Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

Nr. 1108

BRIEF VAN DE MINISTER VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 maart 2024

Hoger onderwijs en wetenschap van wereldklasse kunnen niet zonder internationale samenwerking en wetenschappelijk talent van over de hele wereld. Tegelijkertijd zetten statelijke actoren kennis en innovatie steeds vaker in als strategisch machtsmiddel naast of in combinatie met klassieke middelen, zoals spionage. De inzet daarvan kan een bedreiging vormen voor onze nationale veiligheid, Europese waarden en voor de kennissector zelf. Het Dreigingsbeeld Statelijke Actoren 2 laat zien dat Nederlandse kennisinstellingen en wetenschappers doelwit zijn van diverse (digitale) aanvalscampagnes om hoogwaardige technologie buit te maken, en dat kennis en technologie ook op reguliere wijze worden verkregen, bijvoorbeeld via academische samenwerkingen.[1] Daarom werkt het kabinet samen met de kennissector aan het verbeteren van de kennisveiligheid.

Met de kabinetsbrede aanpak kennisveiligheid hoger onderwijs en wetenschap[2] zet het kabinet in op het voorkomen van ongewenste overdracht van kennis en technologie. Ook ziet de aanpak toe op het tegengaan van heimelijke beïnvloeding en bewustwording over samenwerkingen met personen en instellingen uit landen waar grondrechten niet worden gerespecteerd. Daarbij zoeken we steeds de balans tussen enerzijds de kansen en noodzaak van open internationale samenwerking en anderzijds het beschermen van de nationale en EU-belangen, de nationale veiligheid, onze kennis, technologie, waarden en weerbaarheid. Excellente wetenschap kan niet zonder internationale samenwerking. Tegelijkertijd moeten we ons verhouden tot toenemende dreigingen bij internationale samenwerkingen die de nationale veiligheid kunnen schaden.

[1] Dreigingsbeeld Statelijke Actoren 2. AIVD, MIVD en NCTV, november 2022 (bijlage bij Kamerstuk 30 821, nr. 175).
[2] Deze is van start gegaan in 2022. Zie Kamerstuk 31 288, nr. 894.

kst-31288-1108
ISSN 0921 - 7371
's-Gravenhage 2024

Om deze dreigingen tegen te gaan, is de aanpak kennisveiligheid opgenomen in de in april 2023 gepubliceerde Veiligheidsstrategie voor het Koninkrijk der Nederlanden 2023–2029. De aanpak kennisveiligheid is een integraal onderdeel van de interdepartementale aanpak tegen statelijke dreigingen, waarin ook aandacht aan economische veiligheid wordt besteed.[3]

Met deze brief informeer ik uw Kamer, mede namens de Minister van Justitie en Veiligheid en de Minister van Economische Zaken en Klimaat, over de voortgang van de aanpak kennisveiligheid.

Lerende aanpak

Kennisinstellingen[4] en Rijksoverheid zijn gezamenlijk verantwoordelijk voor het realiseren van kennisveiligheid. Eén van de uitgangspunten van de aanpak kennisveiligheid is zelfregulering en het bevorderen van bewustwording door de instellingen en bij onderzoekers. De kennisinstellingen zijn primair aan zet bij veilig internationaal samenwerken. Zij staan voorop bij het beschermen en bevorderen van academische kernwaarden. Ook zijn zij in de positie om te weten waar kansen voor wetenschappelijke ontwikkeling en internationale samenwerking zich voordoen. In die context doen zich ook risico's voor: risico's die afbreuk doen aan de integriteit van de wetenschap of de nationale veiligheid. De kennisinstellingen staan voor de opgave om kansen en risico's tegen elkaar af te wegen.

De Rijksoverheid helpt de instellingen waar het kan. Denk bijvoorbeeld aan de Nationale Leidraad Kennisveiligheid die samen met de sector is opgesteld, met het Loket Kennisveiligheid en de bestuurlijke dialoog. Waar de risico's het grootst zijn en de nationale veiligheid mogelijk in gevaar komt, stelt de Rijksoverheid kaders en bindende voorschriften. Ook treedt de Rijksoverheid op wanneer instellingsbesturen hun verantwoordelijkheid niet waar kunnen maken, of als daarvoor een informatiepositie nodig is die buiten hun bereik ligt.

