Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

Nr. 1003

BRIEF VAN DE MINISTER VAN ONDERWIJS, CULTUUR EN WETENSCHAP

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 23 december 2022

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 van kennisveiligheid in hoger onderwijs en wetenschap.

In het afgelopen jaar zijn grote stappen gezet in deze aanpak door zowel kennisinstellingen als het kabinet. De basis is gelegd, en het is nu zaak het beleid door te ontwikkelen en implementeren. Daarom blijf ik me onverminderd inzetten op de aanpak van kennisveiligheid. Dit doe ik in gezamenlijke inspanning met de kennisinstellingen en de betrokken onderdelen van het Rijk.

In deze voortgangsbrief ga ik eerst in op de actuele ontwikkelingen met betrekking tot de nationale veiligheid waar kennisveiligheid onderdeel van uitmaakt. Vervolgens schets ik de voortgang op de afzonderlijke maatregelen langs de drie lijnen waarlangs het kabinet de maatregelen uit de aanpak kennisveiligheid in 2020[1] heeft ingezet:

I. Bevorderen bewustzijn en zelfregulering van kennisinstellingen, ondersteund door een landelijke infrastructuur:
   a) de Kennisveiligheidsdialoog;
   b) de Nationale Leidraad Kennisveiligheid;
   c) bestuurlijke afspraken, en
   d) het Loket Kennisveiligheid.
II. Toetsingskader ongewenste kennis- en technologie overdracht
III. Inzet EU en internationaal

Deze voortgangsbrief bevat tevens een beleidsreactie op het advies van de Adviesraad voor Wetenschap, Technologie en Innovatie (AWTI) over

[1] Kamerstuk 31 288, nr. 894.

kst-31288-1003
ISSN 0921 - 7371
's-Gravenhage 2022

kennisveiligheid: *Kennis in conflict: Veiligheid en vrijheid in balans*. Dit advies is als bijlage aan deze brief toegevoegd. Ik vind dat een goed gekozen titel voor dit advies. Het beste onderzoek, wetenschap en innovatie vereisen (internationale) samenwerking in vrijheid. Dat geldt zeker voor een land als Nederland. Tegelijkertijd bevestigt de AWTI dat we echt niet naïef mogen zijn in het aangaan van bepaalde internationale samenwerking.

Ontwikkelingen nationale veiligheid

Geopolitieke ontwikkelingen van afgelopen jaar zetten internationale samenwerking verder onder druk. Het nieuwe geopolitieke klimaat is guurder en instabieler. Dit beeld komt ook naar voren in de recente Kamerbrief Open Strategische Autonomie[2] en de Kamerbrief aanpak statelijke dreigingen[3]. Nederland en de Europese Unie worden hierdoor steeds vaker openlijk én heimelijk geconfronteerd met handelingen van statelijke actoren, die onze belangen, waaronder onze nationale veiligheid en Europese fundamentele waarden, kunnen schaden. Kennis en technologie worden door statelijke actoren ingezet om de eigen militaire, technologische, politieke en economische macht te vergroten. Ze zijn daarmee in toenemende mate een strategisch machtsmiddel geworden.

Dat statelijke actoren actief op zoek zijn naar kennis en technologie in Nederland bleek al uit het Dreigingsbeeld Statelijke Actoren (DBSA) uit 2020.[4] Het recente Tweede Dreigingsbeeld Statelijke Actoren (DBSA2)[5] herbevestigt 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 via bijvoorbeeld academische samenwerkingen. Door de verwerving van kennis en technologie vanuit statelijke actoren bestaat het risico op ongewenst eindgebruik wat onze nationale veiligheidsbelangen, maar ook economische belangen of innovatiekracht, kunnen aantasten. Daarnaast vormen diasporagemeenschappen en opposanten van autoritaire regimes doelwit van beïnvloeding en inmenging. Ook dat vindt plaats bij kennis- en onderwijsinstellingen.[6] Dit maakt dat kennisveiligheid onlosmakelijk verbonden is met onze nationale veiligheid. Kennisveiligheid is dan ook onderdeel van de brede aanpak tegen statelijke dreigingen[7] en wordt en expliciet wordt meegenomen in de Rijksbrede veiligheidsstrategie (RbVs) die het kabinet komend voorjaar zal uitbrengen.

De geopolitieke situatie en de risico's die dit met zich meebrengt, betekenen niet dat internationale samenwerking in hoger onderwijs, onderzoek en innovatie vermeden moeten worden. Integendeel, voor hoger onderwijs en wetenschap op topniveau is internationale samenwerking juist van essentieel belang. De strategische inzet van het kabinet richt zicht niet alleen op het beschermen van Nederland *(protect)*, maar ook op het behouden van onze vooraanstaande kennispositie en technologisch leiderschap door internationale en Europese coalities te verstevigen zodat internationale samenwerking ten behoeve van hoogtechnologische innovatie mogelijk blijft (*promote*). Het kabinet bevordert die internationale samenwerking dan ook op verschillende manieren. Bijvoorbeeld binnen het Fonds voor onderzoek en wetenschap

---

[2] Kamerstuk 21 501-02, nr. 2197.
[3] Kamerbrief aanpak statelijke dreigingen en aanbieding DBSA2, d.d. 28 november 2022.
[4] Kamerstuk 30 821, nr. 125.
[5] Dreigingsbeeld Statelijke Actoren 2, november 2022.
[6] Nationale Leidraad Kennisveiligheid, januari 2022, bijlage bij Kamerstuk 31 288, nr. 950.
[7] Kamerbrief aanpak statelijke dreigingen en aanbieding DBSA2, 28 november 2022.

via de matchingsregeling Horizon Europe, het bevorderen van deelname aan Europese Partnerschappen, Erasmus+, maar ook door gerichte kennis- en innovatiemissies naar de Verenigde Staten, Japan en Europese landen ter bevordering van verdere samenwerking.

