Ministerie van Onderwijs, Cultuur en Wetenschap

>Retouradres Postbus 16375 2500 BJ Den Haag

De voorzitter van de Tweede Kamer der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Hoger Onderwijs en Studiefinanciering
Rijnstraat 50
Den Haag
Postbus 16375
2500 BJ Den Haag
www.rijksoverheid.nl

Onze referentie
31177117

Bijlagen
2

Datum 31 januari 2022

Betreft Voortgang en vooruitblik aanpak kennisveiligheid hoger onderwijs en wetenschap

Internationale samenwerking op het gebied van hoger onderwijs en wetenschap is van essentieel belang. Excellent onderzoek van wereldklasse kan niet zonder. Tegelijk constateren we dat kennisinstellingen worden geconfronteerd met uiteenlopende dreigingen vanuit statelijke actoren. Kennisveiligheid omvat daardoor diverse aspecten. Zo kunnen kennis en technologie onbedoeld weglekken en worden ingezet op een manier die onze nationale veiligheid aantast of die op gespannen voet staat met wat wij in Nederland ethisch achten. Ook kan er binnen kennisinstellingen sprake zijn van heimelijke beïnvloeding door statelijke actoren, die de academische vrijheid en wetenschappelijke integriteit aantast.

Kennisveiligheid vergt een robuuste aanpak, waarbij de academische kernwaarden zoals academische vrijheid en wetenschappelijke integriteit steeds het uitgangspunt vormen. Proportionaliteit en maatwerk zijn daarbij leidend ("open waar mogelijk, beschermen waar nodig"). Het is essentieel dat de Nederlandse kennisinstellingen internationaal blijven samenwerken met buitenlandse kennisinstellingen en bedrijven en dat openheid daarbij de norm is; maar het is evenzeer essentieel dat die samenwerking *veilig* verloopt.

Met de Kamerbrief kennisveiligheid hoger onderwijs en wetenschap van november 2020 (hierna: de Kamerbrief kennisveiligheid)[1] presenteerde het kabinet een samenhangend pakket maatregelen om kennisveiligheid in Nederland structureel te verhogen. De aanpak is landenneutraal, dat wil zeggen dat deze toepasbaar is op iedere statelijke actor waar een dreiging van uitgaat. Sindsdien zijn door het kabinet én het kennisveld de nodige stappen gezet. Het onderwerp staat op de agenda, het bewustzijn is toegenomen. Zowel binnen de sector als binnen de Rijksoverheid wordt urgentie gevoeld om hier samen werk van te maken.

Met deze brief wordt uw Kamer geïnformeerd over de voortgang bij de uitwerking van de in de Kamerbrief kennisveiligheid aangekondigde maatregelen.

[1] Kamerbrief d.d. 27 november 2020 (link)

1. Dreigingsbeeld in relatie tot de Nederlandse kennisinstellingen

Het afgelopen jaar is geïnvesteerd in het verder verdiepen van kennis van en inzicht in de dreigingen en risico's waar de Nederlandse kennissector mee wordt geconfronteerd. Het Dreigingsbeeld Statelijke Actoren (DBSA) van de AIVD, MIVD en NCTV van februari 2021[2] en de jaarverslagen 2020 van de AIVD en de MIVD van april 2021[3] besteden hier dan ook opnieuw aandacht aan. Daaruit blijkt dat de dreiging die in de Kamerbrief kennisveiligheid werd geschetst, hierna nog eens toegelicht, niet is afgenomen.

Vanuit de intentie om de eigen militaire, technologische, politieke en economische macht te vergroten, zijn verschillende statelijke actoren ook in Nederland actief op zoek naar kennis en technologie. In de Kamerbrief kennisveiligheid beschreef het kabinet reeds enkele voorkomende methoden die statelijke actoren inzetten tegen kennisinstellingen, ook in Nederland. Hierbij is sprake van een glijdende schaal, waarbij het onderscheid tussen legitieme samenwerking, samenwerking met heimelijke intenties en illegale activiteiten niet altijd eenvoudig te maken is. In het DBSA waarschuwen AIVD, MIVD en NCTV eveneens voor structurele en centraal aangestuurde activiteiten van bepaalde statelijke actoren, die de Nederlandse belangen kunnen aantasten. Ook hieruit komt het beeld naar voren dat hoger onderwijsinstellingen en de wetenschap doelwit zijn van beïnvloeding en inmenging en ongewenste kennisoverdracht.