Het beschermen van belangen, het nemen van maatregelen en het afwegen van kansen en risico's is een complexe opgave, zeker in een geopolitieke context die veranderlijk is. De Rijksoverheid en de kennissector kiezen bij kennisveiligheid daarom voor een gezamenlijke, lerende aanpak. Die lerende aanpak zien we ook terug in de verschillende aspecten en instrumenten van het kennisveiligheidsbeleid.

Voortgang aanpak kennisveiligheid

Hieronder schets ik de voortgang op de afzonderlijke maatregelen in de drie lijnen waarlangs het kabinet de aanpak kennisveiligheid heeft ingezet: 1) bevorderen bewustzijn en zelfregulering; 2) screening kennisveiligheid; en 3) inzet EU en internationaal.

I. Bevorderen bewustzijn en zelfregulering

In het Bestuursakkoord hoger onderwijs en wetenschap van juli 2022 heb ik met de universiteiten en hogescholen afgesproken dat zij de Nationale Leidraad Kennisveiligheid implementeren.[5] Daarbij is het van belang dat

---

[3] Kamerstuk 30 821, nr. 178, bijlage. Veiligheidsstrategie voor het Koninkrijk der Nederlanden.
[4] De universiteiten inclusief de umc's, de hogescholen, de TO2-instellingen en de onderzoeksinstituten van KNAW en NWO.
[5] Bestuursakkoord Hoger Onderwijs en Wetenschap, juli 2022 (Bijlage bij Kamerstuk 31 288, nr. 969).

we met elkaar de voortgang bewaken en tempo blijven maken. De voortgang maak ik op twee manieren inzichtelijk. De eerste is met de uitvoering van de externe audit kennisveiligheid: een nulmeting van hoe ver kennisinstellingen gevorderd zijn met de implementatie. Deze meting levert in 2023 en 2024 drie sectorbeelden op: over de universiteiten die uw Kamer eind vorig jaar ontving[6]; over de hogescholen die ik uw Kamer bij deze brief toezend; en over de NWO- en KNAW-instituten die uw Kamer voor de zomer ontvangt. Ik bespreek de resultaten van de sectorbeelden onder andere met de raden van toezicht van de universiteiten en hogescholen om de voortgang te bewaken. In 2025 wordt de meting herhaald.

Ten tweede ben ik met Universiteiten van Nederland (UNL) en de Vereniging Hogescholen (VH) in gesprek over indicatoren die voor instellingen goed meetbaar zijn en voldoende kunnen zeggen over de voortgang van het beleid. Daarbij denk ik bijvoorbeeld aan het percentage instellingen met een portefeuillehouder kennisveiligheid in het college van bestuur; het percentage instellingen met een adviesteam kennisveiligheid; het percentage instellingen dat in de afgelopen drie jaar een risicoanalyse kennisveiligheid heeft uitgevoerd; en het percentage instellingen dat gerichte bewustwordingsactiviteiten over kennisveiligheid uitvoert. Ik streef ernaar de definitieve indicatoren nog voor de zomer vast te stellen en zal uw Kamer hierover informeren.

Sectorbeelden

Universiteiten

Het Sectorbeeld kennisveiligheid universiteiten, dat ik in oktober 2023 met uw Kamer deelde,[7] liet zien dat de universiteiten belangrijke stappen hebben gezet met het implementeren van maatregelen en dat kennisveiligheid nu een vaste waarde is binnen de universiteiten. Een uitkomst van het sectorbeeld was echter dat universiteiten nog niet beschikken over overzichten van internationale partnerschappen op centraal niveau. Universiteiten zijn gestart met het maken van deze overzichten. Middels de begeleidende brief van het Sectorbeeld heb ik uw Kamer geïnformeerd over de obstakels die zij hierbij tegenkomen. Ik heb UNL gevraagd om mij dit voorjaar nog te informeren over de aanpak die de universiteiten kiezen bij het werken aan de overzichten en daarbij een tijdpad te schetsen.[8] Met UNL blijf ik in gesprek over hoe ik de universiteiten daarin kan ondersteunen.

