategorieën.[83] Dit kan leiden tot schijnveiligheid, omdat er risico's kunnen ontstaan buiten de categorieën of door strategisch gedrag om risicovolle samenwerking zó te beschrijven dat het buiten de categorieën valt. Ten derde kunnen dergelijke lijsten ertoe leiden dat de discussie over waarden niet gevoerd wordt. De multidimensionale afweging van academische, economische en veiligheidswaarden verarmt dan tot een binaire lijst van wat wel en wat niet mag. Een vierde en laatste probleem bij deze beleidsrespons is dat het beveiligen van onderzoek en onderwijs los kan komen te staan van het stimuleren

78 (Fischer, 2021)
79 Het toetsingskader, aangekondigd in de eerste brief kennisveiligheid (Minister van OCW, Minister van J&V, en Staatssecretaris van EZK, 2020) is nog in ontwikkeling. Dus hoe het er precies uit gaat zien, is nog onduidelijk. We baseren ons op de informatie uit de kamerbrief (Minister van OCW, 2022b) en gesprekken. Overigens werd in eerste instantie ook op een toetsing van samenwerkingen en financiële stromen aangestuurd. In recentere berichtgeving wordt alleen het toetsingskader op individuen genoemd.
80 (Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, 2022a)
81 Er komt ook kritiek op de effectiviteit van deze beperkende lijsten (Van den Broek, 2022).
82 Ook op de nieuwe spionagewetgeving is kritiek, met name omdat deze algemeen en onduidelijk is. Onder andere van de Raad van State (Geurts, 2022), juristen en een oud-veiligheidsexpert (Versteegh, 2022).
83 (Shih, 2022)

en versterken van onderzoek.[84] Dit leidt tot aparte, inconsistente beleidssporen die verschillende hoofddoelen nastreven, maar op dezelfde organisaties zijn gericht. En dat verhevigt de dilemma's die in Hoofdstuk 1 werden benoemd.

Voorbeeld accountancy

Een aantal jaar geleden raakte de accountancysector in opspraak, omdat er sprake was van fraude- en corruptieschandalen. Naar aanleiding daarvan zijn er verschillende commissies en werkgroepen opgezet, die rapporten hebben gepubliceerd over de aanpak van de problemen in de sector. Waar verandering eerst uit de sector zelf moest komen, constateerde de Monitoring Commissie Accountancy (MCA) in 2020 dat dezelfde problemen steeds terugkeerden en van verbetering nog geen sprake was. Daarom kwam zij met een nieuw pakket van dertig maatregelen, bovenop de drieënvijftig maatregelen die de vorige commissie voorstelde. En uiteindelijk volgde vanuit het ministerie van Financiën de 'Wet toekomst accountancysector'.[85]

Bij de bekendmaking van de verschillende maatregelen en het wetsvoorstel werd al gewaarschuwd dat te veel regelgeving ter controle zou leiden tot een 'afvinkcultuur'. Een van de voorstellen was om accountants te laten rapporteren over hun werkzaamheden. Maar over de effectiviteit daarvan valt volgens critici te twisten; het zou niets meer zijn dan het aanpakken van de symptomen, in plaats van het aanpakken van het onderliggende probleem.[86] Een overvloed aan regels (*compliance*) werkt bovendien verlammend voor het eigen kritische inzicht van het individu, aldus een hoogleraar 'audit en assurance' in het Financieele Dagblad.[87] Ook creëert een dergelijke afvinkcultuur een papieren werkelijkheid die als excuus dient indien het fout gaat.[88] Momenteel kampt de sector met een groot tekort aan accountants.[89] Het werken in de accountancy is, om verschillende redenen, duidelijk onvoldoende aantrekkelijk voor voldoende instroom van jonge mensen. Vermoed wordt dat de regelgeving hier mede een rol in speelt.

Naast het wantrouwen tussen verschillende actoren en de reflex om risico's te voorkomen, valt ten derde de roep om 'duidelijkheid' op. In onze gesprekken noemen

84 (d'Hooghe en Lammertink, 2022, p. 49)
85 (Monitoring Commissie Accountancy, 2020; Pols, 2020)
86 (Pheijffer, 2021)
87 (Baurichter en Pols, 2020)
88 (Pols, 2022)
89 (Bruins, 2022)

verschillende stakeholders het zogenaamde ‘grijze gebied’ waarin het onduidelijk is of en hoe er moet worden samengewerkt. Dat grijze gebied komt voort uit conflicterende verwachtingen en signalen die kennisinstellingen en onderzoekers ontvangen ten aanzien van internationale samenwerking. Voor kennisinstellingen is het verleidelijk om meer duidelijkheid te vragen, primair van de overheid. Dan wordt al snel gedacht aan relatief simpele beslisregels over wat wel en niet mag. Deze ‘utopie van duidelijkheid’ komt in verschillende gesprekken terug en onderschat de problematiek.[90] Dit is een utopie, omdat het onwaarschijnlijk is dat de overheid vanuit een centrale positie die duidelijkheid kan creëren. Als gevolg van de eerder geschetste complexiteit hangt de beslissing over internationale samenwerking namelijk van zo veel factoren af, dat deze niet op basis van enkelvoudige beslisregels is te nemen. Als de overheid gehoor geeft aan de oproep tot duidelijkheid zijn er grofweg twee opties. Ofwel de overheid ontwikkelt dusdanig beperkende regels, dat veel van de opbrengsten uit internationale samenwerking en daarmee de kwaliteit van kennisontwikkeling onder druk komen te staan. Of de overheid ontwikkelt aanmerkelijk lossere regels, die weinig bijdragen aan kennisveiligheid. Duidelijkheid vervalt daardoor al gauw in schijnduidelijkheid. Deze twee kanten van de medaille schetsen ten volle het dilemma en het belang van het zoeken naar de balans.

Tot slot zijn er de afgelopen tijd duidelijk politieke ingrepen gezien in de beoefening van wetenschap. Het gaat dan vooral om de oproep om na de inval door Rusland in Oekraïne alle banden met Russische en Wit-Russische wetenschappers stop te zetten.[91] Dit soort restrictieve, top-down ingrepen zetten andere waarden, zoals institutionele autonomie onder druk.

2.3 Bewustwording en handelingsperspectieven nog onvoldoende

De bewustwording onder onderzoekers en bestuurders en de beschikbare *tools* zijn in ontwikkeling, maar nog niet voldoende. Door de geopolitieke, economische en technologische ontwikkelingen in de wereld worden kennisinstellingen steeds meer geconfronteerd met uitdagingen op het gebied van kennisveiligheid. Kennis en vaardigheden moeten daarom worden doorontwikkeld.

---

90 Zie ook dit citaat van een vertegenwoordiger van de Nederlandse universiteiten uit 2021: “There is, of course, a call from politics for a clear and unambiguous answer, [but] there just isn’t one. Moreover, politics always lags behind new developments, which is logical because it needs to follow a certain trajectory. Universities, by definition, want to respond to new developments. [Thus], what is needed is a very differentiated answer, one in which there is room for universities to act.” (Snetselaar, 2022)

91 (Fischer, 2022a)

Sinds de ontwikkeling en implementatie van de nationale leidraad kennisveiligheid in januari 2022 is er aanzienlijk meer aandacht voor het onderwerp kennisveiligheid aan kennisinstellingen.[92] Mede dankzij aansporing vanuit de overheid zijn er verantwoordelijken aangewezen bij kennisinstellingen en wordt kritisch gekeken naar bestaande samenwerkingsverbanden en partnerschappen.[93] Dit heeft binnen de kennisinstellingen een ontwikkeling op gang gebracht met als gevolg een toename van bewustzijn en de ontwikkeling van *tools*.[94] Ook tussen de kennisinstellingen worden in toenemende mate kennis, inzichten en praktische handvatten uitgewisseld.[95]

Bewustwording en vaardigheden moeten beter

Toch constateren we, op basis van eigen observaties en gesprekken met betrokkenen, dat de bewustwording van risico's op veel plekken nog onvoldoende is en dat vaardigheden nog onderontwikkeld zijn. Steeds meer onderzoek wordt als *dual use* aangemerkt[96] en statelijke actoren mengen zich in toenemende mate in onderzoek of beïnvloeden dit heimelijk.[97] Daarom nemen de noodzaak en het belang van kennisveiligheid toe. Bestuurders, beleidsmakers, onderzoekers en ondersteunend personeel moeten zich ten volle bewust zijn van dit belang, in staat zijn risico's en dreigingen te herkennen en weten hoe ze moeten handelen. De zoektocht naar nuance en balans, waarvoor in de vorige paragraaf werd gepleit, is geen argument om maar niets te doen. Er moeten harde keuzes (kunnen) worden gemaakt om bepaalde vormen van samenwerking of uitwisseling niet aan te gaan, als de afweging van verschillende waarden negatief uitpakt.

We constateren grote verschillen tussen en binnen kennisinstellingen. Terwijl in specifieke vakgebieden en bij bepaalde kennisinstellingen de bewustwording en vaardigheden rondom kennisveiligheid goed ontwikkeld zijn (zie ook de kaders hieronder), zijn er ook nog plekken waar dit ontbreekt. Dat komt omdat kennisveiligheid in veel opzichten niet goed past bij de cultuur en werkwijze van de meeste kennisinstellingen. Het lijkt erop dat niet iedereen voldoende is doordrongen van de veranderende context waarin internationale samenwerking plaatsvindt en de toenemende complexiteit die deze met zich meebrengt. Wie goed voorbereid wil zijn, moet anticiperen

92 (Snetselaar, 2022)
93 De uitgevraagde risicoanalyse door het ministerie en de aangekondigde audit daarop hebben hier sterk aan bijgedragen (Minister van OCW, 2022b).
94 Een voorbeeld zijn de 'Partnering tools' bij de TU Delft (De Bruijn, 2021).
95 Een groep van Europese universiteiten, waaronder de Universiteit Leiden, bracht onlangs een handboek uit om partnerschappen tussen universiteiten te evalueren (The University of Copenhagen *e.a.*, 2022)
96 (Diercks, Deuten en Diederen, 2019; Evans, 2022)
97 (AIVD, MIVD, en NCTV, 2021)

op toekomstige veranderingen in de wereld. Het denken en doen rondom kennisveiligheid is echter nog tamelijk ‘onvolwassen’.

Inspiratie uit de ervaring met maatregelen bij het NLR

Bij het Koninklijk Nederlands Lucht- en Ruimtevaartcentrum (NLR) wordt hoogwaardige technologische kennis geïdentificeerd, ontwikkeld en voor toepassing gereed gemaakt. NLR opereert als Groot Technologisch Instituut (GTI) in de TO2-federatie en vervult hierbij een spilfunctie tussen wetenschap, bedrijfsleven en overheid. Zodoende werkt NLR regelmatig in opdracht van bedrijven (zoals Airbus en velen anderen), Defensie of het ministerie van Infrastructuur en Waterstaat. Deze opdrachtgevers hebben een verschillende kijk op disseminatie en openheid. Met name bepaalde projecten voor Defensie brengen grote risico’s voor de nationale veiligheid met zich mee als informatie op de verkeerde plek terechtkomt; NLR is erop ingericht om deze risico’s afdoende te beheersen. Dat maakt NLR een interessante casus om te bestuderen.

Om ongewenste kennisoverdracht tegen te gaan, neemt NLR zichtbare en onzichtbare maatregelen. Voor projecten met commerciële belangen wordt bijna altijd met *non-disclosure agreements* (NDA) gewerkt. Een NDA is eenzijdig of tweezijdig en wordt opgesteld op initiatief van NLR of van een klant of stakeholder. Projecten die in samenwerking met Defensie worden uitgevoerd kennen vaak een rubricering (nationaal of NATO), waardoor voorschriften van kracht zijn op basis van die rubricering. In de praktijk is de rubricering vaak Departementaal Vertrouwelijk, maar er worden ook projecten uitgevoerd die strikter vertrouwelijk zijn dan dat.

Bij NLR kunnen ongeveer 350 tot 400 medewerkers aan defensiewerk werken, waarvan een significant deel regelmatig met informatie werkt die gerubriceerd is. Alle medewerkers van NLR die bij defensiewerk betrokken zijn, moeten daarom een Verklaring van Geen Bezwaar (VGB) hebben. Het VGB is een veiligheidsonderzoek, ofwel screening, dat wordt uitgevoerd door de nationale veiligheidsdiensten en is daarmee aanzienlijk diepgaander dan een Verklaring Omtrent Gedrag (VOG). In 2021 werden er door de Unit Veiligheidsonderzoeken (UVO) en gemandateerde partijen 51.354 VGB onderzoeken uitgevoerd waarvan er 388 geweigerd werden.[98] Personen met een buitenlandse nationaliteit kunnen bijna nooit zo’n VGB krijgen, waardoor bij NLR feitelijk al een gedwongen selectie aan de poort plaatsvindt.

