31 288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

Nr. 1261 Brief van de minister van Onderwijs, Cultuur en Wetenschap

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 11 juni 2026

In deze brief informeer ik uw Kamer over de voortgang van de brede aanpak kennisveiligheid. Met deze aanpak heeft het kabinet de afgelopen vijf jaar samen met de kennissector een solide basis gevormd voor een open, veilige en toekomstbestendige wetenschap. Parallel hieraan informeer ik uw Kamer met de brief ‘Stand van zaken screening kennisveiligheid’ over het onderdeel van de aanpak dat gericht is op het tegengaan van ongewenste kennisoverdracht via personen. Met voorliggende brief bied ik u ook de evaluatie van het Loket Kennisveiligheid en het Sectorbeeld kennisveiligheid 2026 aan, en geef ik hier mijn beleidsreactie op.

Kennisveiligheid is cruciaal voor een hoger onderwijs- en wetenschapssector waarin open en veilige internationale samenwerking kan plaatsvinden. Dit is een kernwaarde voor een internationaal toonaangevende wetenschap die bijdraagt aan de uitdagingen van deze tijd. Wetenschap en onderzoek vormen het fundament voor vooruitgang. Daarom investeert het kabinet in onderzoek en wetenschap.[1] De vooraanstaande positie van de Nederlandse kennisinstellingen hangt samen met de academische vrijheid en openheid naar de wereld. Kennisveiligheid beschermt deze kernwaarden.

Dit kabinet blijft samen met de kennisinstellingen inzetten op kennisveiligheid, want de dreiging tegen de Nederlandse kennisveiligheid is onverminderd groot. Dit blijkt uit de jaarverslagen van de inlichtingen- en veiligheidsdiensten en het Dreigingsbeeld Statelijke Actoren 2025.[2] Kennis en technologie zijn geopolitieke machtsmiddelen, die landen inzetten voor het versterken van de eigen politieke, economische en militaire positie. De Nederlandse wetenschapssector is wereldwijd toonaangevend, dat maakt het een belangrijk doelwit voor statelijke actoren om strategische kennis te verwerven om hun machtspositie te

---

[1] Aan de slag – Coalitieakkoord 2026-2030
[2] Openbaar Jaarverslag MIVD 2025, Openbaar Jaarverslag AIVD 2025 en Dreigingsbeeld Statelijke Actoren 2025.

versterken ten opzichte van andere landen. De inlichtingen- en veiligheidsdiensten benadrukken dat het steeds belangrijker wordt om te identificeren welke kennis niet buiten de eigen controle moet vallen en welke belangen hierbij om bescherming vragen.

De kabinetsbrede aanpak kennisveiligheid heeft de afgelopen vijf jaar een solide basis gevormd voor het tegengaan van deze risico's. Ik wil de kennisinstellingen hierbij een compliment maken voor het werk dat zij verzet hebben om zich weerbaarder te maken. Zij hebben veel werk gemaakt van kennisveiligheid, en door de aanhoudende dreiging blijft dat ook nodig. De overheid heeft daarbij ook een belangrijke rol gespeeld. Zo blijkt uit de recente evaluatie van het Rijksbreed Loket Kennisveiligheid dat de ondersteuning vanuit het Loket van grote waarde is geweest. Het Loket biedt hulp aan kennisinstellingen met vragen over kansen, risico's en praktische zaken rondom internationale samenwerking. Verschillende ministeries en de inlichtingen- en veiligheidsdiensten bundelen hierin hun expertise en komen tot een eenduidig advies aan kennisinstellingen.

Daarnaast heeft de overheid een belangrijke rol om internationaal een gelijk speelveld te realiseren. Ik ben mij er zeer van bewust dat veiligheidsrisico's niet stoppen aan de landsgrens. Daarnaast bestaat bij elke maatregel die we binnen de eigen landsgrenzen treffen het risico dat dat ten koste gaat van het open, internationale karakter die de wetenschap kenmerkt. Het is daarom belangrijk om binnen de Europese Unie samen op te trekken met als doel om een gelijk speelveld te creëren. Ik zal mij hiervoor blijven inzetten. Onderdelen uit de Nederlandse aanpak dienen daarbij als voorbeeld. Deze voorbeelden deel ik ook actief met andere landen. De Europese Unie licht ook een aantal Nederlandse voorbeelden als good practice uit in de Research Security Monitor.[3]

