Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

Nr. 1030

LIJST VAN VRAGEN EN ANTWOORDEN

Vastgesteld 5 april 2023

De vaste commissie voor Onderwijs, Cultuur en Wetenschap heeft een aantal vragen voorgelegd aan de Minister van Onderwijs, Cultuur en Wetenschap over de brief van 23 december 2022 inzake de voortgang aanpak kennisveiligheid hoger onderwijs en wetenschap (Kamerstuk 31 288, nr. 1003).

De Minister heeft deze vragen beantwoord bij brief van 5 april 2023. Vragen en antwoorden zijn hierna afgedrukt.

De voorzitter van de commissie,
Michon-Derkzen

De adjunct-griffier van de commissie,
Huls

kst-31288-1030
ISSN 0921 - 7371
's-Gravenhage 2023

1
Zijn de NCTV[1] en/of inlichtingen- en veiligheidsdiensten geraadpleegd over de CSC[2]-beurzen?

Ja, er is regelmatig contact tussen het Ministerie van Onderwijs, Cultuur en Wetenschap en de NCTV en/of de inlichtingen- en veiligheidsdiensten.

2
Zijn de antwoorden op de schriftelijke vragen van het lid Van der Woude over het artikel «Chinese promovendi in Nederland moeten trouw beloven aan de communistische partij» van 14 oktober 2022[3] afgestemd met NCTV en/of AIVD[4]/MIVD[5]?

Deze antwoorden zijn niet afgestemd met deze partijen. Wel zijn de NCTV, AIVD en MIVD actief betrokken bij het vormgeven van het kennisveiligheidsbeleid.

3
Worden brieven met betrekking tot kennisveiligheid ook afgestemd met het Ministerie van Justitie en Veiligheid en in het bijzonder met de NCTV?

De brieven met betrekking tot kennisveiligheid worden afgestemd met het Ministerie van Justitie en Veiligheid, waaronder de NCTV.

4
Hoe gaan andere landen in Europa om met de CSC-beurzen en in hoeverre wordt specifiek beleid gevoerd ten aanzien van CSC-beurzen, eventueel ook in samenwerking met veiligheidsdiensten?

De vraag hoe om te gaan met CSC-beurzen speelt ook in andere Europese landen. Dit zien we ook terug in de media, bijvoorbeeld door artikelen in Zweedse en Duitse media waarover het lid Van der Woude Kamervragen heeft gesteld.[6] Ik beschik niet over een beeld per land en het is lastig om dit op te halen, omdat CSC met alle kennisinstellingen, in Nederland maar ook in Europa, andere contracten afsluit. We spreken met *like-minded* landen binnen en buiten de EU over de vormgeving van effectief kennisveiligheidsbeleid. Binnen de EU neemt Nederland neemt deel aan verschillende gremia waar kennis en informatie over de kansen en risico's van samenwerking met China worden uitgewisseld.

5
In hoeverre werkt Nederland samen met andere gelijkgestemde Europese landen op dit gebied en wordt er bijvoorbeeld relevante kennis en informatie uitgewisseld?

Nederland neemt een leidende rol in het agenderen van kennisveiligheid bij de Europese Commissie en de lidstaten. Zo zal Nederland later dit jaar een mutual learning exercise organiseren op het gebied van kennisveiligheid en is eind 2022 op initiatief van Nederland met gelijkgezinde landen een ministerieel overleg over kennisveiligheid georganiseerd. Daarnaast is er ook op bilateraal niveau nauw contact met lidstaten, onder

---

[1] NCTV: Nationaal Coördinator Terrorismebestrijding en Veiligheid.
[2] CSC: China Scholarship Council.
[3] Aanhangsel Handelingen II 2022/23, nr. 1183.
[4] AIVD: Algemene Inlichtingen- en Veiligheidsdienst.
[5] MIVD: Militaire Inlichtingen- en Veiligheidsdienst.
[6] 2023Z03570 en 2023Z04082.

andere met Duitsland. Ook kennisinstellingen zelf brengen kennisveiligheid ter sprake in hun internationale samenwerkingsverbanden.

Naast het definiëren van risico's is het belangrijk om oog te houden voor de mogelijkheden van internationale wetenschappelijke en onderwijssamenwerking. Zo staat China op bepaalde terreinen wereldwijd aan de top van wetenschap en technologie. Het is daarnaast noodzakelijk om wereldwijde maatschappelijke uitdagingen als de energietransitie en klimaatverandering gezamenlijk aan te gaan. Zoals in de Kamerbrief *Ontwikkelingen Chinabeleid: een verschuiving van de balans* staat[7]: «Het is belangrijk om de balans te bewaren in de betrekkingen en oog te blijven houden voor de mogelijkheden tot samenwerking». Een Memorandum of Understanding (MoU) is een veelgebruikt, niet-bindend middel in de internationale samenwerking. Een MoU geeft structuur aan de samenwerking en fungeert als een kader voor de kennissector.

De huidige MoU's op het gebied van Wetenschap, Technologie en Innovatie en Onderwijs zijn inmiddels meer dan tien jaar oud en dienen geactualiseerd te worden om de balans tussen kansen en risico's goed te houden. Ook andere Europese landen hebben recentelijk hun MoU's met China vernieuwd of zijn hiermee bezig. De Ministeries van Onderwijs, Cultuur en Wetenschap en van Economische Zaken en Klimaat zullen over de MoU Wetenschap, Technologie en Innovatie besprekingen met de Chinese overheid voeren. Het Ministerie van Onderwijs, Cultuur en Wetenschap zal daarnaast in gesprek gaan met de Chinese overheid over een MoU Onderwijs. De Kamer zal voor het einde van het jaar geïnformeerd worden over de voortgang.