In de ontwikkeling en uitvoering van het kennisveiligheidsbeleid moeten we blijvend op zoek naar de balans tussen enerzijds de kansen van open internationale samenwerking en anderzijds het beschermen van de nationale en EU-belangen, onze kennis, technologie, waarden en weerbaarheid. Dit vraagt om het doorontwikkelen van het kennisveiligheidsbeleid, in nauwe samenwerking met de kennisinstellingen, en via een lerende aanpak waarbij we continu kennis en ervaring uitwisselen.

Het doorontwikkelen van het kennisveiligheidsbeleid doen we langs de drie met elkaar samenhangende lijnen waarmee we de aanpak van kennisveiligheid zijn gestart: (1) het bevorderen van bewustzijn en zelfregulering binnen kennisinstellingen, met een overheid die hen daarbij ondersteunt; (2) Als overheid heldere kaders te stellen waar dat nodig is; en (3) werken aan een *level playing field* op het gebied van kennisveiligheid op internationaal niveau.

I Bevorderen bewustzijn en zelfregulering

In een sector waar instellingen in hoge mate autonoom zijn, is het bevorderen van bewustzijn en zelfregulering de eerste stap in de brede aanpak van kennisveiligheid. Kennisinstellingen hebben in het afgelopen jaar belangrijke stappen gezet, waar nodig ondersteund door de landelijke infrastructuur van de Rijksoverheid. Ik schets in deze paragraaf de voortgang per maatregel en blik vooruit op de komende periode.

a. Kennisveiligheidsdialoog

In 2022 is de eerder ingezette kennisveiligheidsdialoog voortgezet en uitgebreid. De eerste serie dialogen bestond uit individuele gesprekken met besturen van vrijwel alle Nederlandse kennisinstellingen. De dialoog is dit jaar verbreed naar dialogen met toezichthouders en beleidsmakers veiligheid van de kennisinstellingen. De dialoog is daarnaast verdiept naar onderlinge uitwisseling van kennis en ervaringen over kansen, risico's en instrumenten om op een verantwoordelijke manier internationale samenwerkingsrelaties aan te gaan.

De opkomst en betrokkenheid bij de dialoogsessies was groot, vanuit zowel universiteiten, hogescholen, TO2-instellingen als overige kennisinstellingen. Bestuurders zien de noodzaak om kennis en expertise op hun instelling te vergroten en werkwijzen te implementeren die passen bij de aard en inrichting van hun instelling. Voor veel instellingen is dit een nieuwe en veeleisende opgave waarvoor voldoende capaciteit moet worden vrijgemaakt. De middelen die uw Kamer met het gewijzigd amendement van de leden Van der Woude, Van der Molen en Van der Graaf beschikbaar heeft gesteld, dragen hier aan bij.[8] Om tot een snelle en gerichte besteding van deze middelen te komen, ten behoeve van het behouden van voldoende capaciteit en het vergroten van kennis en expertise, zal ik overleggen met de betrokken partijen.

Leren van en met elkaar staat centraal in deze serie kennisveiligheidsdialogen. Hiertoe is door de veldpartijen en Rijksoverheid het *netwerk kennisveiligheid* gelanceerd als het platform voor uitwisseling tussen kennisinstellingen. Tijdens de kick-off bijeenkomst kwamen 72 kennisvei-

[8] Kamerstuk 36 200 VIII, nr. 62.

ligheidscoördinatoren, leden van adviesteams en andere beleidsmakers van instellingen bij elkaar. Ook de verschillende betrokken onderdelen van de Rijksoverheid waren vertegenwoordigd. In het adviesrapport van de AWTI, wijst de raad er ook op dat de doorontwikkeling van het gezamenlijk leren en professionaliseren noodzakelijk is. Ik onderschrijf dit advies. Ik ben dan ook van mening dat alle kennisinstellingen dienen deel te nemen aan dit netwerk. Daarom ben ik voornemens om in 2023 het netwerk door te ontwikkelen tot een *learning community*. Hier wordt gezamenlijk gewerkt aan het verwerven en vergroten van de benodigde vaardigheden, handvatten, kennis en expertise door het uitwisselen van kennis en ervaring via doelgerichte trainingen en bijeenkomsten. Vanuit het Loket Kennisveiligheid zal dit netwerk worden gefaciliteerd en ondersteund. Met deze actie wil ik verdere invulling geven aan het advies van de AWTI om te komen tot een aanpak van kennisveiligheid die zowel verduidelijkt als differentieert. Een *learning community* draagt eraan bij om te komen tot maatregelen die proportioneel kunnen worden ingezet.

Zoals toegezegd aan uw Kamer, hadden de dialoogsessies met de toezichthouders tot doel het ophalen van een eerste beeld van de implementatie van de Nationale Leidraad Kennisveiligheid (hierna: leidraad) en de uitvoering van de risicoanalyses op internationale samenwerkingen en financieringsbronnen die daar onderdeel van uitmaakt.[9] Ik heb gesproken met de toezichthouders van hogescholen, met de voorzitters van de raden van toezicht van universiteiten, de voorzitter van de raad van toezicht van de Nederlandse Organisatie voor Wetenschap en Onderzoek (NWO) en de president van de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW). Daarnaast heeft de Minister van Economische Zaken en Klimaat (EZK) gesproken met de raden van toezicht van de TO2. De opbrengst van deze gespreken geef ik hieronder weer, bij de rapportage over deze onderdelen.

b. Nationale Leidraad Kennisveiligheid

De leidraad is door de Rijksoverheid en de kennissector gezamenlijk opgesteld en op 31 januari 2022 gepresenteerd. Het doel van de leidraad is om kennisinstellingen concrete handvatten te bieden bij het vormgeven van hun beleid op het gebied van kennisveiligheid. Bij de implementatie van de leidraad vertalen kennisinstellingen de richtlijnen naar interne processen en procedures waarmee een groeiend veiligheidsbewustzijn doordringt tot in de haarvaten van kennisinstellingen.