Hogescholen

Ook bij de hogescholen is inmiddels een nulmeting gedaan. Het Sectorbeeld kennisveiligheid hogescholen (bijlage 1) geeft de resultaten weer. Uit dit Sectorbeeld blijkt dat de aandacht voor kennisveiligheid bij hogescholen sinds 2022 in een stroomversnelling is geraakt. Met name de grotere hogescholen hebben belangrijke stappen gezet met het implementeren van maatregelen. Tegelijkertijd is er een aantal hogescholen dat de relevantie van het kennisveiligheidsbeleid voor hun instelling lager inschat, omdat zij geen sensitief onderzoek doen, geen internationale partnerschappen hebben of nauwelijks buitenlandse werknemers en studenten hebben.

---

[6] Kamerstuk 31 288, nr. 1077.
[7] Kamerstuk 31 288, nr. 1077.
[8] Zie ook het verslag van een schriftelijk overleg over het sectorbeeld. Kamerstuk 31 288, nr. 1105.

Er gaat veel goed. Meer dan de helft van de hogescholen heeft restrictief toegangsbeleid voor bepaalde ruimtes. Daarnaast heeft het merendeel van de hogescholen beleid omtrent restrictieve toegang voor bepaalde onderzoeksgegevens en documenten. De meerderheid van de hogescholen heeft aandacht voor kennisveiligheid als onderdeel van het personeelsbeleid. Ruim twee derde (26 van de 37) van de hogescholen heeft een risicoanalyse uitgevoerd.

Er moeten ook zaken beter, want elf hogescholen hadden op het moment van de meting nog geen risicoanalyse uitgevoerd. Ook laat het Sectorbeeld zien dat nog niet alle hogescholen over een bestuurlijk portefeuillehouder en adviesteam kennisveiligheid beschikken, terwijl ik hierover afspraken met de hogescholen heb gemaakt in het Bestuursakkoord. Dat de mate van beleidsontwikkeling bij hogescholen sterk uiteenloopt is deels te verklaren door de grote diversiteit die het hbo kenmerkt. Risicoprofielen kunnen daardoor sterk verschillen en maatregelen moeten proportioneel zijn. Toch moeten die risico's dan wel eerst in beeld worden gebracht.

Ik heb met de VH gesproken over uitkomsten van het Sectorbeeld. Een schriftelijke reactie van de VH treft uw Kamer als bijlage aan (bijlage 2). De VH heeft aangekondigd bij alle hogescholen na te gaan of er concrete vervolgstappen zijn gezet naar aanleiding van de nulmeting. Als blijkt dat de gemaakte afspraken in het Bestuursakkoord nog niet zijn nageleefd zal de VH mij hierover uiterlijk in september 2024 informeren. Ik zal de bestuurders aanspreken die de afspraken dan nog niet zijn nagekomen. Daarnaast heeft de VH de hogescholen gevraagd om ervoor te zorgen dat zij inzicht hebben in eventueel risicovolle internationale partnerschappen, en voor zover zij dit nog niet hebben, dit uiterlijk in voorjaar 2025 te realiseren.

Verder neem ik de uitkomsten van dit Sectorbeeld mee in de eerder aangekondigde actualisatie van de Nationale Leidraad Kennisveiligheid, want de VH vraagt terecht aandacht voor specifieke uitdagingen waar de hogescholen voor staan. Tot slot nodigt dit Sectorbeeld uit om na te denken over hoe de landelijke aanpak van kennisveiligheidsbeleid verder gedifferentieerd kan worden. Dit neem ik mee in de verkenning naar de mogelijke ontwikkeling van een *capability maturity model* op het gebied van kennisveiligheid.[9] Over de uitkomsten van deze verkenning informeer ik uw Kamer rond de zomer van dit jaar.

CSC-beurzenprogramma

Verantwoorde internationale wetenschappelijke samenwerking vraagt van kennisinstellingen dat zij kansen pakken en internationale samenwerkingen aangaan en tegelijkertijd zicht hebben en houden op eventuele risico's en afhankelijkheden die zich daarbij voordoen. Dit vergt een afweging tussen de kansen en risico's bij iedere samenwerkingsvorm. Een voorbeeld hiervan is de samenwerking met Chinese wetenschappers. Wetenschappelijke samenwerking met China is belangrijk voor Nederland. China en Nederland kunnen elkaar op sommige wetenschappelijke en technologische gebieden enorm vooruithelpen. Daarom tekenden de Minister van EZK en ik afgelopen jaar een Memorandum of Understanding (MoU) over Science, Technology and Innovation met de Chinese Minister van Science and Technology.[10] Dit MoU, dat in zijn aard

[9] Naar aanleiding van het AWTI-advies *Kennis in conflict – veiligheid en vrijheid in balans* doe ik een verkenning naar een vorm van monitoring waarbij de mate van volwassenheid van beleid in beeld kan worden gebracht.