6
Zijn de afspraken met betrekking tot kennisveiligheid, die u beschrijft in het Bestuursakkoord Hoger Onderwijs en Wetenschap 2022[8], een uitputtende lijst van afspraken of zijn er specifiekere afspraken gemaakt om de werking in de praktijk ook effectief te laten zijn?

Sinds de start van het kennisveiligheidsbeleid in 2020 is samenwerking tussen de overheid en de kennisinstellingen, ieder vanuit de eigen verantwoordelijkheid, de fundering waarop het beleid is gestoeld. Ik heb vanaf de start een constructieve dialoog met het kennisveld geïnitieerd. Zoals aangekondigd in mijn voortgangsbrief van 23 december 2022 jl.[9] zet ik de dialoog met kennisinstellingen dit jaar voort. De dialoog is niet gericht op het maken van afspraken, maar op het gezamenlijk ontwikkelen van een effectieve aanpak en het verder vergroten van het bewustzijn en handelingsvermogen. Ik ondersteun de kennisinstellingen op verschillende manieren. Samen met het kennisveld is de Nationale Leidraad Kennisveiligheid (hierna: leidraad) opgesteld, waarin we duidelijkheid en handvatten bieden. In het bestuursakkoord zijn afspraken gemaakt over de implementatie van de leidraad. De overheid heeft een stevig landelijk Loket Kennisveiligheid (hierna: loket) opgericht dat adviezen verstrekt, dat dient als expertisepunt en het netwerk kennisveiligheid faciliteert. De leidraad, het loket en de gezamenlijke insteek van de Nederlandse aanpak worden internationaal inmiddels als best practice gezien.

7
Gaan universiteitsbesturen op een eenduidige wijze om met het Loket Kennisveiligheid?

---

[7] Kamerstuk 35 207, nr. 61.
[8] Kamerstuk 31 288, nr. 969.
[9] Kamerstuk 31 288, nr. 1003.

Universiteitsbesturen zijn zelf verantwoordelijk voor het nemen van maatregelen omtrent kennisveiligheid. Als overheid ondersteunen we hen daar actief bij door hen met de adviezen van het loket in staat te stellen afgewogen beslissingen te nemen. Om een eenduidige aanpak van kennisveiligheid vast te houden en te bevorderen wordt er door het loket consistent geadviseerd. In vergelijkbare gevallen worden vergelijkbare mogelijke mitigerende maatregelen aangedragen om de kennisinstelling een eenduidig handelingsperspectief te bieden. Van de advisering door het loket gaat een normerende werking uit, maar hoe een instelling aanbevelingen opvolgt is de verantwoordelijkheid van de instelling zelf. In de bestuurlijke dialoog met kennisinstellingen besteed ik aandacht aan een eenduidige aanpak van kennisveiligheid over de sector heen. Kennisinstellingen voeren hierover ook onderling al het gesprek. Hoe kennisinstellingen in het algemeen omgaan met het afwegen van risico's en het nemen van mitigerende maatregelen, wordt op sectorniveau zichtbaar door de audit die dit jaar plaatsvindt.

8
Gaan universiteitsbesturen op zodanige wijze om met het Loket Kennisveiligheid, zodat u hier inzicht in heeft en de effectiviteit van het loket kan worden gemeten?

De opgave op het gebied van kennisveiligheid kan alleen effectief worden aangepakt met het totale pakket aan maatregelen, zoals ook toegelicht in het antwoord op vraag 10. Het loket toetst of de adviezen bruikbaar zijn door na behandeling van een vraag een evaluatie aan de indiener te sturen. Via de kennisveiligheidsdialoog met bestuurders van kennisinstellingen krijg ik informatie over wat zij met de adviezen van het loket doen. Hier geven bestuurders voorbeelden van concrete casussen waarbij zij naar aanleiding van een advies een samenwerking met een onderzoeker of instelling bewust hebben afgewogen en er vervolgens voor hebben gekozen deze af te houden of te continueren.

9
Is er een overzicht van welke restrisico's, door niet het Loket Kennisveiligheid te raadplegen, door instellingen aanvaard zijn, welke gemitigeerd zijn en welke vermeden, en wie daar verantwoordelijk voor is?

Rijksoverheid en kennisinstellingen zijn gezamenlijk verantwoordelijk voor het kennisveiligheidsbeleid. Dat doen we ieder vanuit een eigen rol en verantwoordelijkheid, zoals in het antwoord op vraag 10 uiteen wordt gezet. In het kader van de dialoog hebben bestuurders van kennisinstellingen mij voorbeelden gegeven van risico-inschattingen die zij maken en de maatregelen die zij nemen. Daarbij kunnen zij gebruik maken van de leidraad en van de adviezen van het loket. Het loket vervult geen controlerende functie maar raadt indien nodig sterk aan bepaalde maatregelen te nemen. De audit die dit jaar plaatsvindt, zal op sectorniveau meer inzicht geven in hoe kennisinstellingen omgaan met het afwegen van risico's en het nemen van mitigerende maatregelen. De sectorbeelden die het resultaat zijn van de audit, zullen worden geagendeerd inreguliere overleggen met de sectororganisaties en in de bestuurlijke kennisveiligheidsdialoog.

10
Waar ligt de verantwoordelijkheid voor het aanvaarden van een mogelijk risico voor de nationale veiligheid door een universiteit; is dat bij het universiteitsbestuur, bij u, bij beide of bij geen van beide?