98 (AIVD, 2022)

De VGB voor medewerkers op onderzoeksposities is onderdeel van de voorschriften van de Algemene Beveiligingseisen Defensieopdrachten (ABDO)[99], die voor NLR van toepassing zijn. Dit betekent dat er fysieke bescherming is aan het pand (bijvoorbeeld voldoende afstand tussen het gebouw en de omheining, beveiliging van het gebouw en voor bezoekers geldt een identificatieplicht) en stelt eisen aan de digitale omgeving (bijvoorbeeld virusscanners, spamfilters en ICT-omgeving geheel in eigen beheer). Ook is NLR ISO 27001 gecertificeerd.[100] De betrouwbaarheid van het netwerk (cybersecurity) wordt continu gemonitord en extern bewaakt via een zogeheten Bitsight-score. Ook moeten medewerkers hun wachtwoorden elke drie maanden wijzigen. Deze maatregelen zorgen ervoor dat technologische kennis van NLR zo min mogelijk wordt gedeeld (*need-to-know*), waardoor het risico op onwenselijke kennisoverdracht wordt verkleind.

Er worden bij NLR geen specifieke maatregelen genomen om heimelijke beïnvloeding te voorkomen. Ook zijn er geen speciale maatregelen tegen onethische praktijken tijdens het samenwerkingsonderzoek (anders dan de gedragscode wetenschappelijke integriteit) of bij het gebruik van onderzoeksuitkomsten. Bij NLR is de overheid leidend, wat wil zeggen dat de organisatie aansluit bij het overheidsbeleid als het gaat om ethische kwesties rondom technologische ontwikkelingen. Ethiek is bij medewerkers steeds vaker onderwerp van gesprek, bijvoorbeeld als het gaat om onderzoekssamenwerking met landen die een twijfelachtige mensenrechtensituatie kennen. Daarnaast geldt voor de (medewerkers van) NLR de Nederlandse gedragscode wetenschappelijke integriteit. De gedragscode is bij invoering formeel bekend gemaakt, maar er is niet gemeten hoeveel medewerkers van NLR zich actief bewust zijn van deze code.[101]

Handelingsopties ontbreken

In de maatregelen die momenteel worden getroffen is vooral aandacht voor preventie: het identificeren en vooraf mitigeren van de risico's. Veel vragen die binnenkomen bij het kennisveiligheidsloket hebben daar betrekking op. Een volgende stap is om mensen handelingsbekwaam te maken bij internationale samenwerking die niet risicoloos, maar wel wenselijk is. Vervolgens moeten betrokkenen bij risicovolle trajecten in staat zijn om een samenwerking ordentelijk te kunnen afbreken. Dit is vergelijkbaar met de aanpak van

99 (Ministerie van Defensie, 2019)
100 https://www.iso.org/isoiec-27001-information-security.html
101 (KNAW *e.a.*, 2018)

cybersecurity, waarbij eerst werd ingezet op een groeiend bewustzijn en vervolgens werd nagedacht over detecteren van en interveniëren op incidenten.

Op dit moment is er naar verhouding minder aandacht voor de vaardigheden die nodig zijn bij het detecteren van en interveniëren op relaties of projecten die mogelijk problematisch worden. Wat doet een onderzoeker bijvoorbeeld als hij of zij vermoedt dat een collega in Nederland of in het buitenland niet in vrijheid onderzoek kan doen of onder druk gezet wordt? Welke financiële en relationele gevolgen heeft het stopzetten van contracten of samenwerkingsprojecten? In Australië bijvoorbeeld worden deze vragen serieus genomen. Universiteiten worden aangemoedigd om trainingen voor het versterken van wetenschappelijke integriteit, en het herkennen en registreren van buitenlandse inmenging te organiseren voor onderzoekers.[102]

Naast het verbeteren van de bewustwording, vaardigheden en handelingsperspectieven moet er meer aandacht komen voor het identificeren en pakken van (veilige) kansen.[103] De vraag is dan welk type samenwerking zonder noemenswaardige risico's kan worden aangegaan.

Inspiratie uit ervaring met maatregelen en vaardigheden bij ARCNL

The Advanced Research Center for Nanolithography (ARCNL) is een publiek-private instelling die in 2014 door NWO, de Universiteit van Amsterdam en de Vrije Universiteit, en ASML (producent van apparatuur voor het produceren van halfgeleiders) is opgezet. Sinds 2022 is ook de Rijksuniversiteit Groningen aangesloten. ARCNL is ontstaan vanuit een aanbesteding die ASML in 2013 heeft uitgezet, vanwege de wens om een nieuw onderzoeksinstituut op te zetten dat het bedrijf met fundamentele kennis kan voeden. ARCNL heeft deze aanbesteding gewonnen. Het is sinds 2015 een onafhankelijk onderzoeksinstituut en onderdeel van het NWO-institutenportfolio. ARCNL richt zich op de wetenschapsgebieden van de fundamentele natuurkunde en scheikunde, in de context van technologieën voor (nano)lithografie, voornamelijk voor de halfgeleiderindustrie.

ARCNL bevindt zich als instelling op het snijvlak van het academische en het industriële veld. Wetenschappelijke artikelen worden gepubliceerd en *peer-reviewed,* groepsleiders geven college aan universiteiten en het instituut levert wetenschappelijke bijdragen op internationale conferenties. De onderzoeksvragen

102 (d'Hooghe en Lammertink, 2022, p. 49)
103 (d'Hooghe *e.a.*, 2018)

worden voornamelijk gedreven door toepassing bij de industriële partner ASML, die profiteert van de stroom aan ideeën uit het onderzoek.

Vanwege ARCNL's unieke (kennis)positie, acteert de instelling als een spin in het web dat breder is dan (nano)lithografie. ARCNL werkt met veel partners samen uit diverse gebieden. Ook de onderzoekers van ARCNL komen van over de hele wereld. De sensitieve kennis en technologie waar ARCNL onderzoek naar doet, maakt dat kennisveiligheid bij ARCNL veel aandacht krijgt.

ARCNL gaat op verschillende manieren met potentiële risico's om. Nieuw personeel wordt 'aan de voordeur' gescreend. Er wordt een risico-inschatting gemaakt op basis van verschillende signalen of triggers. Niet alleen wordt bepaald of iemand wordt aangenomen, maar ook tot welke delen van het onderzoek en tot welke bijeenkomsten hij of zij toegang krijgt. Dit wordt vooraf met de nieuwe collega besproken.

ARCNL hanteert dezelfde aanpak als het gaat om de bescherming van kennis en technologie. Voordat onderzoeksresultaten gepubliceerd worden, worden deze gescreend door een raad met experts uit verschillende vakgebieden. Er wordt gekeken of de resultaten mogelijk tot commercieel-relevante toepassingen zouden kunnen leiden en zo ja, dan wordt eerst een patent aangevraagd.

Daarnaast is er sprake van databescherming. Data is gecompartimenteerd en per onderzoeksgroep afgeschermd. Ook zijn de toegangsrechten tot de data beperkt. Tot slot wordt het gebouw zelf beschermd: niet alle doorgangen zijn vrij toegankelijk en alle kantoren kunnen op slot. De werknemers zijn zich bewust van het feit dat niet iedereen overal toegang toe heeft en zijn alert op opvallende situaties.

3

Drie aanbevelingen voor een lerende aanpak rond kennisveiligheid

De AWTI heeft drie aanbevelingen om de aanpak rondom kennisveiligheid te verbeteren. Deze aanbevelingen geven een gelaagde en praktische invulling aan het advies om te werken aan een lerende aanpak voor kennisveiligheid, met blijvende aandacht voor nuance en meer bewustwording. Ze zijn gericht op de conceptualisatie, differentiatie en realisatie van de aanpak van kennisveiligheid.

Met een lerende aanpak rondom kennisveiligheid kunnen Nederlandse kennisinstellingen nu en in de toekomst beter omgaan met de complexe uitdagingen van internationale samenwerking bij kennisontwikkeling en in hoger onderwijs. Lerend, omdat het een illusie is te denken dat het beleid in Nederland in één keer goed is. De omstandigheden veranderen immers continu. Dat is niet erg, mits de aanpak zó is ontworpen dat het lessen over wat wel en niet goed werkt, kan incorporeren. Zo'n aanpak biedt een antwoord op de toenemende complexiteit, zonder onnodig afbreuk te doen aan de waarde van internationale samenwerking. Per definitie vraagt deze aanpak blijvend aandacht.

Het bevorderen van kennisveiligheid is volgens de AWTI vooral een verantwoordelijkheid van de overheid, in samenspel met kennisinstellingen. Bij de overheid komen de verschillende nationale belangen en perspectieven rondom kennisveiligheid en gerelateerde thema's bijeen, en worden ze afgewogen. Dit advies richt zich dan ook primair op de overheid. Maar het advies spreekt ook de kennisinstellingen aan, want juist daar zal een leerproces rondom kennisveiligheid moeten plaatsvinden. Het is van groot belang dat expertise en maatregelen worden ontwikkeld in de context van onderzoek en de onderzoekers. Dit moet gebeuren in de nabijheid van de onderzoekers omdat voor het bespreken van dit onderwerp vertrouwen nodig is en kennis van de onderzoekspraktijk. Dit vraagt om leiderschap op dit onderwerp vanuit de sector zelf. Immers, wanneer de aanpak bottom-up onvoldoende voortgang maakt, leidt dit uiteindelijk tot een minder genuanceerde, meer restrictieve top-down reactie vanuit de overheid.

Bij de ontwikkeling van de aanbevelingen is gebruik gemaakt van de resultaten van de LAC-studie naar de aanpak rondom kennisveiligheid in andere landen.[104] De hoofdconclusie van die studie is dat een effectieve aanpak is gebaat bij een coherente en pragmatische set aan maatregelen, goede coördinatie tussen betrokkenen, en

104 (d'Hooghe en Lammertink, 2022)

overheidssteun voor bottom-up activiteiten van kennisinstellingen. Deze lessen komen terug in onze aanbevelingen.

De drie parallelle aanbevelingen hebben betrekking op verschillende ‘niveaus’ waarop ontwikkelingen nodig zijn, waardoor een gelaagde invulling van het advies ontstaat. Aanbeveling 1 draagt bij aan een beter begrip van kennisveiligheid, in relatie tot andere belangrijke thema’s en ontwikkelingen in het buitenland. Deze aanbeveling is primair gericht aan de overheid, in samenspel met de kennisinstellingen, maar moet leiden tot een brede, publieke discussie ter conceptualisatie van kennisveiligheid onder overheden, kennisinstellingen, veiligheidsdiensten, buitenlandse posten en denktanks.

Aanbeveling 2 draagt bij aan het ontwikkelen van een professionele, gedifferentieerde aanpak voor Nederland. Ook hier moet de overheid het voortouw nemen, maar dienen kennisinstellingen, veiligheidsdiensten en andere experts (bijvoorbeeld op het gebied van integrale veiligheid) aan te sluiten en mee te denken. De aanpak specificeert en operationaliseert het begrip kennisveiligheid en definieert maatregelen. Dit is in lijn met de noodzaak van een coherente set aan maatregelen en coördinatie tussen betrokkenen.

Aanbeveling 3 is gericht aan kennisinstellingen en stuurt aan op de noodzakelijke veranderingen in het denken en doen van onderzoekers, bestuurders, ondersteuners, beleidsmedewerkers en leidinggevenden. Dit sluit aan bij de noodzaak van een pragmatische set aan maatregelen. De overheid heeft hier een ondersteunende rol, wat past bij de observatie uit de LAC-studie dat het ondersteunen door de overheid van bottom-up initiatieven uit de sector bijdraagt aan effectief beleid.

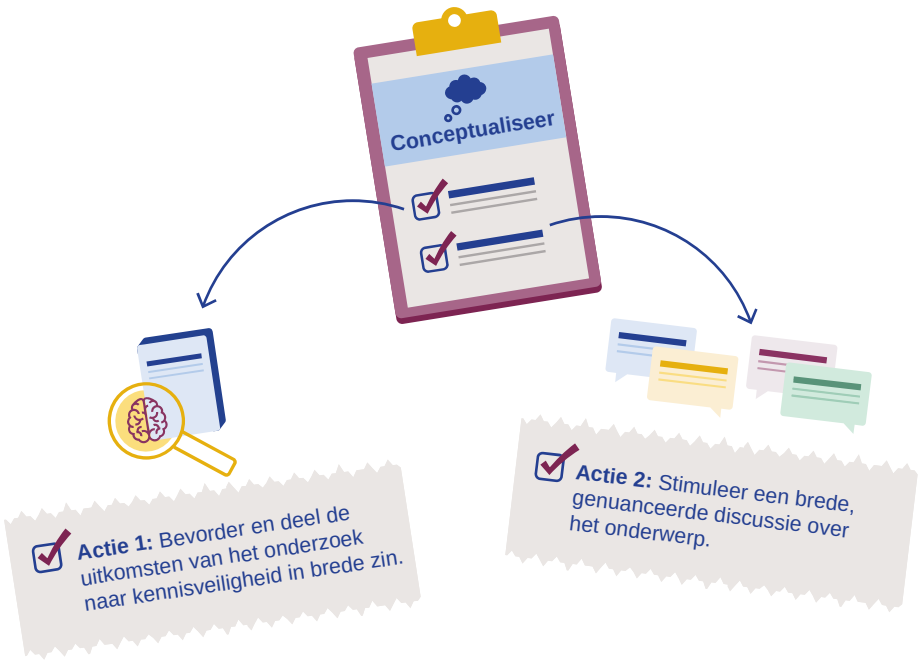
De aanbevelingen om tot een lerende aanpak te komen zijn dus gelaagd en grijpen bovendien op elkaar in. Toch dienen ze nadrukkelijk gelijktijdig, interactief en niet volgtijdelijk te worden opgepakt om tot maximale leeropbrengsten te leiden.