Uit gesprekken met raden van toezicht, en uit de dialoogsessies in het algemeen, blijkt dat instellingen het resultaat van hun inspanningen zichtbaar zien worden. Er zijn kennisveiligheidscoördinatoren aangesteld en adviesteams kennisveiligheid ingericht. Instellingen geven voorbeelden van concrete casussen waarbij zij een samenwerking met een onderzoeker of instelling bewust hebben afgewogen en er vervolgens voor hebben gekozen deze af te houden naar aanleiding van risico's op het gebied van kennisveiligheid. Daarbij gebruiken instellingen regelmatig de kennis- en expertise van het Loket Kennisveiligheid. Tegelijkertijd geven instellingen aan dat het tijd kost expertise op te bouwen, het beleid verder te implementeren en de urgentie tot op het niveau van individuele onderzoekers door te laten dringen. Met de uitvoering van de eerder aan uw Kamer toegezegde audit op de risicoanalyse en de implementatie van de leidraad zal concreet worden hoe ver kennisinstellingen zijn met de implementatie van de leidraad.

[9] Kamerstuk 31 288, nr. 943.

c. Bestuurlijke afspraken Kennisveiligheid

Op initiatief van het lid Van der Woude[10], dat breed gesteund werd door uw Kamer, heb ik kennisinstellingen opgeroepen een risicoanalyse van internationale samenwerkingsverbanden uit te voeren en daarover te rapporteren aan hun raad van toezicht.[11] Universiteiten en hogescholen hebben zich in het Bestuursakkoord Hoger Onderwijs en Wetenschap 2022 gecommitteerd aan de implementatie van de leidraad, de uitvoering van risicoanalyses en het participeren in een externe audit.[12] Uw Kamer heeft vervolgens de motie van de leden Van der Woude en Van der Molen aangenomen waarin wordt opgeroepen om de risicoanalyses op systematische wijze uit te laten voeren en om de externe audit uit te breiden met de uitkomsten en de aanpak van de risicoanalyses.[13] In het reguliere bestuurlijke overleg over kennisveiligheid met het kennisveld, de regiegroep kennisveiligheid, heb ik hiervoor aandacht gevraagd.

Risicoanalyse

Uit de dialogen met de raden van toezicht blijkt dat de meeste instellingen op bestuursniveau een scherper beeld hebben van de risico's op het gebied van kennisveiligheid. Besturen hebben daarbij niet alleen aandacht voor het risico van het weglekken van kennis, met name relevant in het bètadomein, maar zijn zich ook in toenemende mate bewust van het risico van beïnvloeding door statelijke actoren, ook in het alfa- en gammadomein. De risicoanalyses dragen bij aan het creëren van de randvoorwaarden voor kennisveiligheid binnen de bedrijfsvoering van instellingen, zoals het personeelsbeleid, inzicht in geldstromen en andere voorwaarden voor bestaande en nieuwe internationale samenwerkingen. Ik heb op basis van de dialogen ook geconstateerd dat niet alle instellingen zo ver zijn gekomen met de risicoanalyses als ik had verwacht. De AWTI wijst er in haar advies op dat betrokkenen binnen kennisinstellingen zich niet allemaal voldoende bewust zijn van de veranderde geopolitieke context waarin internationale wetenschappelijke samenwerking plaatsvindt. Dit maakt de voortzetting en uitbreiding van de kennisveiligheidsdialoog en de gevraagde risicoanalyses, met de ontwikkeling van het toetsingskader, in mijn ogen extra urgent. Ik heb kennisinstellingen daarom via Universiteiten van Nederland (UNL) en de Vereniging Hogescholen (VH) nogmaals opgeroepen de risicoanalyses versneld en systematisch op te pakken.[14] Met de financiële impuls die volgt uit het gewijzigd amendement van de leden Van der Woude, Van der Molen en Van der Graaf[15] vertrouw ik erop dat ook de kennisinstellingen die tot dit moment minder ver zijn gekomen de benodigde stappen versneld kunnen zetten. De aanpak en uitkomsten van de risicoanalyses worden daarnaast meegenomen in de externe audit, zoals uw Kamer heeft verzocht in de motie van de leden Van der Woude en Van der Molen.[16]

Externe audit

Zoals toegezegd tijdens het spoeddebat kennisveiligheid op 2 juni 2022 gaat een externe audit kennisveiligheid van start.[17] Met een aanbestedingsprocedure is onderzoeksbureau Oberon in samenwerking met Dialogic aangetrokken als uitvoerende partij. De voorbereidende

[10] Kamerstuk 31 288, nr. 943.
[11] Kamerstuk 31 288, nr. 950.
[12] Kamerstuk 31 288, nr. 969.
[13] Kamerstuk 31 288, nr. 979.
[14] Kamerstuk 31 288, nr. 950.
[15] Kamerstuk 36 200 VIII, nr. 62.
[16] Kamerstuk 31 288, nr. 979.
[17] Kamerstuk 31 288, nr. 966.

werkzaamheden zijn van start gegaan en de audit bij universiteiten start begin 2023, waarna de audits in het voorjaar bij de hogescholen starten. Met NWO en KNAW heb ik afgesproken dat in de tweede helft van 2023 ook bij hen een externe audit start.

Kennisinstellingen ontvangen elk een terugkoppeling van hun individuele resultaten. Het onderzoeksbureau levert daarnaast een sectorbeeld op met bevindingen op geaggregeerd niveau per type kennisinstelling (universiteiten; hogescholen; etc.). Ten behoeve van dit sectorbeeld wordt bij een selectie van kennisinstellingen een kwalitatief verdiepend onderzoek uitgevoerd. Het eerste sectorbeeld, dat van de universiteiten, kan ik rond de zomer met uw Kamer delen. Het sectorbeeld van de hogescholen deel ik bij de voortgangsrapportage in december 2023 met uw Kamer. Conform de motie van de leden Van der Woude en Van der Molen[18] ga ik komend jaar over de resultaten van de audits in gesprek met de besturen en de raden van toezicht van kennisinstellingen. Net als tijdens de dialoog, betrek ik daarbij ook de inlichtingen- en veiligheidsdiensten en de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV). Ik wil samen met hen kijken of de risicoanalyses verder aangescherpt kunnen worden en of we de leidraad kunnen door ontwikkelen. Ook ben ik van plan de audit in 2025 te herhalen zodat we scherp in beeld houden hoe het kennisveiligheidsbeleid binnen de instellingen wordt vormgegeven.