Het vormgeven en uitvoeren van kennisveiligheidsbeleid is een brede en gedeelde maatschappelijke opgave van kennisinstellingen en van de Rijksoverheid. Beide hebben daarin een eigen verantwoordelijkheid die gericht is op het mitigeren van kennisveiligheidsrisico's. In het bestuursakkoord hebben we afspraken gemaakt over wat de kennisinstellingen doen om het kennisveiligheidsbeleid te implementeren. De wijze waarop ze daar invulling aan geven, is aan de instellingen zelf. Het bestuur van een kennisinstelling en in het bijzonder de bestuurlijk portefeuillehouder is verantwoordelijk voor het beleid binnen de instelling en is er in individuele casussen voor verantwoordelijk om een bewuste afweging te maken.

Het is de rol van de overheid om de kennisinstellingen daarbij te ondersteunen en de dialoog hierover te organiseren. Dit heeft geleid tot de Kennisveiligheidsdialoog, de leidraad, bestuurlijke afspraken over onder meer een externe audit en de totstandkoming van het loket waarin advisering, informatievoorziening en kennisdeling centraal staan. Daar waar de risico's voor de nationale veiligheid het grootst zijn, is het de rol van de overheid wettelijke kaders te stellen. Bijvoorbeeld in de vorm van exportcontrole of sanctieregelingen. Daar wordt de Screening Kennisveiligheid (hierna: screening) aan toegevoegd. Tot slot pakt de overheid een leidende rol op internationaal niveau. Bijvoorbeeld in de EU en in internationaal verband met *like-minded* landen om te komen tot een *level playing field*.

11
Hebben alle universiteitsbesturen inzicht in alle adviezen die vanuit hun eigen instelling zijn gedaan bij het Loket Kennisveiligheid en delen zij dat inzicht met u?

Het loket is een laagdrempelig contact- en expertisepunt waar eenieder die verbonden is aan een kennisinstelling terecht kan met vragen omtrent kennisveiligheid. Wanneer bij het loket een vraag wordt ingediend door iemand anders dan een coördinator of medewerker kennisveiligheid of integrale veiligheid, wijst het loket er in het advies op dat het voor de kennisopbouw goed is het advies met deze functionarissen te delen. Of er binnen een instelling afspraken worden gemaakt over het behouden van overzicht, is aan henzelf. Zoals beschreven in het antwoord op vraag 10, heeft de overheid een ondersteunende en faciliterende rol welke de instellingen in staat stelt hun verantwoordelijkheid waar te maken. Het is niet passend om de instellingen te vragen hun overzicht met de overheid te delen. In het kader van de bestuurlijke dialoog en de learning community wordt wel informatie met elkaar gedeeld ten behoeve van het leren van elkaar en de doorontwikkeling van de aanpak van kennisveiligheid. Kennisinstellingen voeren hierover ook onderling al het gesprek.

12
Beargumenteren universiteitsbesturen, indien zij een risico (aangegeven door het Loket Kennisveiligheid) aanvaarden, niet alleen desgevraagd waarom zij een risico aanvaarden? En indien zij risico's denken te kunnen mitigeren, hoe denken zij dat te gaan doen?

Het mitigeren van de risico's in individuele casussen valt binnen de verantwoordelijkheid van kennisinstellingen. De wijze waarop ze risico's mitigeren en het beleid daarop vormgeven, is aan de instellingen zelf. De instellingen kunnen daarbij gebruik maken van de ondersteuning die de overheid biedt. In het kader van de dialoog bevorderen we het gesprek over het mitigeren van maatregelen en hebben bestuurders van kennisinstellingen voorbeelden gegeven van de risico-inschattingen die zij maken

en de wijze waarop zij risico's mitigeren. De audit die dit jaar plaatsvindt, zal op sectorniveau inzicht geven in hoe kennisinstellingen omgaan met het afwegen van risico's en het nemen van mitigerende maatregelen

13
Zijn er duidelijke afspraken met universiteitsbesturen gemaakt over wat zij doen met adviezen die een risico aangeven?

Om een eenduidige aanpak van kennisveiligheid vast te houden en te bevorderen worden in vergelijkbare gevallen vergelijkbare mogelijke mitigerende maatregelen aangedragen. Ieder advies is maatwerk en de context van iedere kennisinstelling is weer anders. Wel besteed ik in de bestuurlijke dialoog en kennisinstellingen onderling aandacht aan de consistentie van het kennisveiligheidsbeleid over de instellingen heen.

14
Wat is de doorlooptijd van een aanvraag bij het Loket Kennisveiligheid? Beperkt dit de werking van het loket?

Snelheid van de advisering was bij de oprichting van het loket voor koepelorganisaties een belangrijke voorwaarde. Daarom streeft het loket ernaar om binnen vijftien werkdagen een advies te geven. Bij het grootste deel van de adviezen lukt dit. Op dit moment zien we een forse toename van het aantal en van de complexiteit van de vragen. Ook nu streeft het loket naar een goede balans tussen een snel proces en een inhoudelijk gedegen advies.

15
Hebben instellingen een centraal informatiepunt over kennisveiligheid?

Ja, de overheid faciliteert een centraal informatiepunt over kennisveiligheid in de vorm van het loket dat hulp biedt aan iedereen die verbonden is aan een kennisinstelling met vragen over kansen, risico's en praktische zaken rondom internationale samenwerking. De website van het loket is een centraal informatiepunt voor alle zaken omtrent kennisveiligheid. Daarnaast kunnen instellingen voor specifieke casussen bij het loket advies opvragen. Het loket organiseert ook informatiesessies en evenementen voor het netwerk kennisveiligheid. Dit netwerk wordt in 2023 doorontwikkeld tot learning community.