[10] Stcrt. 2023, nr. 27504

niet-bindend is, biedt een algemeen kader voor wederkerige samenwerking waarbij Nederland verschillende academische kernwaarden als uitgangspunt voor onderwijs- en onderzoekssamenwerking heeft opgenomen.[11]

Tegelijkertijd zijn ook vragen gesteld over de inzet van internationale beurspromovendi die in Nederland aan een onderzoek werken op basis van het beurzenprogramma van de Chinese Scholarship Council (hierna: CSC). Naar aanleiding van mediaberichten en de daaropvolgende Kamervragen van het lid Van der Woude heb ik dit programma laten onderzoeken door Instituut Clingendael.[12] Het onderzoeksrapport is bijgevoegd bij deze brief (bijlage 3). Ik ga hieronder in op de conclusies en aanbevelingen.

Naar schatting ontvangen zo'n 3.800 buitenlandse promovendi in Nederland een internationale beurs met als doel de doctorstitel te behalen.[13] Iets meer dan de helft hiervan ontvangt een beurs van CSC – ongeveer 2.000. Deze promovendi worden gezien als waardevolle onderzoekers die een belangrijke bijdrage leveren aan de wetenschap. Het rapport wijst uit dat er landelijk en op instellingsniveau geen financiële of wetenschappelijke afhankelijkheid is van het CSC-beurzenprogramma. Wel bestaat bij elf afdelingen en faculteiten meer dan 15 procent van het totale aantal internationale promovendi uit CSC-bursalen. Dit laatste zie ik als een kwetsbaarheid en ik ga met instellingen in gesprek over de vraag hoe zij dit soort afhankelijkheden denken te gaan beperken. Dit heeft voor mij prioriteit.

CSC heeft met enkele Nederlandse universiteiten overeenkomsten gesloten. Deze overeenkomsten bevatten geen politieke voorwaarden. In contracten met individuele promovendi, dat wil zeggen tussen de staat en de promovendus, worden wel voorwaarden gesteld waardoor zij kwetsbaar kunnen zijn voor druk vanuit hun thuisland. Ik wil niet treden in contracten met individuen. Wel kan ik, samen met de Nederlandse kennisinstellingen, de voorwaarden creëren om zorgvuldig met veiligheidsrisico's om te gaan.

De onderzoekers adviseren om de instellingen kaders en richtlijnen mee te geven over omgang met CSC-beurzen. Ze adviseren ook om op landelijk niveau een overleg met CSC te organiseren over de voorwaarden voor beursverstrekking en deze ook te agenderen in Europese samenwerkingsverbanden. Het rapport beveelt daarnaast aan om gecertificeerde vertalingen van relevante CSC-documenten te publiceren. Tot slot wordt geadviseerd kennisinstellingen te stimuleren om te diversifiëren in financiering van promovendi en ze aan te moedigen om na te denken over het voorkomen van risicovolle strategische afhankelijkheden in de samenwerking met China.

Ik ga graag – samen met de kennisinstellingen – aan de slag met deze aanbevelingen. Mijn inzet is om de instellingen te ondersteunen bij het maken van risico-afwegingen met betrekking tot kennisveiligheid. Het Loket Kennisveiligheid speelt hierin nu al een belangrijke rol. Het rapport

---

[11] Deze waarden worden tegenwoordig ook opgenomen in andere MoU's op het gebied van onderwijs en wetenschap. Andere voorbeelden zijn de lopende vernieuwing van het MoU met het Ministry of Education van China en gesprekken over MoU's en Letter of Intents met Zwitserland, Zuid-Korea en Indonesië.

[12] Kamerstuk 31 288, nr. 1030.