Advies. Gelijktijdig uitvoeren van de drie aanbevelingen door de overheid en de kennisinstellingen leiden gezamenlijk tot een lerende aanpak.

Aanbeveling 1. Conceptualiseer: verbeter het begrip van kennisveiligheid

Het denken en doen rondom kennisveiligheid staat nog in de kinderschoenen en is daarom vatbaar voor eenzijdige bekritisering vanuit specifieke perspectieven (zie pararagraaf 2.1). De overheid heeft, in samenspel met de kennisinstellingen, daarom een leidende taak in het verder ontwikkelen van het begrip kennisveiligheid in al z'n facetten en in het balanceren van verschillende waarden en belangen. De discussie over thema's en waarden is nooit af, maar moet wel gevoerd worden. Conceptualisering is cruciaal voor de aanpak van kennisveiligheid en is de basis voor bewustwording, het herkennen en mitigeren van risico's, en het identificeren van kansen voor samenwerking.

Aanbeveling 1. Conceptualiseer: verbeter het begrip van kennisveiligheid.



Om te zorgen voor een breed gedragen en goed begrip van wat kennisveiligheid is, zijn twee concrete acties van de overheid vereist:

Actie 1. Bevorder en deel de uitkomsten van het onderzoek naar kennisveiligheid in brede zin

Het onderzoek naar kennisveiligheid in Nederland en daarbuiten komt langzamerhand op gang.[105] Het verrijkt en onderbouwt begripsvorming van kennisveiligheid en laat zien hoe het onderwerp zich verhoudt tot andere thema's als *open science*, internationalisering, strategische autonomie[106] en wetenschappelijke integriteit. Op dit moment zijn de relaties en wederzijdse afhankelijkheden tussen deze concepten nog onvoldoende helder. Zo laat de internationale LAC-studie zien dat in het buitenland verschillend wordt gedacht over het conceptuele fundament van een kennisveiligheidsaanpak: het ene land vertrekt vanuit een veiligheidsperspectief en het andere vanuit een perspectief van wetenschappelijke integriteit.[107] Bovendien zijn de intuïtieve verschillen tussen vakgebieden in termen van risico's (e.g. drone-technologie versus onderzoek naar mensenrechten) nauwelijks in kaart gebracht als het om kennisveiligheid gaat. Het is raadzaam om vernieuwend conceptueel en empirisch onderzoek naar kennisveiligheid te intensiveren, gegeven het uitdagende en dynamische karakter van het onderwerp.[108] Ook evaluatieonderzoek naar kennisveiligheidsbeleid en -maatregelen is hard nodig. Effectief bevonden maatregelen en praktijken kunnen vervolgens worden meegenomen in de professionalisering van de aanpak bij kennisinstellingen en overheden (zie aanbeveling 2).

Actie 2. Stimuleer een brede, genuanceerde discussie over het onderwerp

Kennisveiligheidsbeleid is niet alleen een intellectueel vraagstuk, maar kent nadrukkelijk ook een normatieve afweging. Om die afweging te kunnen maken, is het nodig dat verschillende waarden worden samengebracht. We zien in de media en de politiek een verhitte discussie, maar ook tekenen van een genuanceerd gesprek. Ook in het buitenland wordt gewaarschuwd tegen het op de spits drijven van de discussie, vooral om te voorkomen dat onderzoekers afhaken. In Frankrijk heeft een parlementair rapport over wetenschappelijk patrimonium en academische vrijheid een belangrijke rol gespeeld in het stimuleren van het publieke debat (zie het kader hierna).[109] Er zijn er ook die juist pleiten voor een duidelijkere formulering van de risico's om het bewustzijn te vergroten.[110] De AWTI pleit voor een genuanceerde discussie omdat dit past bij de ontwikkelingsfase van het beleid.

---

105 (van der Wende en Kirby, 2020; d'Hooghe, 2021; Wellerstein, 2021; Clark, 2022; De Bruijn *e.a.*, 2022; OECD, 2022; Shih, 2022; Snetselaar, 2022)
106 Een begrip als strategische autonomie is overigens ook nog onder-gedefinieerd
107 (d'Hooghe en Lammertink, 2022, p. 51).
108 Dit onderwerp leent zich bij uitstek voor interdisciplinair onderzoek (AWTI, 2022). Denk bijvoorbeeld aan onderzoek naar onderzoekspraktijken, onderzoek naar publicatie patronen, veiligheidsonderzoek naar risico's en dreigingen. Zie ook (Hudson *e.a.*, 2022, p. 3).
109 (d'Hooghe en Lammertink, 2022, p. 21)
110 (d'Hooghe en Lammertink, 2022, p. 48).

Rapport Franse senaat: 'Beter beschermen van wetenschappelijk patrimonium en academische vrijheid'

Het rapport 'Beter beschermen van wetenschappelijk patrimonium en academische vrijheid'[111] van André Gattolin is het resultaat van een initiatief uit 2021 van de *Rassemblement des démocrates, progressistes et indépendants* (RDPI). Het rapport beschrijft non-Europese staatsinvloeden en hun impact op de Franse kennisinstellingen, en vraagt aandacht voor de realiteit van deze dreiging. Met het rapport willen de auteurs instellingen voorbereiden op wat een van de grootste uitdagingen van de 21e eeuw wordt genoemd: het behouden en beschermen van de Franse wetenschappelijke erfenis of eigendommen, academische vrijheden en wetenschappelijke integriteit. Het rapport geeft een beschrijving van de dreiging en zwaktes in het Franse systeem, een toetsingskader van invloeden, de impact van buitenlandse mogendheden op de universitaire sector en het gerelateerde overheidsbeleid.

Het rapport laat zien dat elke genomen maatregel ter bescherming van de Franse academische sector een complexe afweging is. Zo is er enerzijds een academische traditie waarin kennis en ideeën vrij circuleren, en zijn er anderzijds de nieuwe strategieën, ontworpen voor de lange termijn en uitgevoerd met aanzienlijke middelen door regeringen die soms als 'vijandig' beschouwd kunnen worden. Het rapport pleit voor differentiatie: de reactie op buitenlandse inmenging moet 'multivariabel' en schaalbaar zijn, gezien het feit dat strategieën van buitenlandse actoren veranderlijk zijn en juist gericht zijn op het uitbuiten van zwakke plekken. Het rapport benoemt vijf doelen en met daaronder 26 concrete(re) voorstellen. De doelen zijn:

- het probleem van buitenlandse inmenging een politieke prioriteit maken;
- het beschermen van academische vrijheid waarbij academische autonomie wordt gerespecteerd;
- transparantie en wederkerigheid in internationale wetenschappelijke samenwerking van nationaal belang maken;
- het versterken van de administratieve procedures die de partnerschappen met instellingen voor hoger onderwijs en onderzoek controleren;
- het promoten van een referentiedocument van normen en richtlijnen, nationaal, internationaal en in Europa.

Dit rapport, met zijn concrete voorstellen, heeft een belangrijke rol gespeeld in het stimuleren van het publieke debat.[112]

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

De voorgestelde acties onder deze eerste aanbeveling hebben een internationale dimensie, want ook in Europa zijn de begrippen rondom kennisveiligheid nog onvoldoende geconceptualiseerd. Er ontstaan in toenemende mate spanningen tussen enerzijds het stimuleren van mondiale samenwerking rond onderzoek en innovatie, waarin de aansluiting met andere landen wordt gezocht[113] en anderzijds de activiteiten ten behoeve van open strategische autonomie[114], waarin eenzijdige of onwenselijke afhankelijkheden worden geminimaliseerd. Daarbij is het begrip (open) strategische autonomie nog ondergedefinieerd: men is het nog niet eens over wat dat precies betekent.

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

Er is in Nederland behoefte aan een aanpak van kennisveiligheid die zowel verduidelijkt als differentieert. De duidelijkheid in de sector is nodig zodat onderzoekers weten wat wel en niet kan. De differentiatie betekent dat mitigerende maatregelen proportioneel worden ingezet, waarbij kansen en risico's afhangen van het type onderzoek, gebruikte data, sociale context en samenwerkingspartners, en ingrijpen op bewust en onbewust gedrag (zie paragraaf 2.2). Top-down, binaire, bindende regels bieden in de regel onvoldoende ruimte voor deze differentiatie en mogelijkheid tot nuance. Daarom is een aanpak nodig die een brede set aan kennis incorporeert, afwegingen van verschillende nationale belangen internaliseert en praktische handvatten biedt voor kennisinstellingen om kennisveiligheid te professionaliseren. Onze tweede aanbeveling grijpt dan ook direct in op de conclusie van de LAC-achtergrondstudie die pleit voor een coherente en pragmatische set aan maatregelen. De organisatorische diversiteit van het landschap van kennisinstellingen zou beter gebruikt moeten worden voor deze differentiatie. Structurering van de kennis en kunde rondom kennisveiligheid, ten behoeve van de professionalisering van de aanpak, helpt om het hoofd koel te houden.

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

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

Om tot een gedifferentieerde aanpak te komen, zijn twee acties van de overheid nodig:

Actie 1. Ontwikkel een sectorbreed model ter professionalisering van de aanpak van kennisveiligheid

Een sectorbreed model onderscheidt verschillende domeinen van kennisveiligheid en definieert welk type maatregelen, afspraken en systemen passend zijn om de risico's in dat domein te mitigeren. Ons voorstel is geïnspireerd op de *capability maturity models*, die gebruikt worden voor cybersecurity (zie het kader hierna op pagina 47).
Domeindoelen bij kennisveiligheid zijn bijvoorbeeld: voorkomen van onwenselijke kennisoverdracht, samenwerken op basis van reciprociteit, tegengaan van zelfcensuur, of voorkomen van financiële afhankelijkheden. Deze zeer uiteenlopende aspecten van kennisveiligheid vragen om specifieke maatregelen. De verbetering van het begrip kennisveiligheid (aanbeveling 1) helpt bij het bepalen van dergelijke domeinen. Dit is geen eenmalige actie, maar vraagt om voortdurende aandacht en aanpassing.

Bij de ontwikkeling van een dergelijk model is betrokkenheid van verschillende stakeholders van belang. Dit zijn partijen binnen de kennissector maar ook daarbuiten, zoals de veiligheidsdiensten en het Ministerie van Buitenlandse Zaken. Zij bezitten cruciale kennis en expertise om het model effectief en legitiem te maken.[115] Openbare informatie (zoals het Dreigingsbeeld statelijke actoren) en niet-openbare informatie kunnen input zijn voor het model. Als zodanig verbindt en verenigt het model de beschikbare kennis en expertise rondom dit onderwerp en expliciteert het verantwoordelijkheden.

Het model kan worden gebruikt door verschillende functionele onderdelen binnen kennisinstellingen, zoals een afdeling of een onderzoeksgroep. Cruciaal daarbij is dat niet elk risico binnen de domeinen voor elk functioneel onderdeel in even grote mate aanwezig is. Dit hangt bijvoorbeeld af van het onderzoeksgebied, de toepassingsmogelijkheden van de kennis, de samenwerkingsverbanden van de onderzoeksgroep en de gebruikte data (zie de bespreking van differentiatie in paragraaf 2.2). Iedereen kan dus gebruik maken van hetzelfde model, maar vult het specifiek in voor de betreffende context. Het model impliceert een gelaagde aanpak (op onderzoeksgroepniveau, instellingsniveau, in samenspel met de relevante actoren buiten de instelling). Daardoor is het ook mogelijk te escaleren naar verschillende niveaus binnen en buiten de instellingen.

Het model definieert vervolgens verschillende niveaus die aangeven hoe sterk ontwikkeld de aanpak van een risico is. Daarbij geldt *less is more*: het streven is om met minimale ingrepen de risico's voldoende te mitigeren. Dus waar geen risico's zijn, worden geen maatregelen getroffen. Maar waar wel risico's zijn worden verschillende niveaus onderscheiden: de *maturity indicator levels*. De specifieke context van een afdeling of onderzoeksgroep bepaalt welk niveau nodig is. Het streven is dus om een situationele balans van risico's, kansen en maatregelen te bereiken.

Capability maturity model[116]

Een *capability maturity model* is een set van indicatoren die de bekwaamheid (*capability*) en volwassenheid (*maturity*) van een specifieke sector weergeeft. Het is een descriptief model, geen prescriptief model. Het wordt bijvoorbeeld gebruikt bij het

115 In deze context is de ervaring uit het Verenigd Koninkrijk interessant. Daar blijkt dat de richtlijnen van de veiligheidsdiensten, de universiteiten en de onderzoeksfinanciers goed in lijn met elkaar zijn dankzij goed overleg (d'Hooghe en Lammertink, 2022, p. 49).

116 (Muneer, 2022)

verhogen van cybersecurity in cruciale sectoren. De invulling van het model bestaat doorgaans uit *best practices* en praktijkstandaarden.