d. Loket Kennisveiligheid

In januari 2022 is het Loket Kennisveiligheid (hierna: loket) geopend als het landelijke expertise- en adviespunt voor kennisveiligheid. Expertise van de Ministeries van OCW, EZK, BZ, J&V en de inlichten- en veiligheidsdiensten worden gebundeld zodat kennisinstellingen één antwoord krijgen vanuit de overheid. Het doel van het loket is om bewustwording en zelfregulering in de sector te vergroten door het beantwoorden van vragen over internationale samenwerking en kennisveiligheid, het organiseren van bijeenkomsten met het veld en experts, en het ontwikkelen van handzame tools die door kennisinstellingen kunnen worden toegepast. Het loket draagt ook bij aan het gezamenlijk ontwikkelen van kennis, kunde en vaardigheden binnen de overheid. Het loket geeft kennisinstellingen feitelijke informatie op basis waarvan zij zelf een gedegen afweging kunnen maken. Op basis van de informatie die het van kennisinstellingen ontvangt, kan het loket risico's helpen inschatten. Indien er sprake is van hoge risico's kan het loket een kennisinstelling dringend adviseren deze te mitigeren, dan wel de samenwerking niet aan te gaan. De verantwoordelijkheid voor de uiteindelijke risico-inschatting en risicomitigatie ligt bij de kennisinstellingen zelf.

Het groeiende bewustzijn van kennisveiligheid, de implementatie van de leidraad en de uitvoering van risicoanalyses is zichtbaar in de toename van het aantal vragen dat wordt ingediend bij het loket. Sinds de opening van het loket zijn 148 vragen ingediend (d.d. 21 december 2022). Universiteiten en hogescholen dienen het vaakst een vraag in bij het loket. Het overgrote deel van de indieners zijn (kennis)veiligheidscoördinatoren van instellingen. De meeste vragen betreffen het wel of niet aangaan van een internationale samenwerking met een kennisinstelling of bedrijf (40) en het aangaan van een samenwerking met een onderzoeker verbonden aan een bepaalde buitenlandse instelling (39). De indiener heeft in veel gevallen naar aanleiding van de eigen risicoafweging zelf al twijfels over de samenwerking, maar vraagt het loket om meer informatie voor het maken van een definitieve afweging. Veel vragen (89) gaan over een samenwerking met partners uit China (52), Rusland (21) en Iran (16).

[18] Kamerstuk 31 288, nr. 979.

Thema's waarover veel vragen worden gesteld zijn dual-use[19] en sanctiewetgeving. Het blijkt voor kennisinstellingen lastig in te schatten wanneer een onderzoeksgebied geclassificeerd wordt als dual-use of om andere redenen sensitief is. De onderzoeksgebieden waar vragen over worden gesteld zijn erg divers, maar gaan vaak over sleuteltechnologieën. Voor veel indieners blijkt het onduidelijk welke internationale sancties precies gelden met betrekking tot kennisoverdracht. Er blijkt behoefte aan meer informatie over welke vakgebieden dual-use of sensitief zijn en welke sancties precies van toepassing zijn. Ik ben voornemens om hierover meer informatie met de kennisinstellingen te delen, bijvoorbeeld via het netwerk kennisveiligheid.

Naast het voortzetten van de laagdrempelige en snelle maatwerkadvisering, wordt vanuit het loket in 2023 ook ingezet op het versterken van de bewustwording, door de doorontwikkeling van het netwerk kennisveiligheid. Het loket organiseert daarvoor webinars en themasessies, ontwikkelt e-learning modules en organiseert trainingen. Vanuit het loket start daarnaast een bewustwordingscampagne om kennisveiligheid tot in de haarvaten van de kennisinstellingen door te laten dringen. Dit sluit aan op de aanbevelingen van de AWTI.

De internationale belangstelling voor onze ervaringen met het loket is groot. Verschillende landen volgen de ontwikkeling van het loket in Nederland met interesse en gebruiken het als inspiratie voor de eigen beleidsontwikkelingen. Een aantal landen werkt aan beleidsinstrumenten in lijn met het loket en de Verenigde Staten heeft recent aangekondigd een soortgelijk beleidsinitiatief op te zetten. Het loket is ook de inspiratie voor de pilot van een vergelijkbaar loket economische veiligheid voor bedrijven die werken met waardevolle (technologische) kennis en ook een expliciet doelwit vormen van statelijke actoren. Momenteel wordt verkend hoe dit loket kan worden opgezet. Het vergroten van het veiligheidsbewustzijn bij zowel kennisinstellingen als bedrijven bevordert bovendien de veiligheid daar waar sprake is van publiek-private samenwerking. Tot slot wordt door alle betrokken ministeries en organisaties gezamenlijk onderzocht hoe ongewenste kennis- en technologieoverdracht via bedrijven, onder meer via kennismigranten en bedrijven die erkend referent zijn, kan worden tegengegaan.

II Toetsingskader ongewenste kennis- en technologieoverdracht

De tweede stap in onze aanpak van kennisveiligheid is het stellen van heldere kaders, daar waar de risico's voor de nationale veiligheid het grootst zijn. Eerder heb ik uw Kamer gemeld dat het kabinet werkt aan een toetsingskader om ongewenste kennis- en technologieoverdracht tegen te gaan. Het gaat hierbij om de toetsing van individuen die als onderzoeker willen werken of willen studeren op kennisgebieden waar men toegang heeft tot kennis en technologie die risico's voor de nationale veiligheid met zich mee kunnen brengen, de risicovakgebieden. Denk bijvoorbeeld aan kennis die kan worden ingezet voor zowel civiele als militaire doeleinden (dual-use) of kennis en technologie die om andere redenen sensitief zijn in het licht van de nationale veiligheid. Het toetsingskader heeft tot doel sensitieve kennis en technologie beter te beschermen door aanstellingen van wetenschappers en toelating van studenten van buiten de Europese Unie tegen te gaan, in geval uit een toets blijkt dat er sprake is van een risico voor de nationale veiligheid.