16
Onder welke voorwaarden, op welke manier en op welke termijn worden de middelen van het amendement Van der Woude c.s.[10] concreet ingezet?

In de Kamerbrief over de planning van het wetsvoorstel voor de screening die uw Kamer recent heeft ontvangen, is tevens uiteengezet hoe het amendement wordt uitgewerkt.[11] Hierin staat toegelicht dat de middelen afzonderlijk over de instellingen worden verdeeld via lumpsumfinanciering. Voor de volledige uitwerking verwijs ik naar deze brief.

17
Is er een beeld hoeveel fte[12] elke instelling heeft aangesteld met betrekking tot kennisveiligheid?

---

[10] Kamerstuk 36 200 VIII, nr. 62.
[11] Kamerbrief «Tijdpad wetstraject Screening Kennisveiligheid en uitwerking amendement middelen kennisveiligheidsbeleid» d.d. 05-04-2023, Kamerstuk 36 200 VIII, nr. 213.
[12] fte: fulltime-equivalent.

Het is de verantwoordelijkheid van instellingen, en in het bijzonder van de portefeuillehouder kennisveiligheid in het College van Bestuur, om het kennisveiligheidsbeleid op hun eigen instelling uit te voeren. Hieronder valt ook dat zij zelf bepalen hoeveel fte zij hiervoor inzetten. Dit is immers ook afhankelijk van de aard en context van de instelling.

18
Wordt er gemonitord of elke instelling genoeg uitvoeringscapaciteit heeft voor de genomen maatregelen op het gebied van kennisveiligheid?

Zoals aangegeven in het antwoord op vraag 17 betreft dit de verantwoordelijkheid van de kennisinstellingen. Dit wordt door mij niet gemonitord.

19
Welke kennisinstellingen hebben meegedaan aan de kennisveiligheidsdialoog en welke niet en wat was daar dan de reden voor?

Sinds de start van de kennisveiligheidsdialoog in 2020 is met het grootste gedeelte van de kennisinstellingen (universiteiten, UMC's, hogescholen, NWO- en KNAW-instituten) gesproken over kennisveiligheid. De gesprekken hebben op het niveau van zowel besturen als raden van toezicht van kennisinstellingen plaatsgevonden. Ook op het niveau van beleid wordt het gesprek gevoerd binnen het Netwerk Kennisveiligheid. In de dialoog is brede betrokkenheid van kennisinstellingen bij de ontwikkeling van het kennisveiligheidsbeleid zichtbaar. Uit de dialoog blijkt ook de grote diversiteit die het kennisveld rijk is en die ertoe leidt dat het belang van en de behoefte aan het gesprek over kennisveiligheid voor de ene instelling groter is dan voor de ander.

20
Wat zijn de meetbare doelen die u beoogt met de learning community en hoe gaat u de effectiviteit en doelmatigheid van de learning community in de toekomst beoordelen?

In 2022 is, gefaciliteerd door het loket kennisveiligheid, een netwerk van kennisveiligheidsexperts en -coördinatoren op kennisinstellingen ontstaan. Ik heb aangekondigd in 2023 in te zetten op doorontwikkeling van dit netwerk tot een learning community. Deze ontwikkeling wordt ingezet vanuit het loket kennisveiligheid. In 2023 worden diverse evenementen, webinars en trainingen door experts georganiseerd en worden e-learnings en andere praktische tools gelanceerd. Over de verdere invulling van de learning community ben ik in gesprek met het kennisveld. Het uitgangspunt van de learning community is dat kennisinstellingen gezamenlijk werken aan het verwerven en vergroten van de benodigde vaardigheden, handvatten, netwerk, kennis en expertise. Bij de volgende voortgangsrapportage over het kennisveiligheidsbeleid neem ik uw Kamer mee in de voortgang van de ontwikkeling van de learning community.

21
Wat is per maatregel de voortgang van de implementatie van de Nationale Leidraad Kennisveiligheid?

Dit beeld kan ik uw Kamer nu nog niet geven. De audit die dit jaar plaatsvindt, zal op sectorniveau een beeld geven van de voortgang van de implementatie van de Nationale Leidraad Kennisveiligheid. Het sectorbeeld van de universiteiten verwacht ik, zoals toegezegd in mijn Kamerbrief over de voortgang van de aanpak van kennisveiligheid, rond de zomer met uw Kamer te kunnen delen. Het sectorbeeld van de

hogescholen verwacht ik bij de volgende voortgangsrapportage kennisveiligheid in december 2023 met uw Kamer te kunnen delen.

22
Hoe groot zijn de verschillen tussen instellingen wat betreft de implementatie van de Nationale Leidraad Kennisveiligheid?

De audit die dit jaar plaatsvindt, zal op sectorniveau een beeld geven van de verschillen tussen de instellingen wat betreft de implementatie van de Nationale Leidraad Kennisveiligheid.

23
Op basis van welke inhoudelijke expertise is gekozen de externe audit bij Oberon en Dialogic te beleggen?

De externe audit kennisveiligheid is een beleidsonderzoek omdat deze is vormgegeven als een 0-meting van de stand van implementatie van de Nationale Leidraad Kennisveiligheid. Oberon en Dialogic hebben als onderzoeksbureaus ruime ervaring met het uitvoeren van beleidsonderzoek.