Om het niveau van bekwaamheid vast te stellen, maakt het model gebruik van een schaal die het niveau van volwassenheid definieert (maturity indicator level, MIL). Het beschrijft zodoende hoe bekwaam een organisatie(onderdeel) op verschillende veiligheidsonderdelen (domeinen) is. Organisaties kunnen de schaal gebruiken om hun huidige bekwaamheid vast te stellen, al dan niet in vergelijking met anderen, en kunnen eventueel de mogelijkheden identificeren voor een volgend niveau.

Streven naar het hoogste niveau van volwassenheid is niet zonder meer het doel. Het gaat om het juiste niveau, gegeven de risico's. Er moet dus continu een afweging gemaakt worden in welke mate het wenselijk is.

Figuur 1. Model, domein, doelen en praktijken in een *capability maturity model*[117]

Modelopbouw Het model omvat verschillende domeinen. De praktijken binnen een domein worden gegroepeerd op basis van doelprestaties die het domein ondersteunen. Praktijken representeren de activiteiten die een organisatie uitvoert om een bepaalde bekwaamheid in het domein te vestigen. Het model verzorgt voor elk domein een doelverklaring, die een samenvatting is van de hoofdintentie van het domein. In het geval van het domein 'risicomanagement' kan dat bijvoorbeeld zijn 'het vestigen en bijhouden van plannen en procedures om risico's in onderzoek te identificeren, analyseren en managen, in lijn met de doelen van de organisatie.'

Het *capability maturity model* is dus een coherent en algemeen bruikbaar model dat differentiatie in maatregelen om kennisveiligheid te bewaken mogelijk maakt. Het model helpt om te voorkomen dat kwaadwillende actoren gebruik kunnen maken van de 'zwakste schakel' in het Nederlandse, of zelfs Europese onderzoeksecosysteem. Het geeft kennisinstellingen en hun onderdelen bovendien een manier om zichzelf te

117 Figuur versimpeld overgenomen uit (Muneer, 2022)

vergelijken met andere organisaties. En het draagt bij aan samenwerking, kennisuitwisseling en het voorkomen van concurrentie om lucratieve maar mogelijk ongewenste contracten.[118] In tegenstelling tot bindende en algemeen geldende lijsten van landen of vakgebieden, behoudt deze aanpak ruimte voor differentiatie en draagt bij aan een lerende houding (reflexiviteit) van kennisinstellingen (bijvoorbeeld via benchmarks). De lijsten met risicovakgebieden, risicolanden of risico-organisaties kunnen overigens wel input vormen voor het model. Bovendien, voor de ontwikkeling van het model starten we niet bij nul. Het model kan een vliegende start maken door gebruik te maken van het de nationale leidraad kennisveiligheid, gemaakte risicoanalyses en al ontwikkelde *tools*.

Actie 2. Verken hoe organisatorische diversiteit van kennisinstellingen in Nederland beter benut kan worden voor kennisveiligheid

Er bestaat in Nederland een divers landschap aan kennisinstellingen, variërend van minder tot meer toepassingsgericht en langs verschillende disciplinaire of thematische lijnen. De AWTI heeft deze diversiteit al vaker als waardevol aangeduid;[119] ook voor kennisveiligheid kan deze diversiteit beter benut worden. Een voorbeeld. In de VS komt het voor dat onderzoek dat als ‘classified’ wordt aangemerkt, wordt overgebracht naar nationale onderzoeksinstituten (National Laboratories), waar de veiligheid beter bewaakt kan worden. In Nederland kan een dergelijk onderzoek overgeheveld worden van de ene kennisinstelling naar een andere die beter is toegerust op het mitigeren van kennisveiligheidsrisico’s. Zo sluiten het type onderzoek en de bijbehorende risico’s beter aan op de organisatorische eigenschappen van de kennisinstelling, bijvoorbeeld omdat het niveau van de kennisveiligheidsaanpak op bepaalde onderdelen hoger is. Ook kunnen aparte rechtspersonen – verbonden aan, maar op afstand van de betreffende kennisinstelling – aanvullende veiligheidsmaatregelen treffen die niet eigen zijn aan de aard van de kennisinstelling.

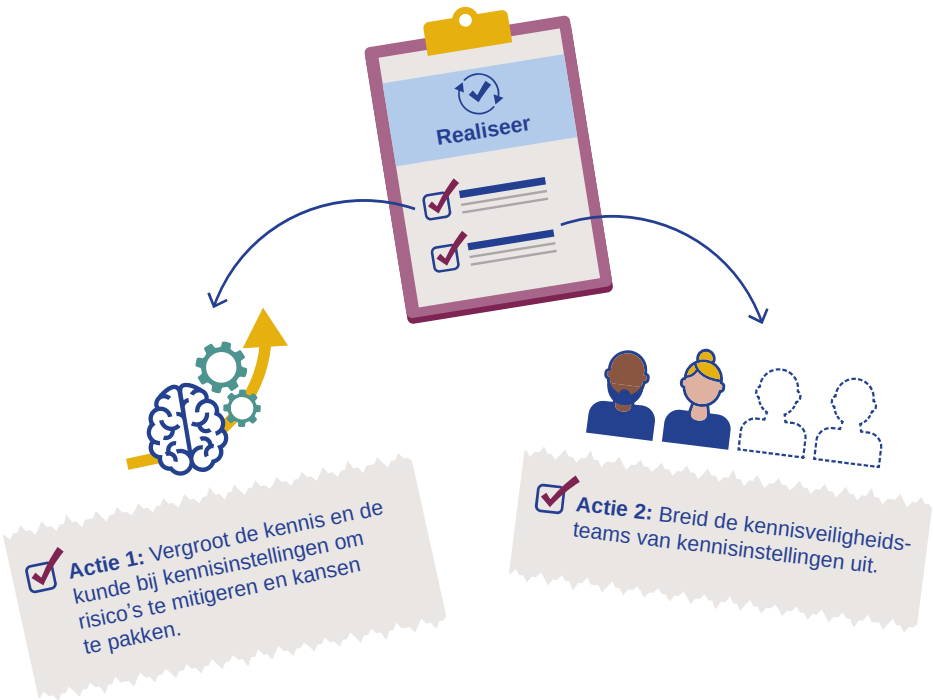
Aanbeveling 3. Realiseer: vergroot het bewustzijn en de capaciteit

Het bewustzijn en de capaciteiten (kennis en kunde) rondom kennisveiligheid zijn nog onderontwikkeld (zie paragraaf 2.3). Daarom beveelt de AWTI kennisinstellingen aan om hier veel aandacht aan te besteden. Het professionaliseringsmodel (aanbeveling 2) vormt belangrijke input voor het ontwikkelen en implementeren van maatregelen, afspraken en

118 Deze vorm van competitie tussen kennisinstellingen is de achilleshiel van een aanpak voor kennisveiligheid. Zie ook de best practices uit (d’Hooghe en Lammertink, 2022, p. 49).
119 (AWTI, 2017a)

veiligheidssystemen. Het uitwerken en implementeren van het model kost tijd; we adviseren daar niet op te wachten. Integendeel, juist de ervaring die nu opgedaan wordt bij kennisinstellingen kan input vormen voor het model.

Aanbeveling 3. Realiseer: vergroot het bewustzijn en de capaciteit.



Om kennisinstellingen slagvaardiger te maken als het gaat om kennisveiligheid bevelen we twee acties aan:

Actie 1. Vergroot in de breedte en de diepte het bewustzijn, de kennis en de kunde bij kennisinstellingen om risico's te mitigeren en kansen te pakken

Op verschillende plekken in de kennisinstellingen moeten individuen zich bewust zijn van de nieuwe risico's die ontstaan als gevolg van geopolitieke veranderingen. Naast bewustwording vergt kennisveiligheid nieuwe vaardigheden en instrumenten. Denk daarbij aan aanvullende *due diligence*, screening procedures, checklists en databeveiliging. We adviseren kennisinstellingen om expertise te verzamelen en te delen

binnen en buiten de instelling, gebruikmakend van kennis en externe informatie.[120] Interne en externe trainingen over kennisveiligheid zouden vaker onderdeel moeten zijn van de opleiding van onderzoekers. Uit het internationaal vergelijkende onderzoek van het LAC blijkt het belang van materiële en immateriële ondersteuning van de overheid.[121] De overheid adviseren we dan ook om kennisinstellingen te ondersteunen met informatie, advies en middelen, zodat daadwerkelijk de ruimte ontstaat om te investeren in preventie, detectie en actie bij problemen rond kennisveiligheid. Die ondersteuning voorkomt dat extra aandacht voor kennisveiligheid de werkdruk bij onderzoekers onnodig verder vergroot. Een bewustwordingscampagne is een concrete invulling van deze actie. De (nationale) Trusted Research campagne in het VK bijvoorbeeld is inspirerend voor Nederlandse kennisinstellingen (zie het kader hieronder).

Trusted Research Campaign

De 'Trusted Research Campaign' is ontwikkeld door het Centre for the Protection of National Infrastructure (CPNI) en het National Cyber Security Centre (NCSC) namens de Britse overheid. Het doel van de Trusted Research Campaign is om 'het bewustzijn te vergroten van de risico's die verbonden zijn aan onderzoekssamenwerkingen waarbij organisaties of onderzoekspartners betrokken zijn die banden hebben met landen waarvan de democratische en ethische waarden anders zijn dan de onze', waarbij met 'onze' natuurlijk het VK wordt bedoeld.[122]

Trusted Research behelst een aanpak die tot doel heeft om de integriteit van het systeem van internationale onderzoekssamenwerking te waarborgen. Dit systeem wordt als essentieel gezien voor het aanhoudende succes van de Britse onderzoeks- en innovatiesector. Onderdeel van Trusted Research zijn richtlijnen en begeleiding voor zowel de academische als de industriële sector. Beide sectoren zijn betrokken bij het tot stand komen van het advies.

De richtlijnen zijn te vinden op de website van de CPNI zelf (zie: https://www.cpni.gov.uk/trusted-research), maar ook in verschillende te downloaden documenten. Al het materiaal wordt ondersteund en overzichtelijke gemaakt met *infographic*s, checklists en verwijzingen naar al bestaande maatregelen die lezers moeten helpen bij de beoordeling van sensitief onderzoek of het maken van strategische afwegingen.

120 In onze gesprekken hebben we gehoord dat sommige kennisinstellingen hier al ver mee zijn, zie bijvoorbeeld (De Bruijn, 2021), maar andere nog niet.
121 (d'Hooghe en Lammertink, 2022)
122 (UKRI, 2021; d'Hooghe en Lammertink, 2022, p. 36; Karásková, Šebok en Blablová, 2022; CPNI, zonder datum).

Actie 2. Breid de kennisveiligheidsteams van kennisinstellingen uit

De kennisveiligheidsteams hebben een belangrijke positie binnen kennisinstellingen. De problematiek die zij tegenkomen is complex. Om een goed en zwaarwegend (of wellicht zelfs bindend) advies te kunnen geven binnen de kennisinstelling, is een uitbreiding van hun expertise en capaciteit van belang. Dit kan bijvoorbeeld in de vorm van een netwerk of een commissie.[123] Deze netwerken of commissies hebben de taak om onderzoekers, decanen en andere beslissers te adviseren over samenwerking, financiering en het aannemen van personen. Ze hebben een directe lijn met het college van bestuur van de betreffende kennisinstelling. Met de uitbreiding van de teams krijgen onderzoekers meer ‘rugdekking’. Niet met het doel om risico’s te minimaliseren, maar om een afgewogen beslissing te nemen.

Het is cruciaal dat de expertise rond kennisveiligheid zich ontwikkelt aan de kennisinstellingen, in de nabijheid van onderzoekers en het onderzoek, en met voldoende oog voor het academische perspectief. Fysieke, sociale en organisatorische nabijheid draagt namelijk bij aan het onderling vertrouwen en begrip, wat essentieel is bij gevoelige onderwerpen als kennisveiligheid. Een nationaal centrum voor kennisveiligheid zou onvoldoende voeling hebben met de gevoeligheden of uiteenlopende problematiek binnen de individuele kennisinstellingen.

De uitgebreide kennisveiligheidsteams opereren niet in isolatie, maar staan in goed contact met de overheid, bijvoorbeeld via het kennisveiligheidsloket en via een voortgezette kennisveiligheidsdialoog. Ook de netwerken of commissies moeten met elkaar in contact staan. Daar ligt een taak voor de organisaties van de Kenniscoalitie.[124] Het instellen van een overlegplatform kennisveiligheid is een concrete invulling van deze actie.

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

Bijlagen

Bijlage 1 Hoe is dit advies tot stand gekomen?

Voor dit advies zijn drie fases doorlopen. In het voorjaar van 2022 heeft de AWTI een verkenning uitgevoerd naar de thematiek rondom kennisveiligheid. We zetten een aantal typische kennisveiligheidsincidenten op een rij, schetsten de beleidsaanpak, en spraken met beleidsadviseurs van onder andere de ministeries van OCW en EZK. Dit heeft geresulteerd in de startnotitie, die uiteenzet welke stappen voor dit advies worden doorlopen.