Nederland loopt het risico dat gedeelde kennis later ingezet kan worden voor doeleinden die direct onze nationale veiligheid raken, bijvoorbeeld in de vorm van militaire middelen, of dat de gedeelde kennis gebruikt wordt voor doeleinden die indruisen tegen onze fundamentele normen en waarden, bijvoorbeeld voor (massa)surveillancemiddelen. Bovendien kan door het ongewenst wegvloeien van gevoelige kennis, technologie en intellectueel eigendom naar andere landen onze innovatiekracht worden aangetast. Ook dient Nederland zich te houden aan sancties die gelden vanuit de VN en de EU ten aanzien van Iran en Noord-Korea.

Naast de verwerving van kennis en technologie vinden er in relatie tot kennisinstellingen ook beïnvloedings- en inmengingsactiviteiten plaats door statelijke actoren. Daarbij probeert een actor bijvoorbeeld meningen en publicaties te beïnvloeden en wetenschappelijk onderzoek en onderzoeksresultaten te censureren. Een actor kan hiervoor bijvoorbeeld gebruik maken van een financiële afhankelijkheid. Ook houden sommige statelijke actoren hun burgers in de gaten om te voorkomen dat zij onwelgevallige meningen over het thuisland verkondigen. De druk van deze activiteiten kan leiden tot zelfcensuur, waarbij individuen en groepen zich niet altijd openlijk kritisch uit durven te laten of academici worden gehinderd om onderzoeksresultaten te publiceren wanneer deze onwelgevallig zijn voor een bepaalde statelijke actor. Dit is een bedreiging van fundamentele vrijheden als de vrijheid van meningsuiting en voor kernwaarden als academische vrijheid en wetenschappelijke integriteit.

In de vandaag gepubliceerde Nationale Leidraad Kennisveiligheid (zie hierna, paragraaf 2.2) wordt in meer detail ingegaan op de intenties en werkwijzen van statelijke actoren en wordt kennisinstellingen handelingsperspectief geboden hoe met deze uitdagingen om te gaan.

2. Versterkte zelfregulering binnen de kennissector

[2] Dreigingsbeeld Statelijke Actoren d.d. 3 februari 2021 (link)
[3] Jaarverslag AIVD 2020 (link) en Jaarverslag MIVD 2020 (link)

De kennissector wordt gekenmerkt door een hoge mate van autonomie. Instellingen maken risicoafwegingen en geven zelf invulling aan hun interne beleid op het vlak van kennisveiligheid, uitgaand van bestaande wettelijke kaders, gedragscodes en richtlijnen. De overheid staat de instellingen daarbij met raad en daad terzijde. De door het kabinet in de Kamerbrief kennisveiligheid aangekondigde maatregelen helpen de zelfregulering binnen de kennissector te versterken en om, waar nodig, kaders te stellen. Hierna wordt de voortgang per maatregel beschreven en wordt vooruitgeblikt op de komende periode.

2.1 Kennisveiligheidsdialoog

In de tweede helft van 2020 is de kennisveiligheidsdialoog van start gegaan: een reeks gesprekken op bestuursniveau tussen de Rijksoverheid en vrijwel alle kennisinstellingen van Nederland.

Er zijn in dit kader door OCW in samenwerking met de NCTV en de AIVD gesprekken gevoerd met Universiteiten van Nederland (UNL) en de veertien daarbij aangesloten universiteiten, met de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW) en de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO) en de negentien daaraan verbonden onderzoeksinstituten en met Nederlandse Federatie van Universitair Medische Centra (NFU) en de zeven daarbij aangesloten universitair medische centra. Ook zijn er gesprekken gevoerd met Vereniging Hogescholen (VH) en een selectie van twaalf hogescholen. Daarnaast zijn er door EZK bestuurlijke en technische workshops georganiseerd voor de vijf instellingen voor toegepast onderzoek (de TO2-instellingen TNO, Marin, NLR, Deltares en Wageningen Research) en Wetsus. Als vervolg hierop is een serie verdiepende thematische sessies georganiseerd.