24
Hoe wordt de externe audit concreet vormgegeven?

Het onderzoek start met een zelfevaluatie vragenlijst die alle kennisinstellingen invullen. Deze vragenlijst is opgesteld door onderzoeksbureaus Oberon en Dialogic en besproken met en getoetst bij het kennisveld met de betrokken partijen via een klankbordgroep die hier speciaal voor is ingericht. De onderzoeksbureaus analyseren de antwoorden op de vragenlijst. Zij delen de analyse van de antwoorden op de vragenlijst op instellingsniveau alleen met de betreffende instelling. Zo krijgt de instelling zelf een beeld van waar zij staat en kan zij aan de slag met eventuele aandachtspunten of aanbevelingen die hieruit volgen.

Op basis van de analyse en de review stellen de onderzoeksbureaus een sectorbeeld op waaruit blijkt waar de kennisinstellingen nu staan met de uitwerken van het kennisveiligheidsbeleid. Om dit sectorbeeld in te kleuren, voeren de onderzoeksbureaus tot slot een kort verdiepend onderzoek uit – in de vorm van case studies – bij een klein aantal kennisinstellingen.

Ik ga dit najaar in de dialoog met de kennisinstellingen in gesprek over de sectorbeelden, de analyse die zij op instellingsniveau hebben ontvangen en over de mogelijkheid een sectorbreed model, geïnspireerd op *capability maturity model's*, te ontwikkelen zoals de Adviesraad voor Wetenschap, Technologie en Innovatie (hierna: AWTI) aanbeveelt.

25
Hoe implementeren kennisinstellingen de verplichting tot het doen van een risicoanalyse?

De aanpak en uitkomsten van de risicoanalyse door kennisinstellingen maken onderdeel uit van de externe audit kennisveiligheid, zoals uw Kamer aan mij heeft gevraagd in de motie van de leden Van der Woude en Van der Molen[13]. Op basis van de sectorbeelden die in de loop van dit jaar worden opgeleverd, kan ik uw Kamer een antwoord geven op deze vraag.

[13] Kamerstuk 31 288, nr. 979.

26
Kunt u kwantificeren hoeveel instellingen wel en niet de benodigde stappen voor de risicoanalyse hebben doorlopen en wat is de volgende stap die u gaat zetten als instellingen de risicoanalyses niet systematisch oppakken?

Naar aanleiding van de externe audit kennisveiligheid kan ik uw Kamer straks op sectorniveau een beeld geven van de aanpak en de uitkomsten van de risicoanalyses. Op basis van de dialoogsessies met de Raden van Toezicht blijkt dat de meeste instellingen het uitvoeren van de risicoanalyses serieus hebben opgepakt of hier vóór mijn verzoek al op systematische wijze invulling aan gaven. Naar aanleiding van de resultaten van de externe audit ga ik met de kennisinstellingen en externe experts in gesprek, zoals uw Kamer van mij gevraagd heeft in de motie van de leden Van der Woude en Van der Molen[14].

27
Is er een lijst van de CDIU[15] specifiek ingericht voor instellingen?

De Centrale Dienst voor in- en uitvoer (CDIU) hanteert geen lijst specifiek voor instellingen. Onderzoeksinstituten dienen namelijk de reguliere wetgeving te volgen inzake exportcontrole.

De CDIU heeft echter wel in nauwe samenwerking met het Ministerie van Buitenlandse Zaken van 2019 tot en met 2021 deelgenomen aan een Technical Expert Group van de EU Commissie die gericht was op het ontwikkelen van handvatten voor onderzoeksinstituten, inzake onderzoek op het gebied van dual-use items. Hieruit is een document voortgevloeid met uitgebreide informatie en aanbevelingen, aan de hand waarvan onderzoeksinstituten hun interne organisatie zo kunnen inrichten dat zij de juiste stappen ondernemen als er sprake is van onderzoek op het gebied van dual-use items.[16]

28
Wat heeft de sturende en leidende rol van Nederland in de EU[17] tot nu toe opgeleverd?

Op initiatief van Nederland is in een verband van gelijkgezinde landen in toenemende mate aandacht voor kennisveiligheid. Zoals ik recent aan uw Kamer heb toegelicht in de voortgangsbrief over kennisveiligheid, krijgt dit concreet vorm in bijvoorbeeld ministeriële en ambtelijke overleggen met *like-minded* landen binnen en buiten de EU waar onder andere best practices worden uitgewisseld. In bilateraal verband spreek ik regelmatig met Ministers uit andere lidstaten over kennisveiligheid, waarbij ik zie dat andere lidstaten graag leren van de Nederlandse aanpak en kennis willen uitwisselen. Ook bij de Europese Commissie is er bewustzijn over kennisveiligheid, wat zich uit in bijeenkomsten om kennis uit te wisselen en publicaties zoals de Guidelines on Research & Innovation foreign interference[18]. Nederland levert hier een actieve bijdrage aan. Hoewel de ontwikkelingen in de EU positief zijn, zie ik nog veel kansen en noodzaak in de EU om kennisveiligheid te verhogen. Ik blijf mij daarom in EU-verband inzetten op het verhogen van bewustwording over kennisveiligheid, het faciliteren van beleidsleren, het gezamenlijk inzichtelijk maken

---

[14] Kamerstuk 31 288, nr. 979.
[15] CDIU: Centrale dienst voor in- en uitvoer.
[16] https://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:32021H1700&from=EN.
[17] EU: Europese Unie.
[18] https://op.europa.eu/en/publication-detail/-/publication/3faf52e8-79a2-11ec-9136-01aa75ed71a1/language-en.

van risico's én kansen rond samenwerking met derde landen, en betere coördinatie van nationale beleidsmaatregelen.