[19] Dual-use betreft kennis die kan worden ingezet voor zowel civiele als militaire doeleinden.

In de Kamerbrief van 31 januari 2022[20] is aangegeven dat voor het toetsingskader een aantal vragen moet worden beantwoord met betrekking tot de doelgroep en de risicovakgebieden. Het antwoord op die vragen licht ik hieronder toe. Daarnaast zal ik vooruitblikken op wat in de komende periode aan verdere uitwerking noodzakelijk is voordat het toetsingskader in werking kan treden.

Juridische basis en doelgroep

De eerste vraag betrof de juridische basis voor de toetsing en de keuze voor de doelgroep. Zoals aangegeven in de voortgangsbrief van 31 januari 2022. heeft het kabinet onderzocht of een vorm van toetsing mogelijk is waarbij uitsluitend derdelanders, burgers van buiten de Europese Unie, worden getoetst. Deze variant lijkt proportioneel en doelmatig in het licht van de actuele dreigingsanalyses. Derdelanders die bij een Nederlandse kennisinstelling onderzoek willen gaan doen of een studie willen volgen en daarbij toegang krijgen tot een risicovakgebied zullen straks onderwerp zijn van een kennisveiligheidstoets. Met toegang tot een risicovakgebied wordt hier bedoeld dat de derdelander toegang tot of de beschikking krijgt over technologie die als sensitief in de zin van de nationale veiligheid is aangemerkt. De aanpak heeft een generiek karakter en kan worden toegepast op ieder land van buiten de Europese Unie waar een dreiging op het gebied van kennisveiligheid van uitgaat, zodat we voorbereid zijn op ontwikkelingen in het dreigingsbeeld.

Het is noodzakelijk om een wettelijke basis te creëren voor de kennisveiligheidstoets. Een toets zoals beoogd moet op zorgvuldige wijze bij wet worden geregeld, omdat met deze vorm van toetsing ongeacht de uitkomst in negatieve zin in de levens van burgers wordt ingegrepen. Deze vorm van toetsing die plaatsvindt voorafgaand aan de aanvraag voor een verblijfsvergunning is tevens nieuw. Om die reden is gebleken dat er geen bestaande wettelijke kaders zijn om bij aan te sluiten. De betrokken bewindspersonen zullen bij wet worden belast met de toets. Ook zal worden vastgelegd wat deze toets precies behelst. Daarbij moet tevens worden bezien welke waarborgen er gelden tegen de inbreuk op privacy en grondrechten en een grondslag worden gecreëerd voor de verwerking van (bijzondere) persoonsgegevens.

De resultaten van de kennisveiligheidstoets zullen worden betrokken bij de behandeling van de aanvraag om een verblijfsvergunning in het kader van onderzoek of studie. De Vreemdelingenwet 2000 bevat een grondslag om dergelijke aanvragen af te wijzen in geval van een gevaar voor de nationale veiligheid. De kennisveiligheidstoets zelf is geen vreemdelingrechtelijke toets, maar de uitkomst van de toets kan een indicator zijn dat er een gevaar voor de nationale veiligheid is.

Afbakening risicovakgebieden

De tweede vraag betrof de afbakening van de risicovakgebieden waarop het toetsingskader van toepassing wordt. Bij de afbakening van de risicovakgebieden wordt de vraag beantwoord welke kennis en technologie vanuit het oogpunt van nationale veiligheid risicovol is.

Voor een integrale benadering van de invulling van de vraag welke kennis en technologie risicovol is, is samen opgetrokken met de NCTV en het Ministerie van EZK. De vraag welke technologieën sensitief zijn in het licht van de nationale veiligheid speelt niet alleen bij het toetsingskader dat voor het tegengaan van ongewenste kennis- en technologieoverdracht via

[20] Kamerstuk 31 288, nr. 948.

kennisinstellingen wordt ontwikkeld, maar ook bij andere beleidsinstrumenten, zoals bij de investeringstoets in het kader van de Wet veiligheidstoets investeringen, fusies en overnames (hierna Wet Vifo)[21]. Voor de afbakening van deze sensitieve kennis en technologieën is OCW samen met het Ministerie van EZK een traject gestart met de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO). Hierbij ligt de focus op de risico's die kunnen ontstaan uit moedwillig en ongewenst gebruik of misbruik van de technologie.

Dit traject heeft vooralsnog geleid tot het ontwikkelen van een proces voor het benoemen van risicovakgebieden, onder meer ten behoeve van de verdere beleidsvorming rondom onder meer het toetsingskader. Momenteel wordt met gebruikmaking van het ontwikkelde proces onderzocht welke kennis en technologiegebieden ten grondslag zullen worden gelegd aan het toetsingskader, waarbij afstemming zal plaatsvinden met de inlichtingen- en veiligheidsdiensten, NCTV en relevante experts. Ook wordt feedback gevraagd van de kennisinstellingen. Zodra duidelijk is welke kennis- en technologiegebieden onder het toetsingskader zullen vallen worden de kennisinstellingen gevraagd in kaart te brengen waar de sensitieve kennis en technologieën zich binnen kennisinstellingen bevinden. Bij vragen of twijfelgevallen omtrent mogelijke sensitiviteit van een vakgebied kunnen de instellingen terecht bij het loket voor informatie.

Tot slot is van belang om op te merken dat technologie continu in ontwikkeling is. Een regelmatige herijking is daarom nodig. Na inwerkingtreding van het toetsingskader zal periodiek worden geëvalueerd en geactualiseerd. Over de verdere voortgang van de afbakening van de risicovakgebieden en over hoe deze periodieke actualisatie wordt uitgevoerd informeer ik uw Kamer in de eerste helft van 2023.