Ondanks deze stappen is verdere inspanning door de overheid en kennisinstellingen noodzakelijk. Gezien de aanhoudende dreiging is het bereiken van een hoger beschermingsniveau vereist. Daarbij is de volgende stap het verankeren van kennisveiligheid op alle niveaus van de instelling en het gericht nemen van maatregelen

---

[3] European Commission: Directorate-General for Research and Innovation, *Research security monitor 2025 – Raising awareness and building resilience – Staff working document*, Publications Office of the European Union, 2026, https://data.europa.eu/doi/10.2777/4186725

waar deze het meeste nodig zijn. Ik ondersteun de kennisinstellingen hierbij met de benodigde praktische instrumenten en expertise vanuit het Loket. Ook stel ik tot en met 2031 in totaal € 80 miljoen beschikbaar aan de instellingen voor het nemen van digitale en fysieke beschermingsmaatregelen. Daarnaast ga ik samen met de instellingen kennisveiligheidsprofielen opstellen. In het najaar ga ik met de bestuurders in gesprek over het bereiken van het hogere kennisveiligheidsniveau en de monitoring van de voortgang.

Leeswijzer

Aan de hand van het sectorbeeld schets ik in deze brief eerst de stappen die kennisinstellingen de afgelopen jaar hebben gezet. Daarna geef ik verdere toelichting bij de acties die ik onderneem om kennisveiligheid verder te verankeren. Vervolgens ga ik in op het belang van een nationaal en internationaal gelijk speelveld en mijn inzet hierop. Ten slotte schets ik het vervolg op de aangekondigde acties.

1. Een solide basis - instellingen en de overheid pakken risico's aan

De kennisinstellingen boeken vooruitgang

Om inzicht te verkrijgen in de voortgang van de implementatie van kennisveiligheidsmaatregelen heb ik een meting laten uitvoeren bij de kennisinstellingen. Dit was een vervolg op de nulmeting in 2023-2024.[4] Uit het resulterende Sectorbeeld kennisveiligheid 2026 blijkt dat de aanpak van de afgelopen vijf jaar heeft geleid tot vergroting van het bewustzijn en bestendiging van kennisveiligheid in de kennissector. Universiteiten, hogescholen en onderzoeksinstituten hebben over de volle breedte vooruitgang geboekt ten opzichte van de nulmeting. Waar zij ten tijde van de nulmeting nog beleid aan het vormgeven en vaststellen waren, zijn ze dat nu aan het uitvoeren en evalueren. Kennisinstellingen gaan volwassener om met de risico's waarmee zij worden geconfronteerd bij internationale samenwerking binnen de huidige geopolitieke context.

[4] Kamerstuk 31 288, nr. 1077 (universiteiten), Kamerstuk 31288 nr. 1108 (hogescholen) en Kamerstuk 31288 nr. 1148 (KNAW/NWO).

Concreet is bij kennisinstellingen deze solide basis gevormd door:

- de verantwoordelijkheden voor kennisveiligheid binnen de instelling te beleggen;
- vaste kaders en procedures voor risico-inschattingen in te voeren;
- de vertaalslag te maken van sanctie- en exportwetgeving naar interne procedures;
- risico's te herkennen bij de werving van personeel en samenwerking tussen HR-personeel en adviesteams kennisveiligheid;
- het opstellen van centrale, actuele overzichten van internationale samenwerkingen;
- het verbreden en verdiepen van kennisveiligheidsbewustzijn door trainingen en informatievoorziening;
- het opstellen van beleid of een protocol voor buitenlandse dienstreizen, en;
- het ontwikkelen van beleid rondom fysieke en digitale beschermingsmaatregelen.

Impact van kennisveiligheid op de wetenschap

Voor kennisinstellingen is de impact van het kennisveiligheidsbeleid voelbaar, zo blijkt uit het sectorbeeld. Sommigen ervaren beperking van de academische vrijheid, bijvoorbeeld omdat er consequenties zijn voor het aangaan van samenwerkingen en aannemen van personeel. De NOS bevestigde vorig jaar dit beeld: honderden samenwerkingen en sollicitaties zijn niet doorgegaan op advies van kennisveiligheidsteams. Tegelijkertijd zien steeds meer instellingen kennisveiligheid ook als beschermende factor voor academische vrijheid en integriteit. Met zorgvuldige afwegingen kunnen zij bijvoorbeeld heimelijke