29
Kunt u per aanbeveling en per aanbevolen actie van het AWTI[19]-rapport[20] aangeven of die aanbeveling wordt overgenomen en zo ja, hoe die aanbeveling wordt geïmplementeerd?

Het advies van de AWTI is opgebouwd langs drie aanbevelingen gericht aan zowel overheid als kennisinstellingen, bestaande uit (1) Het verbeteren van het begrip van kennisveiligheid; (2) het differentiëren tussen risico's en (3) het vergroten van het bewustzijn en de capaciteit. In de kamerbrief van 23 december 2022 heb ik aangegeven dat ik de AWTI erkentelijk ben voor hun advies, en dat ik er in lijn met hun advies naar streef om te komen tot een lerende aanpak in samenwerking met het kennisveld. Een belangrijk element in deze aanpak is het netwerk kennisveiligheid en de doorontwikkeling daarvan tot learning community. In de learning community gaan we gezamenlijk werken aan het verwerven en vergroten van de benodigde vaardigheden, handvatten, netwerk, kennis en expertise door het uitwisselen van kennis en ervaring via doelgerichte trainingen en bijeenkomsten. Ik heb in de brief aan uw Kamer van 23 december jl.[21] alle kennisinstellingen opgeroepen om actief aan deze community deel te nemen. Bij de verdere invulling van de learning community worden de aanbevelingen van de AWTI meegenomen. In aanvulling op de learning community zet ik ook in 2023 de dialoog met kennisinstellingen voort waarvoor het advies van de AWTI input vormt. Het doel is hierbij om naast het bestuurlijke gesprek, samen met kennisinstellingen dieper in instellingen door te dringen en meer met wetenschappers zelf het gesprek aan te gaan.
De beschrijvingen en analyses van de AWTI bieden in bredere zin houvast voor de verdere doorontwikkeling van ons beleid. Niet altijd als concrete aanbeveling, maar ook als onderdeel van de doorlopende dialoog, binnen de Rijksoverheid en met het veld. De AWTI draagt daar op dit moment zelf ook nog aan bij door het organiseren van presentaties en bijeenkomsten.

30
Wat is de relatie tussen open science en kennisveiligheid?

Binnen open science zijn kortweg drie doelstellingen belangrijk, namelijk a) het gratis (zonder betaalmuur) beschikbaar stellen van wetenschappelijke publicaties, b) het vindbaar, toegankelijk, interoperabel en herbruikbaar maken van onderzoeksdata en -software, zodat de samenwerking tussen onderzoekers en disciplines wordt versneld en c) het vergroten van de publieke betrokkenheid bij wetenschap.

Binnen de open science-doelstellingen is het beschermen van kennis alleen van toepassing op het vindbaar, toegankelijk, interoperabel en herbruikbaar maken van onderzoeksdata- en software. Ten aanzien van onderzoeksdata betekent open science beslist niet dat gevoelige data open wordt gedeeld. Om dit te voorkomen, hanteren universiteiten en financiers als NWO, ZonMw en ook de Europese Commissie, verschillende waarborgen en uitzonderingsgronden. Als waarborg geldt bijvoorbeeld dat onderzoekers, wanneer zij een research data management plan (DMP) opstellen, erop worden gewezen dat zij zorgvuldig met hun data moeten omgaan en dat gevoelige data niet mag worden gedeeld. Een van

[19] AWTI: Adviesraad voor wetenschap, technologie en innovatie.
[20] AWTI, november 2022, «Kennis in conflict: Veiligheid en vrijheid in balans», Bijlage bij Kamerstuk 31 288, nr. 1003.
[21] Kamerstuk 31 288, nr. 1003.

de belangrijkste uitzonderingsgronden voor het delen van onderzoeksdata is Kennisveiligheid. Ook moeten onderzoekers en instellingen zich houden aan de Nederlandse kabinetsaanpak kennisveiligheid, waarin het beschermen van gevoelige informatie centraal staat.

31
Welke verschillen zijn er tussen de regels en afspraken die gelden voor universiteiten, hogescholen, TO2[22]-instellingen en andere instellingen?

Het kennisveiligheidsbeleid is gericht op alle kennisinstellingen: universiteiten, hogescholen, KNAW- en NWO-instituten en de TO2 instellingen (die onder de beleidsverantwoordelijkheid van het Ministerie van Economische Zaken en Klimaat vallen) en maakt daar in principe geen onderscheid tussen. Wel is het zo dat afhankelijk van de aard van de instelling, het soort onderzoek en afhankelijk van met welke landen wordt samengewerkt verschillende juridische kaders en gedragscodes van toepassing kunnen zijn. Dit staat toegelicht in de nationale leidraad kennisveiligheid.

32
Zijn er maatregelen op het gebied van kennisveiligheid die niet in uw brief genoemd worden en die door het Ministerie van OCW of de EU worden overwogen?

De afgelopen jaren zijn al flinke stappen gezet op het gebied van kennisveiligheid. We werken aan het doorontwikkelen van de instrumenten die we al hebben en het uitvoeren van het beleid. Dat doen we langs de drie met elkaar samenhangende lijnen die ook in het antwoord op vraag 10 zijn benoemd: (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. Op dit moment zijn er geen nieuwe maatregelen die door het Ministerie van Onderwijs, Cultuur en Wetenschap worden overwogen. Zoals in antwoord op vraag 24 en 29 is aangegeven, ga ik in de dialoog dit najaar in gesprek over de resultaten van de audit en de aanbevelingen van de AWTI. Als hier of op andere momenten tot aanvullende maatregelen wordt, zal de Kamer hierover worden geïnformeerd.