Uitvoerende partij toetsingskader

Voorzien is dat de toetsing op termijn namens de betrokken bewindspersonen uitgevoerd wordt door een onder de Rijksoverheid vallende uitvoeringsorganisatie. Op dit moment worden gesprekken gevoerd met een aantal uitvoeringsorganisaties. Deze gesprekken bevinden zich in de verkennende fase. De organisaties waarmee we in gesprek zijn onderzoeken momenteel of zij deze opdracht zouden willen en kunnen uitvoeren. Nadat een keuze is gemaakt voor een uitvoerende partij zal onder meer een uitvoeringstoets plaatsvinden en een impactassessment waarbij ook de impact op het kennisveld aan de orde komt. Tevens zal er aandacht zijn voor privacyaspecten en toezicht- en handhaving. Bij de inrichting van de werkprocessen voor de uitvoerende organisatie zullen ook de kennisinstellingen betrokken worden. Wanneer meer duidelijk is over de uitvoeringsorganisatie die de toetsing zal gaan verzorgen, zal ik uw Kamer hierover informeren.

Verscherpt Toezicht

Op dit moment is voor een aantal technische studies en vakgroepen al sprake van Verscherpt Toezicht in het kader van de geldende sanctieverordeningen tegen Noord-Korea[22] en Iran. Vanaf inwerkingtreding van de (wet en) regelgeving waarin het toetsingskader is opgenomen zal het Verscherpt toezicht opgaan in de werkzaamheden van de toetsingseenheid. Tot definitieve inwerkingtreding van benoemde wet- en

[21] Wet veiligheidstoets investeringen, fusies en overnames, stb. 2022, nr. 215

[22] Voor welke technische studies heb ik een ontheffing kennisembargo nodig en hoe vraag ik deze aan? | Rijksoverheid.nl.

regelgeving blijft voor de vakgebieden waar dit nu ook geldt het Verscherpt Toezicht van toepassing.

Vervolgproces

Ik heb uw Kamer eerder bericht dat het toetsingskader realistisch gezien op zijn vroegst in 2023 in werking kan treden, aangezien de invoering van de maatregel complex en ingrijpend is. Nu gebleken is dat er ook wijzigingen op wetsniveau benodigd zijn, zal op korte termijn een wetstraject worden gestart. Benodigde wijzigingen en nieuwe wet- en regelgeving vragen tijd waardoor sprake zal zijn van een langer tijdpad tot inwerkingtreding. Ik voel tegelijkertijd de urgentie om het wetstraject voortvarend op te pakken, samen met de andere betrokken departementen. Ik werk een bijgesteld tijdpad uit voor het benodigde wetstraject op basis van een gezamenlijke juridische analyse die nu wordt uitgevoerd. Het wetsvoorstel zal na afronding van de ontwerpfase de gebruikelijke procedure volgen en eerst in consultatie gaan, dan langs de Raad van State om vervolgens eerst aan uw Kamer en dan aan de Eerste Kamer te worden toegezonden. Ik zal uw kamer in het voorjaar informeren over het verwachte tijdpad.

Het benodigde wetstraject en de tijd die hiermee gemoeid gaat maakt het des te belangrijker om in de tussentijd vol in te zetten op de andere reeds bestaande mogelijkheden, zoals de risicoanalyse en de onafhankelijke audit, de advisering door het Loket Kennisveiligheid en instrumenten zoals het Verscherpt Toezicht. Ook zal worden ingezet op verdere opbouw van expertise binnen de kennisinstellingen. Hierbij is duidelijkheid over welke kennis- en technologiegebieden sensitief zijn vanuit het oogpunt van de nationale veiligheid belangrijke input voor de kennisinstellingen bij het verder vormgeven van hun kennisveiligheidsbeleid. De instellingen krijgen handvatten en informatie mee ten behoeve van het in kaart brengen waar de sensitieve kennis en technologieën zich binnen kennisinstellingen bevinden.

In de tussentijd kunnen de instellingen vragen stellen aan het loket over samenwerkingen in het geval van sensitieve technologie. Kennisinstellingen hebben daarnaast de mogelijkheid direct in contact te treden met de inlichtingen- en veiligheidsdiensten wanneer concrete risico's worden geconstateerd. Tegelijk is snelheid bij invoering van het toetsingskader geboden. Daarom pak ik het wetstraject voortvarend op en laat ik de inrichting van de toetsing zoveel mogelijk gelijk op lopen met het wetstraject, zodat de toetsing na inwerkingtreding van de benodigde wet- en regelgeving zo snel als mogelijk van start kan gaan. Daarnaast zet ik mij ook in Europees verband in om dit vraagstuk te agenderen omdat deze problematiek per definitie over landsgrenzen heen gaat.

III Inzet EU en internationaal

De derde stap in onze aanpak behelst het zoeken van samenwerking en inzet in de EU en in internationaal verband. Het betreft enerzijds het bevorderen van vrije en open samenwerking op het gebied van onderzoek, wetenschap en innovatie, conform de Internationale Kennis- en Talentstrategie.[23] Dit doen we bijvoorbeeld door gerichte kennis- en innovatiemissies en binnen de EU met beproefde instrumenten zoals Horizon Europe en Erasmus+ waarmee zowel samenwerking binnen Europa als samenwerking van Europese onderwijs- en kennisinstellingen met derde landen wordt bevorderd.[24] Anderzijds zetten we in op het

[23] Kamerstuk 31 288, nr. 893.
[24] BNC-fiche Horizon Europe (Kamerstuk 22 112, nr. 3069), BNC-fiche Erasmus+.

ontwikkelen van gedeeld beleid ten aanzien van kennisveiligheid. Beiden zijn essentieel om te zorgen dat internationale samenwerking open en veilig kan plaatsvinden. Daarmee houden we toegang tot de beste kennis, maar maken we ook de aanpak van kennisveiligheid tot een gezamenlijk prioriteit.