Het algemene beeld dat naar voren komt is dat het bewustzijn binnen de sector varieert. Voor een belangrijk deel laten deze verschillen zich verklaren door de verschillen in risicoprofielen van de instellingen. Bestuurders van kennisinstellingen delen over het algemeen het gevoel van urgentie rond kennisveiligheid en er is bereidheid om verantwoordelijkheid te nemen en maatregelen te treffen. Zo hebben de universiteiten gezamenlijk een kennisveiligheidskader uitgewerkt[4] en bestuurlijk trekkers voor kennisveiligheid benoemd, hebben zowel UNL als NWO werkgroepen kennisveiligheid ingesteld die het leren van elkaar bevorderen en worden er bewustwordingscampagnes gevoerd.

De kennisveiligheidsdialoog heeft bijgedragen aan het veiligheidsbewustzijn op bestuurlijk niveau binnen de kennisinstellingen. Tegelijk leverde de gesprekkenreeks het kabinet inzicht op in waar kennisinstellingen behoefte aan hebben en waar nog stappen gezet moeten worden. Zo geven bestuurders van kennisinstellingen aan dat zij behoefte hebben aan heldere kaders van de overheid en aan een loket waar zij terecht kunnen voor informatie en advies.[5] Deze inzichten zijn gebruikt bij de ontwikkeling en uitwerking van de beleidsmaatregelen.

Het is nadrukkelijk de bedoeling dat de dialoog wordt voortgezet en dat het dus niet bij één gespreksronde blijft. Het uiteindelijke doel is om kennisveiligheid door te laten dringen tot in de haarvaten van alle kennisinstellingen. Met de betrokken veldpartijen (VH, UNL, KNAW, NWO, NFU en TO2-federatie) wordt dit voorjaar uitgewerkt welke aanvullende stappen we in die richting gaan zetten.

[4] 'Kader Kennisveiligheid Universiteiten', Universiteiten van Nederland (link)
[5] Ook bij het Rondetafelgesprek over wetenschappelijke samenwerking met onvrije landen dat op 14 oktober jl. plaatsvond in de Tweede Kamer kwamen deze punten naar voren.

2.2 Nationale Leidraad Kennisveiligheid

De Nederlandse kennissector en de Rijksoverheid hebben de afgelopen maanden gezamenlijk de Nationale Leidraad Kennisveiligheid uitgewerkt. Deze is vandaag officieel gepubliceerd. Aan de totstandkoming ervan hebben de veldpartijen (VH, UNL, KNAW, NWO, NFU en TO2-federatie) en verschillende ministeries en diensten van de Rijksoverheid bijgedragen.

De leidraad is een centraal referentiedocument voor zowel de besturen van kennisinstellingen en onderzoekers als de overheid over alle aspecten die met kennisveiligheid samenhangen. Het is de bedoeling dat de leidraad kennisinstellingen en onderzoekers op weg helpt, door hen te wijzen op risico's en dreigingen en daarbij kaders en handelingsopties te schetsen. Het geeft bestuurders van kennisinstellingen een basis waarop zij hun instellingsbeleid kunnen (her)ijken. Zo draagt de leidraad zowel bij aan het bewustzijn als aan de weerbaarheid van de kennissector.

De leidraad is tevens een belangrijk brondocument voor het Rijksbrede Loket Kennisveiligheid (zie hierna, paragraaf 2.4). De Nationale Leidraad Kennisveiligheid zal een belangrijke rol spelen in bewustwordingscampagnes en bij (bestuurlijke) gesprekken over kennisveiligheid. Om de leidraad ook in internationaal verband in te kunnen zetten, wordt voorzien in een Engelse vertaling. De leidraad zal worden geactualiseerd wanneer ontwikkelingen in het dreigingsbeeld en/of de beleidsontwikkeling rond kennisveiligheid daar om vragen.

2.3 Bestuurlijke afspraken kennisveiligheid

Voor alle in de Kamerbrief kennisveiligheid aangekondigde maatregelen geldt dat samenwerking essentieel is. Actieve samenwerking met en inzet van zowel de veldorganisaties voor hoger onderwijs en (toegepast) onderzoek als alle betrokken onderdelen van de Rijksoverheid is cruciaal. Hiertoe is begin dit jaar door OCW een samenwerkingsstructuur in het leven geroepen met reguliere overleggen tussen alle betrokken partijen, zowel op bestuursniveau als op technisch niveau. Naast afstemming over maatregelen die in gezamenlijkheid worden ontwikkeld, is het bespreken van de follow-up ervan een belangrijk doel van deze structuur.