De overheid ondersteunt

Kennisinstellingen staan er niet alleen voor. Een belangrijk uitgangspunt van het kennisveiligheidsbeleid is dat instellingen zelf het beste gepositioneerd zijn om risico's te identificeren en maatregelen te nemen. De overheid ondersteunt en faciliteert hen daarbij, bijvoorbeeld met het Loket Kennisveiligheid en de gezamenlijke Leidraad Kennisveiligheid. De Leidraad biedt concrete handvatten en aandachtspunten voor instellingen om

kennisveiligheidsrisico's te identificeren en te beheersen, en is sinds de publicatie in januari 2022 uitgegroeid tot een belangrijk ankerpunt in het beleid van instellingen. Naar aanleiding van de motie Rooderkerk en Paternotte[5] heeft mijn ambtsvoorganger samen met de kennisinstellingen een landelijke set uniforme risico-indicatoren opgesteld. Deze indicatoren bieden extra houvast bij het inschatten van risico's bij het aangaan van internationale samenwerkingen.

Het Loket is volgens de voorgenoemde evaluatie een doeltreffend instrument. Via de advisering en learning community stelt het Loket bruikbare informatie en instrumenten beschikbaar aan de instellingen. De afgelopen vier jaar heeft het Loket ruim 640 adviezen gegeven over bijvoorbeeld risico's op overdracht van kennis en technologie die kan leiden tot ongewenste militaire toepassingen. Daarnaast organiseert het Loket met de learning community workshops en themasessies over bijvoorbeeld personeelsbeleid. Hiermee faciliteert het Loket kennisuitwisseling tussen de overheid en instellingen, en instelling onderling. Ook stelt het Loket informatie beschikbaar op het digitale platform. Deze activiteiten hebben de afgelopen jaren eraan bijgedragen dat kennisinstellingen adequaat omgaan met kennisveiligheidsrisico's. Tegelijkertijd laten de evaluatie en het sectorbeeld zien dat kennisinstellingen behoefte hebben aan concrete ondersteuning bij complexe casuïstiek, scherpere duiding van sancties en sensitieve technologie en een laagdrempelige sparringpartner. Ook hebben ze behoefte aan concrete en hanteerbare bronnen bij het maken van gerichte risico-afwegingen van affiliaties en de sensitiviteit van onderzoeksthema's. Het evaluatierapport biedt hiervoor nuttige aanbevelingen, die ik zal opvolgen. In paragraaf 2 ga ik hier verder op in.

De in deze brief beschreven maatregelen tegen ongewenste kennis- en technologieoverdracht staan niet op zichzelf. Ongewenste kennisoverdracht kan ook op andere manieren plaatsvinden, zoals via spionage of digitale aanvallen. Vanaf 15 mei 2025 geldt dat meer vormen van spionage strafbaar zijn. Het lekken van gevoelige informatie, ook al is deze niet staatsgeheim, en het handelen in opdracht van een buitenlandse overheid, is nu strafbaar als het de Nederlandse belangen ernstig kan schaden.[6]

---

[5] Kamerstuk 31 288, nr. 1134
[6] Uitbreiding strafbaarstelling spionage

Daarnaast werk ik aan de uitwerking van de aanwijzing van hogescholen en universiteiten onder de Cyberbeveiligingswet. Hierover informeer ik uw Kamer voor de zomer.

2. Gerichte aanpak voor de verankering van kennisveiligheid

Ik wil samen met de instellingen en mijn ambtsgenoten in het kabinet nu verder bouwen op de basis die we met elkaar hebben gelegd. Dat doen we door een bewuste omgang met risico's verder te verankeren op alle niveaus binnen de kennisinstellingen. En dit doen we heel gericht. Samen met de kennisinstellingen zet ik in op gerichte maatregelen waar deze het meeste nodig zijn, gebaseerd op de risico's, belangen en de reeds genomen maatregelen. Uit het sectorbeeld blijkt ook dat kennisinstellingen die meer risico's identificeren, de ambitie uitspreken om tot een hoger niveau van volwassenheid te komen. Ik moedig dit aan, want het is belangrijk dat kennisinstellingen die te maken hebben met meer risico's, passende maatregelen nemen. Dit draagt bij aan de gerichte aanpak.