[13] In 2021 waren 36.472 promovendi verbonden aan Nederlandse universiteiten en universitair medische centra. 55 procent van alle promovendi komt uit het buitenland. Hiervan komt 56 procent van buiten de EER; dat zijn circa 11.000 buitenlandse promovendi (bron: Rathenau Instituut).

biedt ook goede aanknopingspunten om te kijken of er meer instrumenten voor de kennisinstellingen nodig zijn voor de omgang met beurspromovendi uit China of andere risicolanden op het gebied van kennisveiligheid. Na de zomer informeer ik uw Kamer over de resultaten.

Verder meldt het rapport dat deze beurspromovendi te weinig financiële middelen van CSC ontvangen om zelfstandig te voorzien in hun levensonderhoud. Universiteiten werken in UNL-verband op dit moment aan de verbetering van de positie van internationale beurspromovendi, onder andere door het opstellen van een voorlichtingsdocument voor internationale beurspromovendi als verbetering van de informatievoorziening. Over de positie van buitenlandse beurspromovendi heb ik reeds in december 2023 uw Kamer geïnformeerd.[14] Ik heb daarbij aangekondigd in gesprek te zullen gaan met UNL. In dit gesprek zal ik ook de aanbevelingen van Instituut Clingendael betrekken, zoals het diversifiëren in de financiering van promovendi. Verder zal ik in de bilaterale relatie met China op verschillende niveaus blijven uitdragen dat we zowel mogelijkheden als risico's van de samenwerking zien.

Loket Kennisveiligheid

Het Loket Kennisveiligheid speelt een belangrijke rol in de aanpak kennisveiligheid. Begin 2022 is het Loket geopend als het landelijke expertise- en adviespunt voor kennisveiligheid. Het loket heeft inmiddels meer dan 380 vragen beantwoord en adviezen verstrekt. De meeste vragen hebben betrekking op internationale samenwerking met partijen afkomstig uit China, Iran, Rusland en de Golfstaten. Dat de expertise- en adviesfunctie van het Loket in een behoefte voorziet laat het toenemend aantal vragen duidelijk zien. Ook worden de vragen van kennisinstellingen steeds complexer.

In 2023 lanceerde het Loket naast de advisering een nieuwe dienst voor medewerkers van kennisinstellingen: de *learning community* kennisveiligheid. De learning community organiseert netwerkevenementen, die naast het overbrengen van informatie, ook de onderlinge uitwisseling van ervaringen en *good practices* bevorderen. Zo zijn thematische bijeenkomsten en webinars georganiseerd over onder andere samenwerking met kennisinstellingen uit risicolanden op het gebied van kennisveiligheid, personeelsbeleid en het voorkomen van stigmatisering en discriminatie. De interesse in de bijeenkomsten die binnen de learning community worden georganiseerd is groot, met gemiddeld tachtig deelnemers per bijeenkomst. Daarnaast ontwikkelt het Loket praktische handvatten en middelen om kennisinstellingen in staat te stellen om goede risico-inschattingen te maken.

Ondanks de korte tijd dat het Loket bestaat, is het niet meer weg te denken als ondersteuning van kennisinstellingen bij de vormgeving en uitvoering van het kennisveiligheidsbeleid. Omdat kennisveiligheid een dynamisch en groeiend onderwerp is, ontwikkelt het Loket zijn werkwijze, diensten en kwaliteitsborging continu door.

Kennisveiligheidsdialoog

De kennisinstellingen, ondersteund door de Rijksoverheid, staan voor de opgave om kansen en risico's bij internationale samenwerking tegen elkaar af te wegen. Hoe dit in de praktijk vorm moet krijgen, wat men kan tegenkomen en wat daar precies aan ondersteuning voor nodig is, is op voorhand niet bekend. Daarvoor voeren we met elkaar een dialoog. Dit

[14] Kamerstuk 31 288, nr. 1098.

maakt het nauw samen optrekken door kennisinstellingen met de Rijksoverheid cruciaal en de aanpak succesvol. In 2023 heeft deze dialoog tussen de overheid en instellingen veelvuldig plaatsgevonden, onder andere over screening, en samenwerkingen tussen hoger onderwijs, wetenschap en het bedrijfsleven. Bestuurders geven aan de continue dialoog en afstemming te waarderen. Ik zet deze dan ook voort in 2024.