In de context van deze samenwerkingsstructuur hebben de veldpartijen en de Rijksoverheid de afgelopen periode over en weer commitment uitgesproken en afspraken gemaakt. De veldpartijen hebben actief meegewerkt aan de Nationale Leidraad Kennisveiligheid en zich er inhoudelijk aan gecommitteerd. Zij zetten zich in voor een op maat gemaakte doorvertaling binnen de eigen organisatie, rekening houdend met de specifieke kenmerken en uitgangsposities ervan. De Rijksoverheid zal daaraan bijdragen door informatie en expertise te delen, o.a. via het Rijksbrede Loket Kennisveiligheid (zie hierna), en door handvatten te bieden en kaders te stellen. Via de eerdergenoemde samenwerkingsstructuren kan de voortgang gemonitord worden en kan -waar nodig- worden bijgestuurd.

2.4 Rijksbreed Loket Kennisveiligheid

Kennisinstellingen geven aan dat zij bij het afwegen van kansen en risico's rond internationale samenwerking behoefte hebben aan informatie en advies van de Rijksoverheid. Het Rijksbrede Loket Kennisveiligheid[6] dat vandaag officieel van start is gegaan, wil tegemoet komen aan deze behoefte. Het loket is bedoeld als een laagdrempelig centraal contactpunt van de hele Rijksoverheid, waar kennisinstellingen terecht kunnen met hun aan kennisveiligheid gerelateerde vragen. Denk aan vragen rond het toelaten van buitenlandse promovendi en het

[6] www.loketkennisveiligheid.nl De huidige basissite zal de komende maanden verder worden uitgebreid.

aangaan van samenwerkingsverbanden met buitenlandse kennisinstellingen en bedrijven. Daarbij geldt dat de Rijksoverheid informatie deelt en meedenkt, maar dat de kennisinstellingen -in lijn met hun institutionele autonomie- zelf verantwoordelijk blijven.

Na een verkennende fase, begin 2021, is de Rijksdienst voor Ondernemend Nederland (RVO) gevraagd een kortlopend onderzoek (*quickscan*) uit te voeren onder kennisinstellingen om een zo concreet en praktisch mogelijk beeld te krijgen van de wensen en behoeften van de kennisinstellingen. Het eindrapport treft u aan als bijlage bij deze brief.

Het onderzoek laat zien dat er behoefte is aan informatie en advies rond uiteenlopende thema's zoals IT/cyber, samenwerkingen met buitenlandse instellingen en toelating van buitenlandse promovendi en onderzoekers. Er is behoefte aan algemene informatie maar ook aan specifieke informatie in relatie tot landen en vakgebieden en aan de mogelijkheid om te 'sparren' over twijfelgevallen. RVO adviseert daarom o.a. te benadrukken dat het loket ondersteuning biedt bij vragen over verschillende derde landen en een breed spectrum aan thema's rond kennisveiligheid. Ook moeten de medewerkers van het loket serieuze gesprekspartners zijn en niet slechts een doorverwijsfunctie krijgen.
De uitkomsten zijn betrokken bij het bepalen van de reikwijdte en werkwijze van het loket.

Na de zomer is RVO gevraagd de frontoffice van het loket in te richten waar vragen binnenkomen en zo mogelijk direct worden beantwoord. De backoffice wordt gevormd door de inhoudelijk experts van de betrokken departementen en diensten: OCW, EZK, BZ, LNV, NCTV, AIVD en MIVD. Andere onderdelen van de Rijksoverheid kunnen op ad hoc-basis betrokken worden. Het streven hierbij is steeds om binnenkomende meldingen van kennisinstellingen snel en inhoudelijk afgewogen te beantwoorden.

De basisfuncties van het loket zijn vanaf nu operationeel. Er wordt nog gewerkt aan een eigenstandige website, die dit voorjaar *live* zal gaan. De startfase wordt gebruikt om werkendeweg ervaring op te doen. In juni dit jaar is een eerste herijkingsmoment voorzien, waarbij reacties en ervaringen van alle betrokkenen (frontoffice, backoffice en veldpartijen) zullen worden meegenomen. Na de zomer 2022 zal het loket stapsgewijs verder worden doorontwikkeld. Denk aan (pro)actieve kennisdeling, ontwikkeling van praktische *tools* en trainingsmodules en (ondersteuning bij) de organisatie van bewustwordingsactiviteiten.