In de fase daarop is een aantal analyses uitgevoerd. Allereerst is er een stakeholderanalyse gedaan. Ten tweede onderzochten we vanuit verschillende perspectieven de onderliggende waarden die spelen rondom kennisveiligheid (zie Bijlage 4). We hebben, ten derde, een inventarisatie gemaakt van de risico's en dreigingen rondom kennisveiligheid, op basis van verschillende gesprekken en documenten. En tot slot is er een overzicht gemaakt van de beleidsinstrumenten die raken aan kennisveiligheid (zie Bijlage 3).

Parallel is op verzoek van de AWTI door het LeidenAsiaCentre een internationaal vergelijkend onderzoek gedaan naar de maatregelen die overheden en kennisinstellingen nemen om kennisveiligheid te bevorderen. Dit heeft geresulteerd in een aparte studie, die is te vinden op de website van de AWTI, www.awti.nl.

In de finale fase zijn alle inzichten uit de analyses samengebracht, geïnterpreteerd en verwerkt tot een advies. Er is in deze fase ook een aantal gesprekken gevoerd met stakeholders en experts, en er zijn bijeenkomsten bezocht en georganiseerd om de resultaten te valideren en de richting van het advies te bespreken en aan te scherpen.

Bijlage 2 Gesprekspartners

Voor dit advies zijn vele mensen bij uiteenlopende organisaties gesproken. We zijn hen erkentelijk voor hun openheid, tijd en kennis. Een deel van de gesprekspartners is gesproken tijdens een bijeenkomst van de AWTI en de AIV in Den Haag, begin november. Tijdens een werkbezoek in Oostenrijk, spraken we acht experts, beleidsmakers en onderzoekers (niet opgenomen in onderstaande tabel). Voor de internationale studie spraken de onderzoekers nog ongeveer twintig andere mensen.

Sebastiaan den Bak	NWO
Bibi van den Berg	Cyber Security Raad; Universiteit Leiden
Bart van der Berg	Universiteit Utrecht
Nora van Bracht	Ministerie van Onderwijs, Cultuur en Wetenschap
Jan Broeks	Adviesraad Internationale Vraagstukken
Nienke Buisman	Europese Commissie
Mirta Cugini	Datenna
Aad van Dorp	NLR
Juul van Ewijk	Ministerie van Onderwijs, Cultuur en Wetenschap
Marjan Fretz	ARCNL
Sven Hamelink	Nationale Politie
Jennifer Herek	Universiteit Twente; CESAER
Gareth Heywood	Datenna
Just van den Hoek	Neth-ER
Ingrid d'Hooghe	Clingendael Instituut, LeidenAsiaCentre
Hans van der Jagt	Adviesraad Internationale Vraagstukken
Marenne Jansen	Adviesraad Internationale Vraagstukken
Katleen Janssen	KU Leuven
Luuk Klomp	NWO
Linda Krom	TNO
Willemijn Lamet	Universiteiten van Nederland
Floris Lantzendörffer	Ministerie van Economische Zaken en Klimaat
Nina van Lanschot	EclecticIQ
Erwin Mededorp	Universiteit Twente
Max Bueno de Mesquita	Ministerie van Onderwijs, Cultuur en Wetenschap
Irna van der Molen	Universiteit Twente

Marc Moquette	Ministerie van Buitenlandse Zaken
Mirko van Muijen	Ministerie van Onderwijs, Cultuur en Wetenschap Europese Commissie
Karen Passier	Ministerie van Economische Zaken en Klimaat
Jolanda Peters – van Nieuwenhoven	Tilburg University
Jet de Ranitz	SURF
Miriam Roelofs	NWO-I
Joep Roet	Neth-ER
Amber Schilte	Ministerie van Onderwijs, Cultuur en Wetenschap
Henne Schuwer	Adviesraad Internationale Vraagstukken
Haroon Sheikh	WRR
Joris Teer	The Hague Centre for Strategic Studies
Maarten Tossings	TNO
Peter Weijland	TU Delft
Marijk van der Wende	Universiteit Utrecht
Hans de Wit	Boston College
Dick Zandee	Clingendael
-	Algemene Inlichtingen en Veiligheidsdienst
-	Militaire Inlichtingen en Veiligheidsdienst
-	Nationaal Coördinator Terrorismebestrijding en Veiligheid

Bijlage 3 Overzicht maatregelen gerelateerd aan kennisveiligheid

Deze bijlage bevat een overzicht aan maatregelen die bestaan én die gerelateerd zijn aan kennisveiligheid. Het is een breed overzicht, dat desalniettemin onvolledig zal zijn. In dit overzicht wordt onderscheid gemaakt tussen de volgende thema's:

- Maatregelen om kennisverspreiding ten nadele van de nationale veiligheid te voorkomen;
- Maatregelen ter versterking en bescherming van kennisontwikkeling voor de Nederlandse economie;
- Maatregelen ter bescherming tegen buitenlandse inmenging; en
- Maatregelen voor het tegengaan van *misuse* of *ethics dumping*.

Sommige maatregelen vallen onder meerdere thema's en komen zodoende meermaals voor.

Maatregelen om kennisverspreiding ten nadele van de nationale veiligheid te voorkomen

- Bedrijven en kennisinstellingen worden geholpen in het treffen van maatregelen tegen cyberaanvallen. Het Nationaal Cyber Security Centrum (NCSC) is het nationaal expertisecentrum dat ernaar streeft om de Nederlandse samenleving digitaal weerbaar te maken. Het onderneemt daarvoor verschillende activiteiten. Voor vitale bedrijven zijn er speciale organisaties die daarbij helpen. Voor het niet-vitale bedrijfsleven is er het Digital Trust Centre. Voor de kennisinstellingen is SURF de aangewezen partij om cyberveiligheid te versterken.
- Het stelen van kennis is strafbaar. In 2022 is de spionagewetgeving gemoderniseerd.[125] De update is erop gericht om nieuwe vormen van spionage beter te kunnen aanpakken. Schendingen van staats- of bedrijfsgeheimen waren al strafbaar, maar met het nieuwe voorstel komt het in gevaar brengen van de nationale veiligheid en de veiligheid van personen erbij.
- Bedrijven en kennisinstellingen die betrokken zijn bij defensieopdrachten moeten beveiligingsmaatregelen treffen. Zo dienen bedrijven zich te houden aan de Algemene Beveiligingseisen voor Defensieopdrachten (ABDO) om gevoelige

125 (Ministerie van Justitie en Veiligheid, 2022)

informatie te beschermen.[126] De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) controleert dit.

- Bedrijven en kennisinstellingen dienen zich te houden aan exportwetgeving ten aanzien van *dual use* goederen. *Dual use*-goederen zijn goederen die een civiele, maar ook militaire toepassing kennen (bijvoorbeeld een stof die als brandvertrager dient in de bouw, maar ook gebruikt kan worden in de productie van gifgas).[127] Onder deze goederen valt ook kennis, met uitzondering van “fundamenteel wetenschappelijk onderzoek”. Het beleid wordt in Europa vastgesteld en regelmatig geüpdatet (december 2019 voor het laatst). De lange, gedetailleerde lijst van goederen in de verordening wordt opgesteld overeenkomstig internationale afspraken waaronder Australië Groep, het controleregime voor de uitvoer van rakettechnologie en -onderdelen (MTCR), de Groep van nucleaire exportlanden, het Wassenaar Akkoord en het Verdrag inzake chemische wapens.
- Er wordt gewerkt aan een veiligheidstoets op investeringen, overnames en fusies (‘Wet vifo’).[128] Deze geldt voor bedrijven die een vitale aanbieder zijn of die beschikken over sensitieve kennis of technologie. De wet is ontwikkeld om te voorkomen dat ‘kwaadwillende partijen’ zeggenschap krijgen over bedrijven die beschikken over technologie die een militair of strategisch risico vormen voor de nationale veiligheid. Zowel de investeerders als de ondernemingen zelf moeten wijzingen van zeggenschap melden bij het ministerie van Economische Zaken en Klimaat. Een bureau beoordeelt of er een risico ontstaat voor de nationale veiligheid.
- Kennisinstellingen dienen zich te houden aan een tweetal kennisembargo’s.[129] Om te voorkomen dat kennis over het maken van raketten en kernwapens in Iran en Noord-Korea terechtkomt, moet iedereen die een studie of onderzoek doet op dit gebied een ontheffing aanvragen. In 2018 kwam er een verscherpt toezicht op deze wetgeving, via de zogenaamde Taskforce Ongewenste Kennisoverdracht.[130]
- De gedragscode wetenschappelijke integriteit verplicht onderzoekers te werken vanuit een aantal leidende principes: eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid. Het gaat naast methodische normativiteit (is het onderzoek van goede kwaliteit) ook om ethische normativiteit. Daaronder vallen ook (ethische of strategische) risico’s van het openbaar maken van data.

126 (Ministerie van Defensie, 2019).
127 (Ministerie van Buitenlandse Zaken, 2018)
128 (Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, 2022b)
129 https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies
130 (Heerschop en Riedstra, 2021)

- Het afgelopen jaar is er onder de noemer van kennisveiligheidsbeleid een aantal aanvullende maatregelen getroffen die ongewenste kennisoverdracht ten aanzien van de nationale veiligheid moet (helpen) voorkomen. Ten eerste is er een nationale leidraad die moet bijdragen aan de bewustwording en die praktische handvatten biedt. Ten tweede is er een loket kennisveiligheid, waar onderzoekers en kennisinstellingen met specifieke vragen naar toe kunnen.[131] Ten derde is het bij kennisinstellingen verplicht om een bestuurlijk verantwoordelijke en een beleidsteam aan te wijzen voor kennisveiligheid. Ten vierde dienen alle kennisinstellingen een risicoanalyse te doen op internationale samenwerking. Ten vijfde is een externe audit aangekondigd naar het kennisveiligheidsbeleid bij kennisinstellingen. Tot slot is een toetsingskader aangekondigd (verwacht in 2023) waar individuen uit 'derdelanden' toegang moeten vragen om in Nederland te studeren of te werken in sensitieve kennisdomeinen.

Beleid ter versterking en bescherming van kennisontwikkeling voor de Nederlandse economie

- In brede zin is het onderzoeks- en innovatiebeleid erop gericht om het Nederlandse bedrijfsleven innovatief en competitief te houden om de economische concurrentie met andere landen aan te kunnen. Ook in en vanuit Europa wordt onderzoek en innovatie gestimuleerd, bijvoorbeeld via Horizon Europe.[132] Daarbij speelt momenteel de vraag in hoeverre niet-EU-landen mogen deelnemen aan Europese industriële allianties. Ter illustratie, China wordt daarin uitgesloten en alleen met "gelijkgestemde landen" wordt samengewerkt.
- Bedrijven worden aangemoedigd om internationaal zaken te doen, zowel vanuit economische ontwikkeling als ontwikkelingssamenwerking.
- Om cruciale technologische gebieden te versterken, is er in Nederland en Europa aandacht voor het stimuleren van kennisontwikkeling op deze gebieden. Denk bijvoorbeeld aan het Sleuteltechnologiebeleid en het Nationaal Groeifonds. In Europa bestaat het beleid rondom de Key-enabling technologie[133] en recentelijk de European Chips Act.[134]

131 https://www.loketkennisveiligheid.nl/
132 Er zit wel een spanning in dit beleid, want enerzijds wordt aangemoedigd met andere landen samen te werken ten behoeve van kennisontwikkeling, competitiviteit en om geopolitieke redenen. Daarbij wordt de aantrekkelijkheid van Europa gebruikt om derde landen te verleiden samen te werken. Maar anderzijds is Europa ook kritisch op welke landen daarvoor in aanmerking komen. Zie ook (European Commission, 2021b; Molthof, Zandee en Cretti, 2021; Roet, 2022)
133 (Müller en Potters, 2019)
134 (European Commission, 2022)

- De Europese Commissie is gestart met Important Projects of Common European Interest (IPCEIs).[135] Deze laten ruimere publieke financiering toe voor bepaalde ecosystemen. Het is in zekere zin een afzwakking van de staatsteunregels, onder bepaalde voorwaarden. Het hangt samen met het missiegedreven innovatiebeleid en het Europese industriebeleid. De Europese Commissie bepaalt daarbij in hoge mate wat onderzocht moet worden. De Europese Commissie onderzoekt bovendien een mogelijke versoepeling van fusiebeleid waardoor er Europese kampioenen kunnen ontstaan.[136]
- Een andere maatregel betreft het verankeren van technologische standaarden van Europese binnenmarktregels.[137] Deze standaarden rivaliseren met andere standaarden op de internationale markt. Het doorzetten van Europese standaarden biedt daarom strategische voordelen voor de Europese industrie en kan de economische competitiviteit vergroten.
- Nederlandse en buitenlandse bedrijven worden gestimuleerd om zich in Nederland te (blijven) vestigen ter versterking van de Nederlandse economie en kennispositie.[138]
- De kennispositie van bedrijven en kennisinstellingen wordt internationaal beschermd via wetgeving over intellectueel eigendom.
- De Europese Commissie bereidt 'antidwangregelgeving' (*anti-coercion instrument*) voor.[139] Hierin worden economische eisen gesteld aan bedrijven om overheden onder druk te zetten. Daarin is reciprociteit het uitgangspunt (als Europese bedrijven geen toegang hebben tot een buitenlandse markt, dan krijgt dat land ook geen toegang tot de Europese markt).
- Ter bescherming van cruciale, vitale sectoren bestaan wettelijke sectorspecifieke investeringstoetsen. Deze bestonden al voor de elektriciteits-, gas- en telecommunicatiesector en worden met de nieuwe, eerdergenoemde Wet veiligheidstoets, investeringen, fusies en overnames' (Wet vifo) uitgebreid.[140]
- Het eerdergenoemde kennisveiligheidsbeleid draagt ook bij aan het bewustzijn voor risico's van kennisoverdracht. Dit heeft ook een weerslag op de economische competitiviteit en stabiliteit.