In oktober 2023 publiceerde de KNAW een *position paper* over kennisveiligheid. Hierin schetst de KNAW haar zorg dat de aanpak kennisveiligheid, met name de introductie van screening van wetenschappers, teveel ten koste zal gaan van open wetenschappelijke uitwisseling, academische vrijheid en institutionele autonomie. De KNAW pleit voor een aanpak die volledig berust op bewustwording en zelfregulering door kennisinstellingen, ondersteund door de overheid. Daarbij doet de KNAW een aantal suggesties voor verdere uitwerking van het kennisveiligheidsbeleid, zoals het maken van specifieke afwegingskaders per kennisdomein en het verder uitwerken van de verschillende betekenissen van kennisveiligheid.

Ik ben het eens met de KNAW dat het zwaartepunt van de kennisveiligheidsaanpak ligt bij risicomanagement door kennisinstellingen zelf, maar wil wel benadrukken dat Rijksoverheid en kennisinstellingen gezamenlijk verantwoordelijk zijn voor de tenuitvoerlegging van het kennisveiligheidsbeleid. Ik verschil echter met de KNAW van mening over de invoering van screening van onderzoekers op sensitieve vakgebieden. Hier heeft de Rijksoverheid een kaderstellende rol te spelen. Ik begrijp dat de screening alleen praktisch uitvoerbaar is als we heel precies kunnen aangeven waar de gevoeligheden liggen. Ik zal dit hieronder toelichten.

Het voorgenomen wetsvoorstel screening kennisveiligheid complementeert de bestaande kabinetsinzet door kaders te stellen voor studenten en onderzoekers van buiten de EU voor die vakgebieden waar vanwege de aanwezigheid van sensitieve technologie de risico's voor de nationale veiligheid het grootst zijn. Ik denk dat dit de juiste manier is om op een uniforme, onafhankelijke en zorgvuldige manier de persoonsgebonden risico's te kunnen adresseren. De Rijksoverheid raadpleegt daarvoor de expertise van de kennisinstellingen om precies vast te kunnen stellen welke kennis als sensitief beschouwd kan worden.

Alleen de Rijksoverheid heeft toegang tot alle relevante informatie – zoals bronnen uit het veiligheidsdomein – om tot een zo scherp mogelijke risico-inschatting te kunnen komen en dit op landelijk niveau gelijksoortig te beoordelen. Hierdoor wordt voorkomen dat verschillen in de wijze van screening ontstaan bij de verschillende kennisinstellingen, waardoor rechtsongelijkheid ontstaat. Bij screening vindt immers een risicobeoordeling plaats. Het belang van het individu en de open en vrije wetenschap wordt gewogen ten opzichte van het belang van nationale veiligheid. Dit is bij uitstek een taak van het Rijk. Daarbij wordt met een screening in de persoonlijke levenssfeer van de aanvrager getreden. Het is ook om die reden van belang te voorzien in een effectieve en uniforme wijze van rechtsbescherming en privacybescherming voor het individu.

Tegelijk snap ik de zorg die de KNAW heeft over het mogelijke bereik en de effecten van dit kader. Daarom is mijn inspanning nu gericht op het zorgvuldig en met precisie uitwerken van dit wetsvoorstel.

Nationale Leidraad Kennisveiligheid

Eerder kondigde ik aan de Nationale Leidraad Kennisveiligheid op een aantal punten te willen actualiseren. Uiteraard doe ik dat in samenwerking met de kennissector. Voor deze herziening leveren de Sectorbeelden

kennisveiligheid waardevolle inbreng. Ook neem ik de opbrengsten uit de bestuurlijke dialoog, uit het *position paper* van de KNAW, uit het AWTI-advies over kennisveiligheid van 2022, uit gesprekken over kennisveiligheid op Europees en Internationaal niveau en de signalen die we ontvangen via het Loket Kennisveiligheid zoveel als mogelijk mee. Ik streef naar het opleveren van een nieuwe versie van deze Leidraad in de tweede helft van dit jaar.