3. Toetsingskader ongewenste kennis- en technologieoverdracht

3.1 Toetsing van individuen

Daar waar de risico's voor de nationale veiligheid het grootst zijn, zijn verdergaande maatregelen nodig en volstaat zelfregulering niet. Zoals aangekondigd in de Kamerbrief kennisveiligheid werkt het kabinet aan een toetsingskader om ongewenste kennis- en technologieoverdracht te voorkomen. Het gaat hierbij om de toetsing van individuen die toegang willen tot kennisgebieden waarop de risico's voor de nationale veiligheid het grootst zijn, de risicovakgebieden. Denk bijvoorbeeld aan kennis die kan worden ingezet voor zowel civiele als militaire doeleinden (*dual-use*). Er wordt langs meerdere sporen aan deze maatregel gewerkt.

Daarbij wordt er gekeken naar bestaande regelgeving en processen, zoals het Verscherpt Toezicht[7] en naar ervaringen in andere landen, zoals het Verenigd Koninkrijk[8], Frankrijk[9] en Duitsland[10]. Voorop staat dat het toetsingskader juridisch houdbaar moet zijn en dat het non-discriminatiebeginsel wordt gerespecteerd.

Bij het uitwerken van een juridische basis, is een fundamentele vraag of iedereen ongeacht nationaliteit getoetst zal worden, of dat de toetsing alleen gaat gelden voor derdelanders. Vanuit het oogpunt van proportionaliteit en op grond van de actuele dreigingsanalyses, onderzoekt het kabinet een variant waarbij de kennisveiligheidstoetsing uitsluitend voor derdelanders, burgers van buiten de EU, gaat gelden. Dat betekent dat derdelanders die bij een Nederlandse kennisinstelling toegang willen tot een risicovakgebied een kennisveiligheidstoets moeten ondergaan.

Een andere fundamentele vraag betreft de afbakening van de risicovakgebieden waarop het toetsingskader van toepassing zal worden. Welke kennis en technologie is vanuit het oogpunt van nationale veiligheid risicovol? Deze vraag speelt ook bij andere beleidsinstrumenten, zoals bij exportcontrole[11] en bij het wetsvoorstel voor de investeringstoets[12].

Aangezien de afbakening van sensitieve technologieën in het kader van de investeringstoets wat de inhoudelijke insteek betreft vergelijkbaar is met de afbakening van risicovakgebieden in het kader van het toetsingskader zal het kabinet beide trajecten in beginsel parallel laten lopen. Dit draagt bij aan onderlinge synergie tussen de instrumenten en aan beleidsconsistentie.

Dit traject moet resulteren in een lijst van risicovakgebieden die politiek wordt bekrachtigd en wanneer nodig wordt geactualiseerd. Zowel bij het opstellen van de lijst als bij de vertaling ervan naar onderdelen van individuele kennisinstellingen zal het kabinet het kennisveld betrekken.

Tegelijk met de verdere uitwerking van de juridische basis en de afbakening van de risicovakgebieden zal gestart worden met het uitwerken van de uitvoeringsmodaliteiten. Zo zal er een toetsingseenheid worden ingericht die de toetsingsaanvragen zal gaan behandelen en zal er aandacht zijn voor toezichts- en handhavingsaspecten. Daarbij horen een uitvoeringstoets en een impact assessment waarbij ook de impact op het kennisveld aan de orde komt.

Zoals in de Kamerbrief kennisveiligheid al werd aangekondigd zal het toetsingskader realistisch gezien op zijn vroegst in 2023 in werking treden. Dat is, gezien de complexiteit en ingrijpendheid van de maatregel, nog altijd het uitgangspunt van het kabinet. Het kabinet onderstreept daarbij het belang van zorgvuldigheid en van draagvlak onder de Nederlandse kennisinstellingen.