135 https://www.rvo.nl/subsidies-financiering/ipcei
136 (AIV, 2022, pp. 27–28)
137 (Lippert en Perthes, 2020)
138 (Minister van EZK, 2022)
139 (European Commission, 2021a)
140 (Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid, 2022b)

Maatregelen ter bescherming tegen buitenlandse inmenging

Buitenlandse actoren proberen invloed uit te oefenen op organisaties of personen in Nederland en daarmee de wetenschappelijke, sociale, democratische en maatschappelijke processen in de samenleving aan te tasten. Met de opkomst van autocratische landen wordt dit probleem groter voor kennisinstellingen in Nederland.

- De gedragscode wetenschappelijke integriteit verplicht onderzoekers te werken vanuit een aantal leidende principes: eerlijkheid, zorgvuldigheid, transparantie, onafhankelijkheid en verantwoordelijkheid. Deze gedragscode beschermt zodoende tegen buitenlandse inmenging.[141]
- Het eerdergenoemde cybersecuritybeleid draagt bij aan ongemerkte inmenging via digitale wegen.
- Voor de beveiliging van persoonsgegevens van Europese burgers bestaat de GDPR.[142]
- Het kennisveiligheidsbeleid van de overheid omvat ook maatregelen tegen buitenlandse inmenging. In het bijzonder gaat het om de 'leidraad kennisveiligheid'[143], het 'Loket kennisveiligheid'[144] en de verplichte risicoanalyse.[145] Deze zijn er onder andere op gericht om eventuele kwetsbaarheden voor buitenlandse inmenging te voorkomen.

Maatregelen relevant voor het tegengaan van *ethics dumping* of *misuse*

Hoewel het overgrote deel van de onderzoeksgemeenschap werkt volgens hoge ethische standaarden, zijn er ook plekken op de wereld waar deze minder strikt worden nagekomen. *Ethics dumping* is het gebruik lage ethische standaarden, bijvoorbeeld op het gebied van dierproeven of medisch ethische normen, in onderzoek. *Misuse* is het benutten van kennis voor onethische doeleinden; als de kennis wordt misbruikt tegenover mensen of dieren, waar dan ook ter wereld. Dit kan gaan om militaire toepassing, maar ook om andere onethische praktijken, zoals surveillance, onderdrukking of marteling.

- De *dual use* exportwetgeving en kennisembargo's dragen bij aan het beperken van 'misuse', al gaat het daarbij vooral om kennis met (deels) militaire toepassing. Maar surveillance technologie valt hier bijvoorbeeld niet onder.[146]

---

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

- De eerdergenoemde gedragscode wetenschappelijke integriteit[147] draagt bij aan het tegengaan van *ethics dumping* of *misuse* Wetenschappelijke integriteit is bovendien internationaal afgesproken via het Singapore Statement on Research Integrity, ALLEA[148] en het UNESCO statement on Science and Scientific Researchers.[149]
- Het Nagoya protocol zorgt voor het zorgvuldig gebruik van genetisch materiaal. Onzorgvuldig gebruik van genetisch materiaal kan mensenrechten aantasten. In Nederland controleert de NVWA bedrijven en kennisinstellingen die met genetisch materiaal werken opdat zij dat zorgvuldig doen.[150]
- Het eerdergenoemde Kennisveiligheidsbeleid, inclusief de leidraad, het loket en de risicoanalyse van de afgelopen jaren wil onderzoekers en kennisinstellingen bewuster maken van de risico's van *misuse* of *ethics dumping*.

147 (KNAW *e.a.*, 2018)
148 (ALLEA, 2017)
149 https://en.unesco.org/themes/ethics-science-and-technology/recommendation_science
150 https://www.nvwa.nl/onderwerpen/nagoya-protocol

Bijlage 4 Een reflectie op onderliggende waarden vanuit drie perspectieven

In de discussie omtrent kennisveiligheid wordt regelmatig beroep gedaan, impliciet dan wel expliciet, op waarden. Waarden zijn zaken waarvan we veronderstellen dat ze bijdragen aan 'het goede'. Zo veronderstellen we bijvoorbeeld dat academische vrijheid bijdraagt aan goede wetenschap.

Vanuit deze invalshoek is het ook mogelijk om een *waarden-analyse* uit te voeren. Hierbij wordt vanuit drie perspectieven onderzocht welke waarden relevant zijn voor veilige kennisontwikkeling in een veranderende geopolitieke context. Met andere woorden, hoe raken die waarden door de huidige internationale (geo)politieke ontwikkelingen in het geding en hoe dienen die eventueel door beleid beschermd te worden? De drie perspectieven zijn veiligheid, economie en academie.

De gesprekken die we voeren tonen aan dat vanuit verschillende perspectieven en disciplines mensen werken aan kennisveiligheid. Soms is men ook in gesprek met elkaar, maar is men nog niet tot een coherente blik op het probleem gekomen. Verschillende onderliggende waarden lijken elkaar soms tegen te spreken. Vanuit de drie genoemde perspectieven worden de onderliggende waarden geanalyseerd, de overeenkomsten en verschillen in beeld gebracht, en de achtergrond daarvan beschreven.

Deze notitie beschrijft in drie achtereenvolgende paragrafen eerst binnen elk perspectief de relevante waarden. Elke paragraaf start met de belangrijkste conclusies en werkt daarna de discussie rondom waarden verder uit. Een vierde en laatste paragraaf maakt een vergelijking tussen de drie perspectieven.

Veiligheidsperspectief

Een veiligheidsperspectief draait om de bescherming van de democratie en gewichtige belangen van de staat tegen nationale en internationale dreigingen.[151] Het gaat om het behouden van een bepaalde mate van **stabiliteit en soevereiniteit** die samenhangt met het type samenleving die Nederland is, zowel in politieke (bescherming democratische rechtsstaat) als economische (kennisveiligheid, strategische afhankelijkheden), als materiële zin (grondgebied, fysieke veiligheid). Opvallend is daarbij het frame van de 'wedloop'. De gedachte daarbij is dat andere landen bezig zijn met een technologische of economische inhaalrace en daarvoor soms kennis en techniek uit Nederland proberen te stelen, of achter bedrijfsovernames, fusies en investeringen kunnen zitten die Nederland

151 (AIVD, 2022)

niet goed doen. Dit kan de welvaart, stabiliteit en de openheid van onze samenleving aantasten. [152] Als onderliggende aanname wordt dus het frame van een inhaalrace gehanteerd om de internationale context en de nationale veiligheid van Nederland daarbinnen, te begrijpen. Dat lijkt uit te gaan van een soort *zero-sum* gedachte.

In samenhang daarmee wordt gesteld dat **continuïteit** van vitale infrastructuur, **integriteit** en **exclusiviteit** van kennis en vertrouwelijke informatie en het voorkomen van (ongewenste) strategische afhankelijkheden essentieel zijn voor de economische veiligheid van Nederland en het behoud van onze economische positie. Hierin wordt er dus een verbinding gemaakt tussen economisch belang en de continuïteit en integriteit van de Nederlandse infrastructuur en kennis. Daarin speelt de gedachte van het behouden en intact houden van een bepaalde status quo. Inmenging die de bestaande inrichting verstoord, wordt als bedreiging gezien.

Bovenstaande observaties komen voort uit een analyse van drie deelperspectieven, in lijn met het Dreigingsbeeld statelijke actoren, en de onderliggende waarden daarin:[153]

Territoriale veiligheid is het 'ongestoord functioneren van Nederland en zijn EU- en NAVO-bondgenoten als onafhankelijke staten in brede zin, dan wel in enge zin'. Territoriale veiligheid in enge zin heeft betrekking op de integriteit van het grondgebied van Nederland, de EU en het NAVO-bondgenootschap en de bijbehorende vitale infrastructuur (bijvoorbeeld de Rijksoverheid met bijbehorende vitale processen en hun toeleveranciers). Territoriale veiligheid in brede zin omvat de integriteit van essentiële organisaties, instituten en diensten, kennisinstellingen, bedrijven en topsectoren en internationale verbanden die noodzakelijk zijn voor het soeverein functioneren van de Nederlandse staat. De veiligheid van het digitale domein valt hier ook onder.

Een aantal aspecten hangt samen met veilige kennisontwikkeling. De **integriteit van kennisinstellingen** en de samenhang met het soeverein functioneren van de Nederlandse staat raakt aan heimelijke beïnvloeding: een (niet) statelijke actor die invloed uitoefent op het functioneren van een kennisinstelling, raakt daarmee aan de soevereiniteit van de Nederlandse staat. Ook de veiligheid van het digitale domein raakt aan veilige kennisontwikkeling. Spionage en heimelijke beïnvloeding vinden steeds meer plaats via digitale weg, om politieke, militaire, economische en/of ideologische doelen te bereiken.[154]

152 (AIVD, MIVD, en NCTV, 2021)
153 (AIVD, MIVD, en NCTV, 2021)
154 (AIVD, MIVD, en NCTV, 2021) N.B., er wordt op dit punt niet gespecificeerd of het hier ook om kennisinstellingen gaat.

Een tweede aspect is spionage. **Spionage** vindt plaats als heimelijk of onrechtmatig informatie of objecten worden verkregen door een ander land of in opdracht van een ander land. Als door spionage innovatieve kennis en technologie verdwijnen, tast dat de Nederlandse veiligheid aan, bijvoorbeeld door de ontwikkeling van wapens die mogelijk de territoriale integriteit van Nederland aantasten.[155] Daarnaast kan overdracht van hoogwaardige kennis en technologie leiden tot ongewenst eindgebruik, bijvoorbeeld het ontwikkelen van militaire of surveillancetoepassingen die van invloed zijn op de nationale Nederlandse veiligheid.

Een derde aspect is het belang van **sociale en politieke stabiliteit** voor de democratische rechtsstaat. Het gaat dan om het ongestoord voortbestaan van een maatschappelijk klimaat waarin individuen en groepen ongestoord kunnen functioneren en met elkaar samenleven. Doelwitten binnen dit kader zijn onder andere ook de wetenschap, adviesorganen en onderwijs- en kennisinstellingen. De relatie met veilige kennisontwikkeling wordt gekenmerkt door diasporapolitiek. Dit kan leiden tot zelfcensuur in het publieke debat of het meewerken met inlichtingendiensten, door bijvoorbeeld sensitieve (wetenschappelijke) kennis te delen. Andersom speelt zelfcensuur ook een rol voor Nederlandse wetenschappers die internationaal opereren. De druk van beïnvloedings- en inmengingsactiviteiten kunnen ertoe leiden dat wetenschappers zich niet openlijk kritisch durven uitlaten.[156]

Een vierde aspect is de **economische veiligheid**: het ongestoord functioneren van Nederland als een effectieve en efficiënte economie. Het gaat dan om de continuïteit van vitale processen, de integriteit en exclusiviteit van informatie en kennis en het voorkomen van (ongewenste) strategische afhankelijkheden. Het raakvlak met kennisveiligheid is hier de hoogwaardige kennis, technologie en infrastructuur die Nederlandse topinstellingen en kennisinstellingen bezitten. Deze kunnen het doelwit worden van spionage, maar ook van onwenselijke overdracht door (legale) samenwerkingsverbanden. Daarnaast kan ongewenste overdracht van kennis over bijvoorbeeld de vitale infrastructuur, deze infrastructuur in gevaar brengen, omdat het daardoor makkelijker wordt om er inbreuk op te maken. Economische veiligheid betekent dus binnen het veiligheidsperspectief de veiligheid van vitale processen op basis waarvan de economie functioneert.

Economisch perspectief

Momenteel vindt een transformatie plaats binnen de huidige mondiale economische orde. Sinds een aantal jaar is er dan ook een verschuiving op te merken in het economisch

155 (AIVD, MIVD, en NCTV, 2021, p. 18)
156 (AIVD, MIVD, en NCTV, 2021)

denken binnen Europa. Die verschuiving kan gekarakteriseerd worden door een toenemende rol voor overheden in de economie. Momenteel begint deze verschuiving ook op nationaal niveau een rol te spelen.[157] Hierbij staat het vernieuwde Europese economische denken vaak model.