II. Screening kennisveiligheid: wettelijk kader tegen ongewenste kennis- en technologieoverdracht

Hieronder informeer ik uw Kamer over de voortgang op de uitwerking van de screening kennisveiligheid. Deze betreffen achtereenvolgens het bijgestelde tijdpad van het wetsvoorstel, een nadere invulling van de doelgroep, en de lopende afbakening van de sensitieve technologieën.

Tijdpad wetsvoorstel screening kennisveiligheid

In het schriftelijk overleg dat ik recent met uw Kamer voerde, heb ik aangegeven dat ik tempo wil maken met het wetsvoorstel. In dat kader heb ik uw Kamer geïnformeerd over het bijgestelde tijdpad van de voorgenomen wet screening kennisveiligheid. Daarin heb ik aangegeven het wetsvoorstel voor het zomerreces te willen publiceren voor internetconsultatie. Om het wetstraject te versnellen, zal het wetsvoorstel parallel aan de consultatie voor advisering worden voorgelegd aan in ieder geval de Autoriteit Persoonsgegevens (AP) en het Adviescollege toetsing regeldruk. Ook zal het wetsvoorstel parallel aan de internetconsultatie worden voorgelegd aan Justis voor de uitvoeringstoets, mits uit het nu lopende vooronderzoek van Justis naar voren komt dat zij de opdracht kan uitvoeren. De uitvoeringstoets zal onder meer inzicht geven in de tijd die nodig is voor de implementatie van het wetsvoorstel. Na de zomer ben ik voornemens om het wetsvoorstel aan te bieden aan de Raad van State voor advisering. Mijn streven is het wetsvoorstel vervolgens in de eerste helft van 2025 naar uw Kamer te sturen.

Nadere invulling doelgroep wetsvoorstel screening kennisveiligheid

De definitieve afbakening van de doelgroep staat nog niet vast, omdat ik nog in afwachting ben van het advies van het College voor de Rechten van de Mens over de voorlopig gekozen afbakening. Ik verwacht dit advies in maart 2024 te ontvangen. De voorgestelde afbakening betreft onderzoekers en (master)studenten van buiten de EU die in een zogenoemd risicovakgebied willen gaan werken of studeren in Nederland.

Wel kan ik nu melden dat ik voornemens ben om onderzoekers en studenten die reeds in Nederland verblijven en onderzoek doen of studeren en daarbij in aanraking komen met sensitieve technologie, buiten de doelgroep te laten. Het screenen van deze groep na inwerkingtreding van de wet levert strijd op het met het rechtszekerheidsbeginsel en is met het oog op de uitvoerbaarheid van het wetsvoorstel onwenselijk. Ook ben ik voornemens bachelorstudenten in beginsel uit te zonderen van de screening, omdat de lesstof in de bachelorfase van de studie niet als sensitief aan te merken is.

Afbakening sensitieve kennis en technologie

Een risico-gestuurd, afgewogen en effectief wetsvoorstel vereist een zorgvuldige afbakening van de sensitieve technologieën. Deze afbakening vindt getrapt plaats. Allereerst is voor het wetsvoorstel vereist dat daarin sensitieve technologieën in het kader van kennisveiligheid worden

benoemd. Dit is bijvoorbeeld ook zo gedaan bij de Wet veiligheidstoets investeringen, fusies en overnames.

Momenteel ben ik bezig met de uitvoering van deze eerste afbakeningsstap. Ik heb in 2022 advies gevraagd aan TNO om een eerste afbakening van sensitieve technologieën in het kader van de nationale veiligheid op te stellen. Met behulp van het advies van TNO heeft een interdepartementale werkgroep samen met experts een eerste concept sensitiviteitsbeoordeling gemaakt die voor feedback is voorgelegd aan de kennisinstellingen in de periode maart tot juni 2023. Dit heeft veel reacties opgeleverd, die zijn verwerkt in een herziene conceptbeoordeling. Op dit moment is deze herziene conceptbeoordeling in een tweede feedbackronde voorgelegd aan het kennisveld. Ook zijn begin dit jaar goed bezochte bijeenkomsten met experts uit het kennisveld gehouden over de technologiegebieden geavanceerde materialen, kunstmatige intelligentie (AI), biotechnologie en nanotechnologie.