3.2 Doorlichting van samenwerkingsovereenkomsten

Aan samenwerkingen van Nederlandse kennisinstellingen met buitenlandse kennisinstellingen of bedrijven kunnen risico's voor de nationale veiligheid

[7] Over het Verscherpt Toezicht in het kader van de geldende sanctieregimes tegen Noord-Korea en Iran heeft het kabinet uw Kamer laatstelijk geïnformeerd bij brief van 9 juli jl. (link) Het is de bedoeling dat het toetsingskader het Verscherpt Toezicht vervangt.
[8] Zie https://www.gov.uk/guidance/academic-technology-approval-scheme
[9] Zie http://www.sgdsn.gouv.fr/missions/protection-du-potentiel-scientifique-et-technique-de-la-nation/
[10] Zie https://www.bafa.de/SharedDocs/Downloads/EN/Foreign_Trade/ec_awareness_academia.html
[11] Exportcontrole strategische goederen (link)
[12] Wetsvoorstel Veiligheidstoets investeringen, fusies en overnames (Vifo), ingediend op 30-06-2021 (link)

verbonden zijn. Het is belangrijk dat in de onderliggende samenwerkings- of financieringsovereenkomsten deze risico's zo veel mogelijk worden gemitigeerd.

Uit eerder onderzoek[13] kwam naar voren dat kennisinstellingen niet altijd een volledig beeld hebben van de samenwerkingsovereenkomsten die in naam van hun instelling of onderdelen daarvan zijn of worden aangegaan. De Nationale Leidraad Kennisveiligheid (zie paragraaf 2.2) zegt hierover dat besturen van kennisinstellingen te allen tijde inzicht horen te hebben in de significante samenwerkingen die de organisatie aangaat, zonder daarvoor de betrokken partijen binnen de organisatie nog te moeten consulteren. Ook beschrijft de leidraad waar kennisinstellingen in ieder geval op moeten letten bij het aangaan van samenwerkingen.

Het kabinet herhaalt in deze context de eerdere oproep[14] aan kennisinstellingen om bestaande samenwerkingsovereenkomsten met buitenlandse partners (kennisinstellingen of bedrijven) tegen het licht te houden en na te gaan of fundamentele waarden hierin voldoende geborgd zijn. Waar dat niet het geval is zou het wenselijk zijn dat de afspraken op dit punt worden herzien. In voorkomende gevallen kunnen kennisinstellingen contact opnemen met het Loket Kennisveiligheid (zie paragraaf 2.4) voor informatie en advies.

In de loop van dit jaar zal bekeken worden of er naast deze vorm van versterkte zelfregulering aanvullende maatregelen nodig zijn om de risico's te mitigeren.

4. Ontwikkelingen in partnerlanden en in de EU

Kennis kent geen grenzen en hoger onderwijs en wetenschap zijn sterk internationaal georiënteerd. Zoals het kabinet in de Kamerbrief kennisveiligheid al schreef, kan een aanpak alleen effectief zijn als we samen met onze partners optrekken. Dat geldt zeker binnen de Europese Unie, waarbinnen sprake is van een gemeenschappelijke onderzoeks- en onderwijsruimte en vrij verkeer.

Tegen deze achtergrond heeft het kabinet geïnvesteerd in een internationaal netwerk, o.a. om te leren van de aanpak van andere landen en om gezamenlijk op te trekken in de internationale context. Daarbij is er aandacht voor belangrijke EU- en internationale partners zoals Duitsland, Frankrijk, het Verenigd Koninkrijk, Australië en de Verenigde Staten. De internationale gesprekken inspireren en geven inzicht in wat werkt en wat niet werkt.

In EU-verband zijn belangrijke stappen gezet om kennisveiligheid op de agenda te zetten. De Europese Commissie presenteerde op 19 mei jl. haar mededeling 'Mondiale benadering van onderzoek en innovatie'[15] waarin veel elementen uit de kabinetsaanpak rond kennisveiligheid zijn terug te vinden.
De Raad heeft deze uitgangspunten onderschreven middels Raadsconclusies die door de Raad voor Concurrentievermogen zijn aangenomen.[16] Daarmee bestaat er een gezamenlijke basis om verdere stappen in EU-verband te zetten.

De Europese Commissie heeft in deze context onlangs *Guidelines on R&I foreign interference* gepubliceerd.[17] Doel hiervan is om lidstaten én de Europese kennissector aan te sporen zelf dergelijke leidraden uit te werken. De Nationale Leidraad Kennisveiligheid die vandaag is gepresenteerd, sluit hier derhalve uitstekend op aan.