Concreet onderneem ik de volgende acties:

1. *Kennisveiligheidsprofielen*
   Ik start dit jaar in samenwerking met de instellingen en externe professionals met het opstellen van landelijke kennisveiligheidsprofielen aan de hand waarvan instellingen ingedeeld kunnen worden. Dit doen we zoveel mogelijk op basis van reeds beschikbare informatie en risicoanalyses. Daarmee ondersteun ik de al ingezette koers van het nemen van maatregelen waar deze het meest nodig zijn, op basis van risico's, belangen en genomen maatregelen. Dit zorgt er ook voor dat instellingen die weinig kennisveiligheidsrisico's kennen, proportionele lasten dragen en daar minder werkdruk van ondervinden. Instellingen met een zwaarder profiel kan ik gerichter ondersteunen.

2. *Herziene Nationale Leidraad Kennisveiligheid*
   Samen met de sector heb ik de Nationale Leidraad Kennisveiligheid herzien, zodat deze handvatten blijft bieden voor een volwassener sector. In samenwerking met de inlichtingen- en veiligheidsdiensten is ook het dreigingsbeeld in de Leidraad geüpdatet. Ik publiceer deze Leidraad begin

juli 2026 op de website van het Loket Kennisveiligheid.[7] De koepels brengen deze breed onder aandacht bij de instellingen.

3. *Versterken Loket Kennisveiligheid*
   Ik ga het Loket Kennisveiligheid versterken met een expertisecentrum, zoals naar voren is gekomen in de evaluatie. Dit doe ik binnen de budgettaire kaders van het kennisveiligheidsbeleid. Het Loket kan alleen van meerwaarde blijven als het zijn toegevoegde waarde vergroot. Daarvoor versterk ik bij het Loket zelf de brede expertise over sanctie- en exportwetgeving en (sensitieve) technologieën. Ook gaat het Loket diverse praktische instrumenten beschikbaar stellen aan de instellingen.

   Daarnaast heeft uw Kamer met de motie Martens-America de regering verzocht om te onderzoeken of het wenselijk is dat het Loket Kennisveiligheid de instellingen ongevraagd en proactief te informeren over risico's.[8] Op basis van de genoemde evaluatie concludeer ik dat dit inderdaad het geval is, daarom gaat het Loket dit doen. Daarmee is invulling gegeven aan de motie Martens-America.

4. *Wettelijke verankering Loket*
   In het verlengde van dit voornemen werk ik aan het wettelijk verankeren van de adviestaak van het Loket. Een wetsvoorstel hiervoor is in openbare internetconsultatie geweest.[9] Dit betreft een tijdelijke wet, want het Loket is een tijdelijk instrument. Ik zet mij ervoor in om dit wetsvoorstel voor het eind van dit jaar aan te bieden aan de Tweede Kamer.

   Ook ga ik onderzoeken of het nodig is en wat nodig is om het Loket een structurele plek in de aanpak kennisveiligheid te geven. Dit ga ik doen binnen de budgettaire kaders van het kennisveiligheidsbeleid.

5. *Financiële impuls*

---

[7] https://www.loketkennisveiligheid.nl/documenten/2026/06/04/nationale-leidraad-kennisveiligheid-2026
[8] Kamerstuk 31 288, nr. 1130
[9] https://www.internetconsultatie.nl/adviseringkennisveiligheid/

Om instellingen op weg te helpen bij hun uitdagingen op het vlak van kennisveiligheid en cyberveiligheid investeert dit kabinet tot en met 2031 in totaal € 80 miljoen.[10] De middelen worden via de Rijksbijdrage beschikbaar gesteld aan de universiteiten, hogescholen, umc's en de instituten van KNAW en NWO. Deze middelen helpen instellingen om werk te maken van fysieke en digitale maatregelen ter bescherming van kennisontwikkeling en internationale samenwerking. Dit is in aanvulling op de eerdere € 17,6 miljoen die mijn ambtsvoorganger beschikbaar heeft gesteld.[11] Deze financiële impuls van € 80 miljoen kunnen instellingen onder andere inzetten om zich voor te bereiden op de invoering van de Cyberbeveiligingswet.

6. *Gewenst kennisveiligheidsniveau*
   Ik ga in het najaar met de bestuurders van de instellingen in gesprek over het bereiken van het gewenste kennisveiligheidsniveau, dat door henzelf is geïdentificeerd bij de vervolgmeting. Daarbij ga ik hen uitnodigen om met voorstellen te komen over hoe de voortgang te monitoren en hoe zij dit inzichtelijk maken. Ik vertrouw erop dat de bestuurders ook met hun raden van toezicht hierover in gesprek gaan. Voor het einde van het jaar informeer ik uw Kamer over de uitkomsten hiervan.