Een kernbegrip binnen deze nieuwe manier van denken in het Europese economische beleid is 'open strategische autonomie'. Dit behelst de capaciteit om autonoom, wanneer en waar nodig met wie dan ook, te kunnen handelen. Op militair en veiligheidsgebied is dat niet iets nieuws, maar door economische verschuivingen (China als grootste, gevolgd door India) is strategische autonomie ook noodzakelijk voor politieke overleving.[158] Daarnaast heeft de Covid-19 crisis, maar ook de handelsoorlog tussen de VS en China, aangetoond dat (asymmetrische) economische afhankelijkheid kwetsbaar maakt. Wetenschap, technologie, handel en data worden steeds vaker ingezet als instrumenten in internationale machtspolitiek.[159]

De Europese Commissie wil de Europese markt versterken, en komt in de eerste plaats met ondersteunende maatregelen. Om **economische soevereiniteit** te bevorderen, moet de Europese interne markt beschermd worden en moeten strategische afhankelijkheden beperkt worden. Daarnaast moeten Europese waarden bevorderd worden en omstandigheden gecreëerd voor **een sterke Europese economie**, waarbinnen Europese bedrijven kunnen floreren en de competitie aan kunnen gaan met bedrijven uit Amerika, China en andere landen.[160] Er zit in deze gedachte dus zowel een defensieve als een offensieve component: aan de ene kant de soevereiniteit van de eigen economie behouden, en aan de andere kant de competitie aan kunnen gaan met de ander.[161]

De vraag is dan wat de Nederlandse positie ten opzichte van dit Europese beleid is. In maart 2021 publiceerde Nederland samen met Spanje een document waarin de landen aangeven dat Europa open dient te zijn waar kan, maar autonoom waar moet.[162] Daarmee wordt expliciet de nadruk gelegd op openheid, in plaats van alleen autonomie. De landen waarschuwen in het document voor het feit dat strategische autonomie niet moet leiden tot isolationisme of economisch protectionisme. Daartegenover worden **samenwerking** en **internationale handel** benadrukt, evenals de **efficiëntie** en **competitiviteit** van de Europese interne markt. De onderliggende gedachte is dus dat de economische competitiviteit en efficiëntie afhankelijk is van de **openheid** van deze

157 Zie bijvoorbeeld (AIV, 2022)
158 (Borrell, 2020)
159 (Borrell, 2020; AIV, 2022, pp. 25–26)
160 (Korteweg, Ortega en Otero, 2022, p. 2)
161 (AIV, 2022, p. 26)
162 (Spain en Netherlands, 2021)

economie. En dat geldt zeker voor Nederland. Dat roept de vraag op waar (economische) openheid eindigt, en autonomie (soevereiniteit) begint. [163] Nederland en Spanje pleiten voor **maatwerk** en **proportionaliteit**. De kernvraag is dan natuurlijk wat dat in deze context concreet betekent.

Academisch perspectief

De veranderende geopolitieke context zorgt ervoor dat academische instellingen zich opnieuw moeten verhouden tot een aantal fundamentele kernwaarden. Daarbij moet wel opgemerkt worden dat de academie altijd al binnen een geopolitieke context heeft bestaan. Het meeste academische onderzoek wordt bekostigd door nationale overheden, wat academisch onderzoek in zichzelf al politiek van aard maakt. Bovendien is het idee van mondiale wetenschappelijke onderzoekssamenwerking ontstaan tijdens de Koude Oorlog en heeft het daarmee diepe geopolitieke wortels: het was een poging van Westerse overheden om wetenschap aantrekkelijker te maken voor onderzoekers dan de wetenschap in gesloten, communistische landen.[164]

Academische waarden (zie kader hierna) hebben voornamelijk betrekking op de wijze waarop de academische wereld dient te functioneren: **open**, **gelijkwaardig** en **onafhankelijk**. Enerzijds omdat dat rechtvaardig is, anderzijds omdat dat bijdraagt aan de kwaliteit van onderzoek. Deels staan deze waarden ook ten dienste van de samenleving: uiteindelijk heeft de academie ook de **verantwoordelijkheid** om met onderzoek de uitdagingen in de wereld aan te gaan – en dat in internationaal verband. Academische waarden hebben dus zowel betrekking op de academie of onderzoeker zelf (**institutionele** en **morele autonomie**), als op de buitenwereld (**openheid, internationale samenwerking en maatschappelijke verantwoordelijkheid**). Het is de taak van de academie en onderzoekers om hier steeds een juiste balans in te vinden.[165]

De waarden binnen het academische perspectief kunnen op verschillende manieren in het geding komen. Ten eerste kan het overdragen van hoogwaardige kennis met *dual use* toepassingen (of *dual use* toepassingen zelf) leiden tot de ontwikkeling en verspreiding van wapens die de eigen nationale veiligheid aantasten. Dat staat haaks op de integriteit en ethiek zoals die gedefinieerd zijn in verschillende belangrijke documenten (zie kader hierna).

Ten tweede kunnen institutionele vrijheid en autonomie in het geding komen door financiële afhankelijkheid.

---

163 (Inspectie der Rijksfinanciën, 2020, p. 13)
164 (Fischer, 2022a)
165 (KNAW, 2021, p. 36)

Een derde manier waarop waarden in het geding komen is wanneer docenten of onderzoekers heimelijk beïnvloed worden, met als gevolg (zelf)censuur, beïnvloeding van keuzes van onderzoeksonderwerpen en aantasting van de integriteit van onderzoek.[166] Dit raakt natuurlijk aan de ethische component in het doen van onderzoek, evenals aan de academische vrijheid die wetenschappers zouden moeten hebben in termen van morele en wetenschappelijke autonomie.

Maar academische waarden kunnen ook in het geding komen wanneer wordt gekozen voor een te rigide aanpak van kennisveiligheid. Dit gebeurt bijvoorbeeld bij een langdurig bureaucratisch proces, waardoor belangrijk onderzoek vertraging oploopt. Dit kan ook gebeuren door een rigide beperking van samenwerkingsmogelijkheden, wat de institutionele autonomie, inclusiviteit, maatschappelijke bijdrage en het belang van samenwerking kan aantasten (bijvoorbeeld als het gaat om gelijke samenwerking tussen academische instellingen, of de gelijke toegang tot de academische gemeenschap).

Tot slot staat het borgen van veiligheid in kennisontwikkeling in ieder geval op gespannen voet met open academische samenwerking en het delen van kennis. Tegelijkertijd moet openheid niet alleen vanuit een eigen perspectief worden gezien. De achterliggende waarde daarvan is vooruitgang van wetenschap en maatschappij, maar openheid kan deze vooruitgang ook juist tegenwerken. Zo kan er sprake zijn van het schenden van academische integriteit door het niet delen van data of het achterhouden van bepaalde onderzoeksresultaten.[167] In meer fundamentele zin kan openheid leiden tot ongewenste overdracht van kennis die wordt ingezet voor het ontwikkelen van bijvoorbeeld surveillancetechnologie of chemische wapens waarmee mensenrechten worden geschonden.

Academische waarden

Het onderzoekssysteem in Europa staat momenteel in toenemende mate zowel intern als extern onder druk. Vanuit de Europese vereniging voor onderzoeksfinancierende en -uitvoerende organisaties, Science Europe, is daarom een waarden-kader ontwikkeld, veelal voortbouwend op andere documenten als de Magna Charta Universitatum en de Verklaring van Lima. Dit waardenkader is in lijn met de uitingen van de KNAW.[168] De waarden die hierin worden genoemd zijn: **autonomie en vrijheid, zorg en collegialiteit, samenwerking, gelijkheid, diversiteit en inclusie,**

166 (VSNU, 2021, p. 14).
167 (d'Hooghe en Lammertink, 2020, pp. 42–43)
168 (KNAW, 2021, p. 25; Magna Charta Universitatum Observatory, 2022; Science Europe, 2022)

integriteit en ethiek, en openheid en transparantie. Ook maatschappelijke bijdrage is hierbij belangrijk.

Autonomie en vrijheid[169] betekent vrij van politieke invloed en economisch belang. Deze onafhankelijkheid moet erkend en beschermd worden door de overheid en samenleving. Ieder lid van de academische gemeenschap heeft het recht om hun rol zonder discriminatie, en zonder angst voor repressie in beïnvloeding van een staat of andere bron, te vervullen. Wetenschap kent bovendien een open einde, en daarom is het van belang dat wetenschappers zonder beperking hun eigen nieuwsgierigheid moeten kunnen volgen. Overigens zijn deze autonomie en vrijheid niet absoluut. Zij wordt beperkt door wettelijke verplichtingen die instellingen in het hoger onderwijs hebben, maar ook door andere academische waarden zoals integriteit en transparantie.[170]

Zorg en collegialiteit wordt omschreven als de zorg voor het ecosysteem waar onderzoek in plaatsvindt, inclusief het verantwoord gebruik van hulpbronnen, alsook het creëren van een respectvolle omgeving vrij van intimidatie. Elk lid van de academische gemeenschap geniet immers gewetensvrijheid en vrijheid van gedachten, religie, expressie, vergadering en beweging.[171]

Samenwerking hangt samen met het belang om samenwerking te stimuleren. Zowel binnen bepaalde disciplines, als inter- en transdisciplinair, maar ook met relevante beleidsterreinen, industriesectoren en de samenleving in zijn geheel. Internationale academische samenwerking dient bovendien aangemoedigd te worden, welke regionale, politieke en andere barrières overstijgt. Daarbij dient ook de replicatie en reproductie van onderzoek geborgd te zijn. Universiteiten behoeven daarvoor een betrouwbaar sociaal contract met de maatschappij.[172]

Gelijkheid, diversiteit en inclusie behelst het toegankelijk zijn van alle rollen binnen de wetenschappelijke gemeenschap, onafhankelijk van sekse, gender, geaardheid, religie of andere factoren. Daarnaast wordt ook het belang van de diversiteit van *research inputs* (data, methoden) en *outputs* (vormen van communicatie en verspreiding) benadrukt. Bovendien moet dit alles voor iedereen toegankelijk zijn.

169 N.B. er wordt vaak een onderscheid gemaakt tussen academische vrijheid voor het individu en de instelling, waarbij de laatste wordt omschreven als institutionele autonomie. Beide aspecten vallen hier onder autonomie en vrijheid.
170 (KNAW, 2021, p. 26)
171 (World University Service, 1989)
172 (Magna Charta Universitatum Observatory, 2022)

Integriteit en ethiek refereren aan het behouden van de betrouwbaarheid, eerlijkheid en verantwoordelijkheid in zowel het uitvoeren van onderzoek, als de financiering van onderzoek en het publiceren van de uitkomsten van onderzoek. Dit gaat ook over het voorkomen van het misbruiken van wetenschap en technologie die het verwezenlijken van eerdergenoemde vrijheden benadelen. Instellingen dienen ook kritisch te zijn op het schenden van mensenrechten in de eigen samenleving en solidair te zijn met instellingen wanneer zij hier onderhevig aan zijn.

Openheid en transparantie houdt het delen en toegankelijk maken van alle aspecten van onderzoek in, met het oog op de uitlegbaarheid van onderzoek.

Maatschappelijke bijdrage is de verantwoordelijkheid om te reageren op de ambities en uitdagingen van de wereld en de gemeenschappen die zij dienen, om zo de mensheid ten goede ten komen en bij te dragen aan duurzaamheid. Alle hogere onderwijsinstellingen dienen zich in te zetten voor het verwezenlijken van economische, sociale, culturele, civiele en politieke rechten van de samenleving. Ook zal elke instelling zich richten op hedendaagse maatschappelijke problemen. Bovendien dient elke instelling te streven naar het voorkomen van wetenschappelijke en technologische afhankelijkheid om zo gelijkwaardig partnerschap te bewerkstelligen.[173]

Vergelijking van de verschillende perspectieven

De bespreking van het veiligheidsperspectief, het economische perspectief en het academische perspectief laat zien dat er flink wat spanningen optreden binnen de veranderende geopolitieke context waarin kennisontwikkeling zich begeeft. Tot nu toe zijn deze spanningen steeds benaderd vanuit één perspectief. Er is echter ook een aantal spanningen aan te wijzen *tussen* deze perspectieven.

Autonomie en soevereiniteit

Ten eerste valt op dat autonomie of soevereiniteit in elk van de drie perspectieven terugkomt. Dit lijkt dus een breed gedeelde waarde te zijn, die weliswaar binnen elk perspectief een andere invulling krijgt. Zo betekent autonomie vanuit veiligheidsperspectief het mijden van onwenselijke invloed met het oog op nationale stabiliteit. De samenhang tussen soevereiniteit en stabiliteit levert binnen het veiligheidsprobleem dan ook niet direct spanning op. Dat is anders bij het economische of academische perspectief, waar autonomie ten dienste staat van concurrentiekracht of goede wetenschapsbeoefening. Hier treedt een spanning op, omdat concurrentiekracht

173 (Magna Charta Universitatum Observatory, 2022)

en wetenschapsbeoefening beide werkzaam zijn binnen een internationale context, en dus openheid behoeven. Het economische en academische perspectief kennen daarmee dus een spanning tussen kernwaarden, die het veiligheidsperspectief binnen haar eigen kaders niet kent.

In lijn met de bovenstaande spanning tussen het veiligheidsperspectief enerzijds en het economische en academische perspectief anderzijds, kunnen we ook een stel houdingen identificeren die onderling verschillen. Het veiligheidsperspectief lijkt een houding te hebben die zich kenmerkt door het 'behouden' of 'beschermen' van onze manier van werken en leven, terwijl het economische en academische perspectief een houding hebben die zich het beste laat kenmerken als 'verbeteren' of 'verspreiden'. In economische zin uit zich dat in het vrije verkeer van goederen, diensten en personen om de economische kracht te verbeteren. In academische zin uit zich dat in het vrije verkeer van personen, data, onderzoekssamenwerkingen en -resultaten om zo de maatschappelijke impact van wetenschap te vergroten.