[13] Rapport "Verkenning wetenschappelijke samenwerking Nederlandse en Chinese kennisinstellingen", 2020 (link)
[14] Kamerbrief "Samenwerking met China op het gebied van onderwijs en wetenschap" van 18/12/2020 (link)
[15] Zie voor het BNC-fiche over deze mededeling (link)
[16] Conclusies Raad voor Concurrentievermogen d.d. 28 september 2020 (link)
[17] Zie https://ec.europa.eu/info/files/tackling-ri-foreign-interference

Tot slot heeft de Europese Commissie de mededeling 'Europese strategie voor universiteiten' uitgebracht.[18] In deze mededeling wordt o.a. ingegaan op internationale samenwerking in het hoger onderwijs en het belang van het borgen van waarden zoals academische vrijheid daarbij. Uw Kamer wordt hierover separaat via het reguliere BNC-fiche geïnformeerd.

Nederland zal zich actief blijven inzetten op kennisveiligheid in de EU en internationaal. Specifiek in de EU blijft Nederland inzetten op agendering, zowel richting de lidstaten als de Europese Commissie. Daarnaast kan gezamenlijk met gelijkgezinden binnen de EU een meer aanjagende rol worden opgepakt om de discussie verder te brengen en ervoor te zorgen dat ook andere landen stappen zetten om kennisveiligheid beter te borgen. De onderwijs- en wetenschapsattachés en de innovatie attachés op de Nederlandse ambassades kunnen een belangrijke rol spelen in het uitbreiden en benutten van het internationale netwerk en de informatie-uitwisseling met de internationale partners.

De EU-inzet van het kabinet is met name gericht op:
- het actief agenderen in EU-verband van kennisveiligheid;
- het vergroten van bewustwording over kennisveiligheid bij de EU-lidstaten en het Europese kennisveld;
- het -binnen de competentieverdeling- maken van concrete afspraken en het opzetten van samenwerkingsvormen op EU-niveau over kennisveiligheid;
- het onderling delen van kennis en ervaring en het zoeken van een gemeenschappelijke inzet binnen de EU en bilateraal.

5. Tot slot

Sinds de aankondiging van de kennisveiligheidsaanpak van het kabinet, in november 2020, is er veel in gang gezet. Zowel door de kennissector als door de Rijksoverheid. Het veiligheidsbewustzijn is onmiskenbaar toegenomen. Er is een breed gedeeld gevoel van urgentie rond kennisveiligheid. Er zijn zowel door de Rijksoverheid als door de kennisinstellingen initiatieven genomen die het handelingsperspectief vergroten. Daarmee is de weerbaarheid toegenomen.

Tegelijk betekent dit geenszins dat we er al zijn en we zien helaas dat er met enige regelmaat incidenten zijn die ons met dat feit confronteren. Er moeten dus nog belangrijke stappen gezet worden. De vandaag gepresenteerde Leidraad zal door de kennisinstellingen vertaald worden naar interne procedures en processen. Dit moet ertoe leiden dat het daadwerkelijk in praktijk wordt gebracht. Het veiligheidsbewustzijn kan zo doordringen tot in de haarvaten van de kennisinstellingen.
Het vandaag geopende Loket zal zich de komende tijd moeten ontwikkelen tot een snel, laagdrempelig en effectief contactpunt voor kennisinstellingen. De dialoog met de kennisinstellingen zal ook komend jaar worden voortgezet en het aangekondigde toetsingskader zal te zijner tijd de kennisveiligheid moeten borgen in die gevallen waarin zelfregulering niet afdoende is.
Het kabinet zal zich hier voor blijven inzetten en daarbij samen optrekken met gelijkgezinde landen zowel in EU-verband als bilateraal.

Deze inspanningen van het kabinet en de kennissector gezamenlijk moeten ervoor zorgen dat internationale samenwerking in het hoger onderwijs en het (toegepaste) onderzoek veilig kan plaatsvinden, met oog voor zowel de kansen

[18] Zie https://education.ec.europa.eu/document/commission-communication-on-a-european-strategy-for-universities

als de risico's, en waarbij academische kernwaarden zoals academische vrijheid steeds worden geborgd.

Het kabinet zal uw Kamer nader informeren over de voortgang bij de presentatie van de voorstellen voor het toetsingskader, voorzien voor eind dit jaar.

De minister van Onderwijs, Cultuur en Wetenschap,

Robbert Dijkgraaf

De minister van Economische Zaken en Klimaat

Micky Adriaansens

De minister van Justitie en Veiligheid

Dilan Yeşilgöz-Zegerius