Na de tweede feedbackronde wordt de sensitiviteitsbeoordeling vastgesteld en vindt besluitvorming plaats over op welke wijze de als sensitief beoordeelde technologieën zullen worden opgenomen in het wetsvoorstel screening kennisveiligheid. Dit wordt meegenomen in de consultatieversie van het wetsvoorstel. Daarna wordt de vertaalslag gemaakt naar het aanwijzen van risicovakgebieden. Dit kunnen opleidingen, vakgroepen, projectgroepen, studentenprojecten, en bijvoorbeeld ook bepaalde teams en laboratoria zijn. Over de manier waarop ik dit ga uitwerken, informeer ik uw Kamer als ik het wetsvoorstel voor internetconsultatie aanbied.

III. Inzet EU en internationaal

Nederland heeft het afgelopen jaar actief gewerkt aan de inzet op kennisveiligheid in de EU en internationaal en blijft dat doen. Een centraal element daarin is de inzet op een gelijk speelveld internationaal en specifiek in de EU. Nederland zet in op het uitwisselen van kennis en goede voorbeelden ter versterking van het kennisveiligheidsbeleid. Ook werken we aan een gedeeld internationaal beeld over kansen en risico's van internationale wetenschappelijke samenwerking. Dit gebeurt onder andere door het opbouwen, onderhouden en gebruik maken van een sterk netwerk met gelijkgezinde landen, zowel binnen als buiten de EU. De aanpak op kennisveiligheid is het effectiefst als andere landen ook beleid op kennisveiligheid voeren. Zo voorkomen we dat een potentiële risicovolle samenwerking zich verplaatst en zorgen we dat Nederland een aantrekkelijke plek blijft voor talent en wetenschappelijke samenwerking.

Nederland heeft in 2023 op Europees niveau een sturende en leidende rol gepakt. Dat is gedaan door onder andere sterk te pleiten voor een gezamenlijke EU-aanpak op kennisveiligheid. Nederland heeft bijeenkomsten georganiseerd voor kennisuitwisseling en netwerkvorming, zoals de kennisveiligheidsconferentie van Nederland en Duitsland in Berlijn voor zowel overheid als kennisinstellingen. Ook zijn er drie *Mutual Learning Exercises* met alle EU-lidstaten georganiseerd, waaronder een bijeenkomst in Den Haag voor het uitwisselen van kennisveiligheidsbeleid. Daarnaast is er door Nederland aan een EU-kopgroep gewerkt door met gelijkgezinde landen op dit onderwerp goede voorbeelden uit te wisselen en om gezamenlijk kennisveiligheid op de agenda te krijgen bij de Europese Commissie. Daarin wordt specifiek samengewerkt met Duitsland en Frankrijk.

De Nederlandse inzet, samen met die van gelijkgezinde landen, heeft in 2023 een aantal concrete resultaten opgeleverd. Zo was er een ministerieel debat over verantwoorde internationale wetenschappelijke samenwerking en kennisveiligheid tijdens de Raad voor Concurrentievermogen,[15] kwam kennisveiligheid specifiek voor in de bredere Europese Economische Veiligheidsstrategie[16] en is er de recent gepubliceerde EU-Raadsaanbevelingen over het verbeteren van kennisveiligheid waarover uw Kamer in een BNC-fiche een dezer dagen geïnformeerd wordt.[17] In deze Raadsaanbevelingen is opgenomen dat lidstaten een actieplan kennisveiligheid moeten opstellen in samenwerking met het kennisveld.

Daarnaast is er ook ingezet op internationale samenwerking met landen en netwerken buiten de EU, zoals de Verenigde Staten, het Verenigd Koninkrijk en Japan. Tot slot is het netwerk van Onderwijs- en Wetenschapsattachés en de Innovatieattachés onverminderd waardevol gebleken.

Deze attachés zorgen samen met de collega's op de Nederlandse ambassades voor versteviging en uitbreiding van de internationale samenwerking op kennisveiligheid.

De Minister van Onderwijs, Cultuur en Wetenschap,
R.H. Dijkgraaf

[15] https://data.consilium.europa.eu/doc/document/ST-8824–2023-REV-1/nl/pdf
[16] Kamerstuk 21 501–30, nr. 579
[17] https://research-and-innovation.ec.europa.eu/system/files/2024–01/ec_rtd_council-recommendation-research-security.pdf