Nederland heeft het afgelopen jaar actief gewerkt aan de inzet op kennisveiligheid in de EU en internationaal en zal dat ook blijven doen. Een belangrijk element van de inzet is het opzetten van een netwerk met gelijkgezinde landen, zowel binnen als buiten de EU. Daarbij wordt specifiek samengewerkt met partners zoals Duitsland, het Verenigd Koninkrijk, de Verenigde Staten en de Europese Commissie, evenals de (inkomende) EU-voorzitterschappen. Een belangrijk doel hierbij is het leren van elkaar en een gezamenlijk beeld te krijgen van de risico's. Ook proberen we andere landen te overtuigen om ook maatregelen te nemen en inbreng op te halen voor de verdere vormgeving van beleidsmaatregelen in Nederland. De samenwerking en gesprekken gaan bijvoorbeeld over hoe sensitieve technologieën af te bakenen of hoe kansen en risico's in het vormgeven van internationale samenwerking te kunnen wegen. Verder wordt gesproken over hoe met de gemeenschap van gelijkgezinde landen gezamenlijk beter en efficiënter samen te werken op het thema kennisveiligheid. De samenwerking en gesprekken vinden zowel op ambtelijk als op politiek niveau plaats.

Specifiek in de EU zijn dit jaar stappen gezet, onder meer met de concrete uitwerking van de *Mondiale benadering van onderzoek en innovatie* [25] en de Europese strategie voor universiteiten[26]. Deze voorstellen zijn gericht op de EU-inzet op het bevorderen van internationale samenwerking in respectievelijk onderzoek & innovatie en hoger onderwijs (*promote*). Waarbij ook nadrukkelijk aandacht is voor het beschermen van onze kennis en fundamentele waarden in die internationale samenwerking (*protect*). Daarnaast zijn de EU *Guidelines on Research & Innovation foreign interference* gepubliceerd.[27] Op basis van een ministeriële conferentie in Marseille is afgesproken welke waarden en principes in hoger onderwijs, onderzoek en innovatie de EU moet garanderen bij internationale samenwerking met derde landen. Het gaat dan bijvoorbeeld om academische vrijheid, reciprociteit, ethiek, integriteit en *open science*. Dit geeft belangrijke randvoorwaarden voor de huidige en toekomstige samenwerking van de EU met derde landen. Hierover zijn ook Raadsconclusies aangenomen.

Het is van belang dat specifiek binnen de EU een gelijk speelveld (*level playing field*) tot stand wordt gebracht op het gebied van kennisveiligheid. De EU is immers een gezamenlijke interne markt met een Europese Onderzoeksruimte en Onderwijsruimte. Het kabinet wil daarom voorkomen dat onwenselijke overdracht van kennis plaatsvindt via andere landen en via een omweg alsnog zou leiden tot risico's voor de nationale veiligheid. Verder is het van belang dat onze concurrentiepositie niet wordt aangetast. Daarbij is afstemming met inzet op eerder genoemde beleidsthema's zoals economische veiligheid en open strategische autonomie van belang. Vanuit meerdere ministeries wordt hier gezamenlijk in opgetrokken.

---

[25] BNC-fiche Mondiale benadering van Onderzoek en Innovatie (Kamerstuk 22 112, nr. 3146).
[26] BNC-fiche Europese strategie voor universiteiten en Raadsaanbeveling transnationale samenwerking hoger onderwijs (Kamerstuk 22 112, nr. 3353).
[27] EU Guidelines on Research & Innovation foreign interference.

In lijn met het Coalitieakkoord (Bijlage bij Kamerstuk 35 788, nr. 77) neemt Nederland een sturende en leidende rol in de EU op het gebied van kennisveiligheid. Zo is op initiatief van Nederland met gelijkgezinde landen een ministerieel overleg over kennisveiligheid georganiseerd om te werken aan het gelijke speelveld in de EU. Nederland zet in op het verhogen van bewustwording over kennisveiligheid, zowel bij de Europese Commissie, als de EU-lidstaten en -kennisinstellingen; het faciliteren van beleidsleren in de EU, bijvoorbeeld via workshops; het gezamenlijk werken aan het verzamelen en inzichtelijk maken van data en informatie over kansen en risico's rond samenwerking met derde landen; en betere coördinatie van nationale beleidsmaatregelen.

Het netwerk van Onderwijs- en Wetenschapsattachés speelt in de inzet een belangrijke rol. Inmiddels zijn attachés geplaatst in verschillende landen die belangrijk zijn voor de Nederlandse inzet op kennisveiligheid, zoals in Duitsland, Frankijk, de Verenigde Staten, het Verenigd Koninkrijk en China. De attachés werken daarbij ook nauw samen met de collega's op de Nederlandse ambassades zoals de innovatieattaches.

IV. Aanbieding en beleidsreactie AWTI-advies over Kennisveiligheid

Met deze brief bied ik uw Kamer ook het advies van de AWTI aan. De raad beantwoordt de vraag hoe Nederland moet omgaan met de risico's van internationale samenwerking bij kennisontwikkeling en hoger onderwijs. In ben de AWTI zeer erkentelijk voor dit advies. Gezien de fase van doorontwikkeling van het kennisveiligheidsbeleid, komt dit advies op een goed moment.

De AWTI stelt vast dat internationale samenwerking op het gebied van onderzoek, wetenschap en innovatie essentieel is voor de ontwikkeling van en toegang tot de nieuwste en beste kennis. Voor een land als Nederland is die internationale samenwerking dan ook cruciaal. Tegelijkertijd constateert de AWTI ook de toegenomen risico's van de samenwerking, door het veranderende geopolitieke klimaat. Wat betreft kennisveiligheid stelt de AWTI vast dat er belangrijke stappen zijn gezet door zowel de overheid als kennisinstellingen. Nederland wordt internationaal als voorbeeld gezien wat betreft het beleid op kennisveiligheid. Het uitgangspunt voor de doorontwikkeling van het beleid is gunstig: het Nederlandse kennisveld is open over uitdagingen en deelt in toenemende mate kennis, inzichten en praktische handvatten met elkaar en de samenwerking tussen het kennisveld en de Rijksoverheid is goed ontwikkeld.