Binnen de EU wordt onder diverse noemers aan de verschillende aspecten van kennisveiligheid gewerkt. Ik heb daarbij de belangrijkste maatregelen die kennisveiligheid verhogen reeds in de voortgangsbrief aan uw Kamer gecommuniceerd. EU-beleid is echter continu in ontwikkeling, daarom informeer ik uw Kamer in een volgende voortgangsbrief waar dat van toepassing is over nieuwe relevante ontwikkelingen.

33
Hebben kennisinstellingen, afgezien van hun contact met het Loket Kennisveiligheid, contact met het Ministerie van Justitie en Veiligheid en in het bijzonder de NCTV om veiligheidsrisico's te mitigeren?

De NCTV en het Ministerie van Economische Zeken en Klimaat zijn vanaf het begin af aan betrokken geweest bij de ontwikkeling van het beleid op kennisveiligheid. Zij zijn onder andere betrokken bij de kennisveiligheidsdialoog, het loket en andere gesprekken die gevoerd zijn met de kennisin-

[22] TO2: Toegepast Onderzoek Organisaties.

stellingen. Dit heeft altijd in samenspraak met het Ministerie van Onderwijs, Cultuur en Wetenschap plaatsgevonden, als verantwoordelijk vakdepartement en eerste aanspreekpunt voor de kennisinstellingen. Indien hiertoe aanleiding is kan de NCTV in gesprek gaan met kennisinstellingen naar aanleiding van specifieke vragen omtrent het mitigeren van veiligheidsrisicos. Hierbij wordt samen met het Ministerie van Onderwijs, Cultuur en Wetenschap en de inlichtingen- en veiligheidsdienst(en) opgetrokken. Daarnaast is de Minister van JenV betrokken bij de uitwerking van het wetsvoorstel Screening Kennisveiligheid.

34
In hoeverre worden kennisinstellingen op de hoogte gehouden en betrokken bij het vaststellen van het toetsingskader?

Voor de uitwerking en vormgeving van het wetsvoorstel heeft het Ministerie van Onderwijs, Cultuur en Wetenschap de expertise en kennis van de kennisinstellingen nodig. Om te bepalen welke technologiegebieden aangemerkt moeten worden als risicovakgebieden zijn de Ministeries van Economische Zaken en Klimaat en Onderwijs, Cultuur en Wetenschap samen met de Nederlandse Organisatie voor toegepast-natuurwetenschappelijk onderzoek (TNO) een traject gestart. Dit heeft geleid tot de ontwikkeling van een proces waarmee het Ministerie van Onderwijs, Cultuur en Wetenschap de afgelopen maanden heeft onderzocht welke technologiegebieden ten grondslag zullen worden gelegd aan het wetsvoorstel. Op dit moment krijgen kennisinstellingen via een vertrouwelijk proces de mogelijkheid om hierop te reageren. Daarnaast wordt hen gevraagd welke sensitieve kennis- en technologiegebieden zich bevinden binnen hun instelling. Dit is belangrijke informatie om rekening mee te houden bij de vormgeving van het screeningsproces.

Bij de verdere vormgeving van het screeningsproces – die onder andere zal plaatsvinden gedurende de ontwerpfase van het wetsvoorstel – zullen de kennisinstellingen ook worden betrokken. Daarbij wordt bezien wat de beste manier is om input bij de kennisinstellingen op te halen. We streven ernaar dat het wetsvoorstel de regeldruk op instellingen niet onnodig vergroot en dat de verplichte screening zo goed mogelijk aansluit bij de praktijk van het aanstellen van studenten en onderzoekers.

35
Is bekend of onderwijsinstellingen altijd op college van bestuurniveau besluiten of en hoe zij risico's aangaan inzake samenwerking met partijen uit onvrije landen?

Het is aan onderwijsinstellingen zelf om te bepalen op welk niveau besluiten worden genomen over risico's die gepaard gaan met internationale samenwerking en het mitigeren hiervan. Zoals in de Nationale Leidraad Kennisveiligheid is opgenomen, die door de Rijksoverheid samen met het kennisveld is opgesteld, is het centrale gezag (college van bestuur bij een universiteit of hogeschool) altijd eindverantwoordelijk voor deze beslissing. Het sectorbeeld dat naar aanleiding van de audit wordt opgesteld, zal een beeld geven van wat op centraal en decentraal niveau binnen kennisinstellingen wordt geregeld en besloten.

36
Is bekend of colleges van bestuur minimaal op de hoogte zijn van risico's die zijn aangegaan binnen hun instelling inzake samenwerking met partijen uit onvrije landen?

In de Nationale Leidraad Kennisveiligheid is opgenomen dat een bestuur ten allen tijde inzicht hoort te hebben in de significante samenwerkingen

die de organisatie aangaat. Ik heb de kennisinstellingen vorig jaar opgeroepen een risicoanalyse van de internationale samenwerkingen uit te voeren en daarover te rapporteren aan de Raad van Toezicht. In de kennisveiligheidsdialoog heb ik hierover gesproken met de Raden van Toezicht. In de bestuurlijke dialoog komen kennisveiligheidsrisico's, de afwegingen die daarbij horen en het beleid dat kennisinstellingen hiervoor ontwikkelen ook ter sprake. In de externe audit kennisveiligheid die dit jaar plaatsvindt, worden de aanpak en uitkomsten van de risicoanalyses meegenomen.