7. *Interventies*
   Ik maak gebruik van mijn bestaande bevoegdheden om stappen te zetten als een kennisinstelling een internationale samenwerking wil aangaan waarbij het kabinet toch een risico ziet voor de nationale veiligheid. Deze interventiemogelijkheden zijn uiteengezet in het Stroomschema ongewenste overdracht kennis en technologie, dat mijn ambtsvoorganger heeft opgesteld op verzoek van het lid Martens-America in het commissiedebat kennisveiligheid van 30 januari 2025.[12]

8. *Haalbaarheidsanalyse screening*
   De komende tijd voer ik een haalbaarheidsanalyse uit naar een screening kennisveiligheid in aangepaste, meer

---

[10] Zoals aangekondigd in mijn Beleidsbrief Onderwijs Cultuur en Wetenschap 2026-2030, 24 april 2026, Kamerstuk 36800-VIII, nr. 148
[11] https://www.rijksfinancien.nl/memorie-van-toelichting/2025/OWB/VIII
[12] Stroomschema ongewenste overdracht kennis en technologie, 13 juni 2025. Bijlage bij Kamerstuk 31 288, nr. 1205

beperkte en gerichtere vorm. Deze screening is gericht op het beperken van het risico op ongewenste kennisoverdracht door personen. Gelijktijdig met deze brief informeer ik uw Kamer met de brief ‘Stand van zaken screening kennisveiligheid’ hierover.

3. Een gelijk speelveld is onmisbaar

Het bereiken van een internationaal én nationaal gelijk speelveld blijft een belangrijke pijler van onze bredere inzet op kennisveiligheid. Voor het behouden van toponderzoek in de Nederlandse wetenschapssector en veiligheidsrisico’s te verminderen, is het belangrijk dat kennispartners maatregelen nemen die een gelijk doel hebben: het tegenaan van risico’s. Kennisinstellingen en het kennisintensieve bedrijfsleven zijn in hoge mate met elkaar verweven. Daarom trek ik samen op met de ministers van EZK, BZ, JenV en andere leden van het kabinet.

Voor een internationaal gelijk speelveld heeft Nederland de afgelopen jaren gewerkt aan de inzet op kennisveiligheid in de EU en internationaal. Dit is vooral van belang bij EU-lidstaten en gelijkgezinde landen, waarmee de Nederlandse wetenschapssector veel samenwerkt. Om dit gelijke speelveld te bevorderen, heb ik kennisveiligheid geagendeerd bij internationale gremia, bijvoorbeeld binnen de EU bij de Raad voor Concurrentievermogen, bij de OESO, de G7 en in bilaterale gesprekken. Daarmee geef ik invulling aan de motie Paternotte en Martens-America om kennisveiligheid te agenderen voor de Raad voor Concurrentievermogen.[13]

Internationaal bevorder en steun ik een aantal initiatieven zoals de Raadsaanbeveling Onderzoeksveiligheid (mei 2024), de Research Security Monitor (februari 2026), de opzet van het Centre of Expertise en een Europees due diligence platform, kennisveiligheidsmaatregelen in Europese richtlijnen en verordeningen zoals de ERA Act en KP10 (het nieuwe Europese kaderprogramma voor 2028-2034). Daarnaast moedig ik initiatieven aan van de kennisinstellingen om ook internationaal meer kennis en best practices uit te wisselen, zoals bijvoorbeeld de ENCORS conferentie die 26 en 27 mei heeft plaatsgevonden bij de

[13] Kamerstuk 31288, nr. 1178

TU Delft. Hierbij kwamen meer dan 500 personen uit 32 landen bijeen om kennis uit te wisselen over kennisveiligheid. Het delen van beleidsupdates en uitwisselen van best practices versterkt en verrijkt onze nationale beleidsmaatregelen.

Vervolg

Na de zomer informeer ik uw Kamer over de voortgang van de haalbaarheidsanalyse naar een screening kennisveiligheid in aangepaste, meer beperkte en gerichtere vorm, die het risico op ongewenste kennisoverdracht door personen moet beperken. Zie hiervoor mijn brief ‘Stand van zaken screening kennisveiligheid’. Ook informeer ik uw Kamer dan over de stand van zaken van de onder paragraaf 2 beschreven acties en de behaalde resultaten.

De minister van Onderwijs, Cultuur en Wetenschap,
R.M. Letschert