Vanzelfsprekend loopt door deze spanningen dan ook een nationaal-internationale as. Het economische en academische perspectief zijn van meet af aan een internationaal perspectief, zowel als het gaat om het einddoel (kennis) als om het proces (wetenschap bedrijven). Natuurlijk kent het veiligheidsperspectief ook een internationale component, maar dan juist om de *nationale* belangen te behartigen.

Wie beperkt of verdedigt de waarden?

Ten tweede komt er een meer algemeen punt naar voren als we de verschillende perspectieven met elkaar vergelijken. Waarden komen niet alleen in het geding door 'de ander' (spionage, heimelijke beïnvloeding) maar mogelijk ook door 'eigen' beleid. Een te strikt, risicomijdend beleid zet bepaalde kernwaarden zoals openheid en autonomie ook onder druk. Op economisch gebied is Nederland hier in beleidsmatige zin wel alert op (het pleiten voor *open* strategische autonomie), maar op academisch gebied lijkt er momenteel een tegenovergestelde trend zichtbaar. Waar de focus binnen het beleid eerst lag op zelfregulering van kennisinstellingen, worden nu steeds meer bindende beleidsinstrumenten ingezet zoals het toetsingskader en het bestuursakkoord waar een externe audit onderdeel van is.

Academisch-economische spanningen

Ten derde zijn er een aantal spanningen tussen het economische perspectief en het academische perspectief aan te wijzen. De belangenbehartiger 'Universiteiten van Nederland' noemt de spanning tussen enerzijds het academisch ondernemerschap bestaande uit vrije verspreiding van kennis en zoveel mogelijk vruchtbare samenwerking,

en anderzijds het beschermen van de innovatiekracht ten opzichte van andere landen.[174] Op dit punt staan academische waarden en economische waarden dus op gespannen voet met elkaar.

Daarnaast levert ook de financiële incentivestructuur van de universiteiten een spanning op. Hier komen economische stabiliteit, academische autonomie en het veiligheidsperspectief samen. Internationalisering binnen de wetenschap is lange tijd van belang geweest in het vergroten van de tweede en derde geldstroom. Dit werd ook vanuit de overheid gestimuleerd. Een te grote nadruk op risicomijdende maatregelen kan negatieve effecten hebben op de kansen voor academici. Een mogelijkheid is dat academici daardoor de stap naar het buitenland of bedrijfsleven maken. Er zit dus een spanning in de financiële incentivestructuur van de universiteiten, de academische autonomie van individuele academici en het veiligheidsperspectief.

174 (VSNU, 2021, pp. 14–15)

Bijlage 5 Referenties

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

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

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

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

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

- van der Meulen, B. en Rip, A. (1998) ‘Mediation in the Dutch science system’, *Research Policy*, 27(8), pp. 757–769. doi:10.1016/S0048-7333(98)00088-2.
- Minister van Buitenlandse Zaken (2021) *Recente ontwikkelingen in China en de situatie in Xinjiang*.
- Minister van EZK (2022) *Het belang van het Nederlandse vestigings- en ondernemingsklimaat*.
- Minister van OCW (2022a) *Afschrift brief aan kennisinstellingen inzake implementatie Nationale Leidraad Kennisveiligheid*.
- Minister van OCW (2022b) *Werken aan een sectorbeeld Kennisveiligheid*, *Officiele bekendmakingen*.
- Minister van OCW, Minister van EZK, en Minister van J&V (2022) *Voortgang en vooruitblik aanpak kennisveiligheid hoger onderwijs en wetenschap*.
- Minister van OCW, Minister van J&V, en Staatssecretaris van EZK (2020) *Kennisveiligheid hoger onderwijs en wetenschap*.
- Ministerie van Buitenlandse Zaken (2018) ‘Handboek Strategische Goederen en Diensten’. Rijksoverheid. Beschikbaar op: www.rijksoverheid.nl/exportcontrole (Geraadpleegd: 1 april 2022).
- Ministerie van Buitenlandse Zaken (2019) *Nederland-China: een nieuwe balans*.
- Ministerie van Defensie (2019) ‘ABDO Algemene Beveiligingseisen voor Defensieopdrachten 2019’. Ministerie van Defensie.
- Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid (2022a) ‘Besluit toepassingsbereik sensitieve technologie’. Rijksoverheid. Beschikbaar op: https://www.internetconsultatie.nl/sensitievetechnologievifo/ (Geraadpleegd: 28 september 2022).
- Ministerie van Economische Zaken en Klimaat en Ministerie van Justitie en Veiligheid (2022b) *Wet van 18 mei 2022, houdende regels tot invoering van een toets betreffende verwervingsactiviteiten die een risico kunnen vormen voor de nationale veiligheid gezien het effect hiervan op vitale aanbieders, beheerders van bedrijfscampussen of ondernemingen die actief zijn op het gebied van sensitieve technologie (Wet veiligheidstoets investeringen, fusies en overnames)*, *Staatsblad*.
- Ministerie van Justitie en Veiligheid (2022) ‘Strafbaarstelling spionage gemoderniseerd’, *Rijksoverheid.nl*, 28 februari. Beschikbaar op: https://www.rijksoverheid.nl/actueel/nieuws/2022/02/28/strafbaarstelling-spionage-gemoderniseerd?msclkid=a33c7425bb3a11ec95caff439b37de90 (Geraadpleegd: 1 maart 2022).
- MIVD (2022) *Openbaar Jaarverslag 2021*. Jaarverslag. Den Haag, Militaire Inlichtingen- en Veiligheidsdienst, Ministerie van Defensie.

- Molthof, L., Zandee, D. en Cretti, G. (2021) *Unpacking open strategic autonomy. From concept to practice*. Den Haag, Netherlands Institute of International Relations 'Clingendael'.
- Monitoring Commissie Accountancy (2020) 'Spiegel voor de accountancysector Veel problemen zijn helemaal niet nieuw, ze keren alleen telkens terug'.
- Müller, J. en Potters, L. (2019) *Future technology for prosperity: Horizon scanning by Europe's technology leaders*. Luxembourg: Publications Office of the European Union.
- Muneer, F. (2022) 'Cybersecurity Capability Maturity Model (C2M2)'. U.S. Department of Energy en Office of Cybersecurity, Energy Security and Emergency Response.
- Myklebust, J.P. (2022) 'Researcher arrested on suspicion of being a Russian spy', *University World News. The Global Window on Higher Education*, 28 oktober. Beschikbaar op: https://www.universityworldnews.com/post.php?story=20221026105932263 (Geraadpleegd: 28 oktober 2022).
- National Security Commission on Artificial Intelligence (2021) *Final Report National Security Commission on Artificial Intelligence*. Beschikbaar op: https://www.nscai.gov/2021-final-report/ (Geraadpleegd: 25 oktober 2022).
- Nouwens, M. en Legarda, H. (2018) *China's pursuit of advanced dual-use technologies*. Research paper. London, Internationaal Instituut for Strategische Studies, p. 43. Beschikbaar op: https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance (Geraadpleegd: 20 augustus 2022).
- OECD (2022) *Integrity and security in the global research ecosystem*. Parijs, OECD Science, Technology and Industry.
- Pheijffer, M. (2021) 'Waarom ik blijf schrijven over accountants en fraude', *Financieele Dagblad*, 1 december.
- Pols, M. (2020) 'Commissievoorzitter: "Accountants hebben niet goed genoeg in de spiegel gekeken"', *Financieele Dagblad*, 14 januari.
- Pols, M. (2022) 'Het blijft wachten op de echte verbeteringen in accountancy', *Financieele Dagblad*, 21 juli.
- Rathenau Instituut (2021) *Kennisveiligheid in hoger onderwijs en wetenschap. Een gedeelde verantwoordelijkheid*. Den Haag, Rathenau Instituut.
- Roet, J. (2022) 'Ministers zoeken derde landen, hervormen research assessment en bekritiseren uitvoering missies', *Neth-ER*, 16 juni. Beschikbaar op: https://www.neth-er.eu/onderzoek/ministers-zoeken-derde-landen-hervormen-research-assessment-en-bekritiseren-uitvoering-missies (Geraadpleegd: 16 april 2022).

- Science Europe (2022) *A Values Framework for the Organisation of Research*. Brussel, Science Europe AISBL. Beschikbaar op: https://zenodo.org/record/6637847 (Geraadpleegd: 15 november 2022).
- ScienceGuide (2022a) '"Generieke maatregelen kennisveiligheid onnodige bureaucratie"', *ScienceGuide*, 9 september. Beschikbaar op: https://www.scienceguide.nl/2022/09/generieke-maatregelen-kennisveiligheid-onnodige-bureaucratie/ (Geraadpleegd: 10 september 2022).
- ScienceGuide (2022b) 'Regeringspartijen willen strenger toezicht op aanpak kennisveiligheid door universiteiten', *ScienceGuide*, 16 september. Beschikbaar op: https://www.scienceguide.nl/2022/09/regeringspartijen-willen-strenger-toezicht-op-aanpak-kennisveiligheid-door-universiteiten/ (Geraadpleegd: 16 september 2022).
- Scientific integrity fast-track action committee (2022) *Protecting the integrity of government science*. Washington, DC, National Science and Technology Council.
- Shih, T. (2022) 'Recalibrated responses needed to a global research landscape in flux', *Accountability in Research*, pp. 1–7. doi:10.1080/08989621.2022.2103410.
- Snetselaar, D. (2022) 'DREAMS Lab: assembling knowledge security in Sino-Dutch research collaborations', *European Security*, pp. 1–19. doi:10.1080/09662839.2022.2127317.
- Spain en Netherlands (2021) 'Spain-Netherlands non-paper on strategic autonomy while preserving an open economy'. Permanent representation. Beschikbaar op: https://www.permanentrepresentations.nl/documents/publications/2021/03/24/non-paper-on-strategic-autonomy (Geraadpleegd: 15 april 2022).
- Stone, G.R. *e.a.* (2022) *Report of the Committee on Freedom of Expression*. Chicago, University of Chicago.
- Sue-Yen Tjong Tjin Tai *e.a.* (2018) *Bedrijf zoekt universiteit. De opkomst van strategische publiek-private partnerships in onderzoek*. Den Haag, Rathenau Instituut.
- Teer, J. (2021) *Kennissamenwerking met onvrije landen in een tijd van harde competitie tussen grootmachten: de militaire dimensie*. Den Haag, The Hague Centre for Strategic Studies.
- Teer, J. (2022) *China's militaire opkomst en Europese technologie*. Den Haag, Hague Centre for Strategic Studies. Beschikbaar op: https://www.jstor.org/stable/resrep40031 (Geraadpleegd: 1 augustus 2022).
- The University of Copenhagen *e.a.* (2022) 'The EVALUATE framework and handbook. Harnessing the power of evaluation to build better international strategic partnerships between universities'. The University of Edinburgh.
- UKRI (2021) 'Trusted Research and Innovation Principles'. UK Research and Innovation.

- Universiteiten van Nederland *e.a.* (2022) 'Nationale leidraad kennisveiligheid. Veilig internationaal samenwerken'. Rijksoverheid. Beschikbaar op: https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid (Geraadpleegd: 4 maart 2022).
- Van den Broek, J. (2022) 'Opinie | Deep tech moet de ruimte krijgen in Nederland - NRC', *NRC*, 15 september.
- Van der Dool, P. (2022) '"Het bagatelliseren van dreigingen is geen basis voor beleid"', *NRC*, 4 september.
- Van der Woude, H. en Van der Molen, H. (2022) *Motie van de leden Van der Woude en Van der Molen over de risicoanalyse kennisveiligheid op systematische wijze laten uitvoeren door de instellingen*.
- Versteegh, K. (2022) 'Juristen en oud-spionnen zijn het een keer eens: die nieuwe wet tegen spionage deugt niet', *NRC*, 24 juli, p. 4.
- VSNU (2021) *Kader Kennisveiligheid Universiteiten*. Den Haag, Vereniging van Universiteiten.
- Wellerstein, A. (2021) *Restricted data: the history of nuclear secrecy in the United States*. Chicago: The University of Chicago Press.
- van der Wende, M. en Kirby, W.C. (2020) *China and Europe on the New Silk Road: Connecting Universities Across Eurasia*. Oxford university press.
- van Wijnen, J.F. (2022) 'Wetenschappers zijn bang voor hun toekomst door Googles superieure computer', *Financieele Dagblad*, 1 juli, p. 5.
- World University Service (1989) 'The Lima Declaration on Academic Freedom and Autonomy of Institutions of Higher Education'. World University Service.
- Xie, Y. *e.a.* (2022) 'Caught in the Crossfire: Fears of Chinese-American Scientists', *Physics and Society*, p. 16. doi:arXiv:2209.10642.

Awti Adviesraad voor wetenschap, technologie en innovatie

Adviesraad voor wetenschap, technologie en innovatie
Prins Willem-Alexanderhof 20
2595 BE Den Haag
t. 070 3110920
e. secretariaat@awti.nl
w. www.awti.nl