37
Stelt NWO[23] eisen aan of heeft NWO zicht op de partijen die deelnemen aan de derde geldstroom van onderzoeksprojecten die door NWO gefinancierd zijn?

NWO baseert zich bij de beantwoording van deze vraag op de definitie van derde geldstroom uit het rapport van het Rathenau Instituut «Ontwikkeling derde geldstroom en beïnvloeding van wetenschappelijk onderzoek»[24]. Gelet op deze definitie financiert NWO geen onderzoeksprojecten waarvan de derde geldstroom een onderdeel is. NWO stelt derhalve geen eisen aan de partijen die deelnemen aan de derde geldstroom, evenmin heeft NWO zicht op deze partijen.

38
Me**t welke betrokken partijen bent u voornemens te overleggen over de besteding van de vrijgemaakte middelen?**

Over de besteding van de middelen heb ik overleg gevoerd met UNL, VH, KNAW, NFU en NWO.

39
Op hoeveel vragen is, uitgesplitst naar categorie zoals aangeduid in uw brief, door het Loket Kennisveiligheid geconcludeerd dat er sprake was van een hoog risico?

Het loket weegt per casus zorgvuldig af wat de mogelijke risico's zijn. Wanneer het risico zodanig groot is dat dit een gevaar vormt voor de nationale veiligheid, adviseert het loket dringend om mitigerende maatregelen te nemen, dan wel de samenwerking niet aan te gaan. In een dergelijk geval, kan een advies worden opgevolgd door een gesprek met de Algemene Inlichtingen-en Veiligheidsdienst. Vanwege de gevoeligheid en vertrouwelijkheid van casuïstiek kan ik hier geen nadere uitspraken doen.

40
Burgers uit welke landen worden op dit moment aan een kennisveiligheidstoets onderworpen?

Het verscherpt toezicht ziet op het op een zorgvuldige en non-discriminatoire wijze toetsen van studenten en onderzoekers in gevoelige onderwijs-en onderzoeksgebieden op een mogelijke relatie met het Iraanse ballistische raketprogramma om in te schatten of er een risico bestaat op overtreding van de EU Iran-sanctieverordening 267/2012.[25]

---

[23] NWO: Nederlandse Organisatie voor Wetenschappelijk Onderzoek.
[24] https://www.rathenau.nl/sites/default/files/2020-10/RAPPORT_Ontwikkeling_derde%20geldstroom_en_be%C3%AFnvloeding_wetenschappelijk_onderzoek_Ra
[25] Kamerbrief «Verscherpen toezicht op studenten en onderzoekers uit risicolanden» van 14 maart 2019 (Kamerstuk 30 821, nr. 70), Kamerstuk 30 821, nr. 87 en Kamerstuk 30 821, nr. 100.

Omdat voor toegang tot bepaalde specifieke onderwijs- en onderzoeksgebieden tevens een ontheffing is vereist onder de Sanctieregeling Noord-Korea 2017[26], wordt daarnaast beoordeeld of het risico bestaat dat de op die terreinen verworven kennis bijdraagt aan proliferatiegevoelige activiteiten van Noord-Korea of aan de ontwikkeling van systemen voor de overbrenging van kernwapens in Noord-Korea.

41
Met welke frequentie wordt het toetsingskader na inwerkingtreding geëvalueerd en geactualiseerd?

Het wetsvoorstel wordt momenteel uitgewerkt. Het lijkt echter wel in de rede te liggen om de screening in het kader van kennisveiligheid die wordt ontwikkeld na inwerkingtreding te monitoren en actualiseren indien nodig. Hoe en hoe vaak dit zal gebeuren zal in de komende periode worden uitgewerkt. Zodra ik uw Kamer hier meer over kan berichten zal ik dat doen.
Actualisatie kan bijvoorbeeld aan de orde zijn voor de lijst met risicovakgebieden. Ook dat proces van actualisatie moet nog worden uitgewerkt. Actualisatie kan bijvoorbeeld tweejaarlijks aan de orde zijn, of zoveel eerder of vaker indien er signalen of actualiteiten zijn die dit noodzakelijk maken. De aanpak die we voorstaan heeft een generiek karakter, zodat de aanpak kan worden toegepast op ieder land van buiten de Europese Unie. Hierdoor zijn we voorbereid op ontwikkelingen in het dreigingsbeeld. Monitoring daarvan is hierbij van belang.

42
Heeft u aanwijzingen dat er op dit moment via andere EU-landen onwenselijke overdracht van kennis plaatsvindt die een risico vormt voor de nationale veiligheid?

Het is staand kabinetsbeleid dat ik geen uitspraken doe over de nationale veiligheid in andere lidstaten. In zijn algemeenheid kan echter gesteld worden dat net als Nederland, ook andere lidstaten signaleren dat statelijke actoren uit derde landen ongewenst kennis proberen te bemachtigen of te beïnvloeden. Net als Nederland zetten daarom steeds meer lidstaten van de Europese Unie in toenemende mate in op maatregelen die de kennisveiligheid verhogen. Zoals ik in de voortgangsbrief over kennisveiligheid aan u heb toegelicht, zet het kabinet zich actief in om kennisveiligheid binnen de EU en internationaal hoog op de agenda te zetten en andere landen te stimuleren gezamenlijk op te trekken. Zodat het risico dat onwenselijke overdracht van kennis via andere lidstaten plaatsvindt zoveel mogelijk ingeperkt wordt.

[26] Kamerstuk 30 821, nr. 87.