De AWTI ziet ook belangrijke aandachtspunten. Allereerst concludeert de raad dat een stevig en gedeeld conceptueel kader van kennisveiligheid mist. De AWTI ziet dat partijen vaak redeneren vanuit één perspectief: zuiver economisch, academisch of vanuit het veiligheidsperspectief. Door deze benadering raakt de nuance, waarin alle perspectieven een rol spelen, regelmatig buiten beeld. Ik sluit mij aan bij de constatering dat er steeds een afweging dient plaats te vinden tussen verschillende waarden. Dat is ook waar het kabinet voor staat. Dat is niet alleen van belang vanuit het oogpunt kennisveiligheid, maar raakt ook aan open strategische autonomie, technologisch leiderschap en economische veiligheid. De bevindingen van de AWTI illustreren voor mij de noodzaak tot een blijvende intensieve dialoog met het kennisveld. Ten tweede stelt de raad dat (tenminste een deel van het) kennisveld nog belangrijke stappen te zetten heeft. In hun gesprekken met het kennisveld heeft de raad vastgesteld dat vaardigheden op een aantal plaatsen nog onvolkomen zijn en dat nog niet alle betrokkenen zich voldoende bewust zijn van de

veranderde geopolitieke context waarin internationale wetenschappelijke samenwerking plaatsvindt. Tot slot concludeert de raad dat betere handelingsperspectieven nodig zijn voor kennisinstellingen en individuele wetenschappers om risico's binnen samenwerkingen te beheersen. Hiermee doelt de Adviesraad op de mogelijkheid om goede mitigerende maatregelen te nemen en dat een keuze voor samenwerking niet alleen maar binair, ja of nee is.

Ik herken en onderschrijf zowel de positieve ontwikkelingen als de aandachtspunten die de AWTI in het advies benoemt. Het kabinet heeft niet alleen ingezet op het bevorderen van open en vrije samenwerking door internationale en Europese coalities te verstevigen. De afgelopen twee jaar heeft de Rijksoverheid samen met het kennisveld tevens een stevige basis voor de aanpak van kennisveiligheid neergezet. Het is nu zaak om de aanpak voor de langere termijn te verfijnen en te bestendigen. Dit blijf ik samen met het kennisveld doen en ik doe daarbij een expliciet beroep op kennisinstellingen die nog stappen te zetten hebben.

De AWTI adviseert om de kennisveiligheidscapaciteit bij kennisinstellingen te versterken, het bewustzijn en de vaardigheden op het gebied van kennisveiligheid binnen instellingen te vergroten, de expertise en de achtergronden van de adviesteams uit te breiden en om een professionaliseringsmodel te ontwikkelen. Deze aanbevelingen neem ik ter harte. De middelen die uw Kamer met het gewijzigd amendement Van der Woude, Van der Molen en Van der Graaf beschikbaar heeft gesteld, helpt hierbij.[28] Binnen een systeem dat voor een belangrijk deel van onderop georganiseerd wordt is het van groot belang dat men op alle niveaus in staat is om risico's te signaleren en handelingsperspectieven te onderscheiden. Daarom start vanuit het loket begin volgend jaar de bewustwordingscampagne om het bewustzijn van kennisveiligheid door te laten dringen tot in de haarvaten van de instellingen en wordt vanuit het loket ingezet op de ontwikkeling van handzame tools die door kennisinstellingen kunnen worden toegepast. Ik faciliteer ook de doorontwikkeling van het netwerk kennisveiligheid tot *learning community* en ik roep alle kennisinstellingen op om hier actief aan deel te nemen. Samen met het kennisveld werk ik op deze manier aan het uitwisselen van kennis en ervaring en het verhogen van de expertise en het handelingsniveau. Dit moet mede het aandachtspunt van de AWTI adresseren dat er gewerkt moet worden aan het verduidelijken en differentiëren van kennisveiligheid om daarmee tot mitigerende maatregelen te komen die proportioneel kunnen worden ingezet. Ik kom daarmee ook tegemoet aan de gesignaleerde behoefte van het veld om meer en betere informatievoorziening ter realiseren wat betreft dual-use goederen, zoals blijkt uit de vragen aan het loket.

Tot slot

Dit jaar zijn flinke stappen gezet om de kennissector weerbaarder te maken tegen dreigingen van statelijke actoren. Tegelijkertijd zijn we er nog niet. Er ligt een stevige basis, maar nog niet alle instellingen zijn even ver en doorontwikkeling van onze aanpak is noodzakelijk. Ik kies voor de lerende aanpak die de AWTI mij aanbeveelt en zet alle zeilen bij om het kennis- en vaardighedenniveau binnen kennisinstellingen te verhogen via de *learning community* van het netwerk kennisveiligheid. De externe audit laat ons in 2023 zien waar het kennisveld staat en vormt input voor het aanscherpen van de risicoanalyses en de doorontwikkeling van de leidraad. Via het loket blijven we kennisinstellingen op verzoek voorzien van informatie en advies en hier voegen we pro actieve informatievoorziening aan toe. Ik start het traject om de wettelijke basis voor het

[28] Kamerstuk 36 200 VIII, nr. 62.

toetsingskader te regelen. Ik informeer uw Kamer over het verwachte tijdspad in het voorjaar van 2023. En ik blijf mij in EU- en internationaal verband inzetten op het verbeteren van samenwerkingen op het gebied van kennisveiligheid en het verkrijgen van het noodzakelijke *level playing field*. Samen met de Minister van EZK, blijf ik mij inzetten voor de bevordering van vrije en open samenwerking, met aandacht voor zowel de kansen als de risico's.

De inspanningen van het kabinet en de kennissector moeten er gezamenlijk voor zorgen dat internationale samenwerking in het hoger onderwijs en het (toegepaste) onderzoek veilig kan plaatsvinden, nu en in de toekomst.

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