31288 Hoger Onderwijs-, Onderzoek- en Wetenschapsbeleid

Nr. 1205 Brief van de minister van Onderwijs, Cultuur en Wetenschap

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 13 juni 2025

Wetenschap floreert bij open internationale samenwerking waarin wetenschappers onafhankelijk en in vrijheid hun werk kunnen doen. Daarin kunnen er helaas ook risico's voor de nationale veiligheid ontstaan bijvoorbeeld wanneer specifieke actoren toegang of invloed krijgen op sensitieve kennis en technologie. In de kabinetsbrede aanpak voor kennisveiligheid streeft het kabinet daarom naar de balans tussen maximale openheid en maatregelen die voor de nationale veiligheid noodzakelijk zijn.

In voorgaande brieven[1,2] heb ik uw Kamer geïnformeerd over een aantal grote ontwikkelingen in de kabinetsbrede aanpak voor kennisveiligheid sinds de start van deze regeerperiode. Daarin heb ik uw Kamer bijvoorbeeld geïnformeerd over de vorderingen ten aanzien van het wetsvoorstel Screening Kennisveiligheid en de start van de internetconsultatie. Deze brief vult daar op aan door uw Kamer te informeren over een aantal recente vorderingen en de uitvoering van een aantal moties en toezeggingen op het gebied van kennisveiligheid.[3,4,5]

1. Nationale Leidraad Kennisveiligheid, overzichten en uniforme risico-indicatoren

Kennisinstellingen hebben een belangrijke rol binnen de kabinetsbrede aanpak. Met hulp van de Rijksoverheid zijn juist kennisinstellingen in positie om de balans te vinden tussen kansen en risico's en om risicogerichte maatregelen te treffen binnen de eigen organisatie. De Nationale Leidraad Kennisveiligheid (hierna: Leidraad Kennisveiligheid) vormt daarin een belangrijke schakel. De Leidraad Kennisveiligheid is een gezamenlijk instrument van de Rijksoverheid en de kennissector, en biedt concrete handvatten en aandachtspunten voor het kennisveiligheidsbeleid van instellingen. In lijn met de aankondiging in de brief van 25 oktober 2024 heb ik

[1] Kamerstuk 31 288 nr. 1158 (voortgangsbrief oktober 2024)
[2] Kamerstuk, 31 288 nr. 1187 (aankondiging consultatiefase wetsvoorstel)
[3] Tweede Kamer, TZ 202501-136 (toezegging stroomschema kennisveiligheid)
[4] Kamerstuk 31 288 nr. 1158 (aankondiging actualiseren Leidraad)
[5] Kamerstuk 31 288 nr. 1134, Motie Rooderkerk en Paternotte

samen met de sector gewerkt aan het actualiseren van de Leidraad Kennisveiligheid op een drietal onderdelen. Deze onderdelen zijn gekozen als opvolging van de urgentste aandachtspunten in de sectorbeelden kennisveiligheid (2023 en 2024) en in het AWTI-advies *'Kennis in conflict'* (2022). Een vierde onderdeel komt voort uit de uitvoering van de motie Rooderkerk en Paternotte.[6] De actualisatie is op deze punten met succes afgerond.

In deze actualisatie is ten eerste de definitie van kennisveiligheid verduidelijkt. Ten tweede gaat de Leidraad Kennisveiligheid nu dieper in op de omgang met kennisveiligheid in het personeelsbeleid. Ten derde zijn er uitgangspunten voor het bijhouden van overzichten van risicovolle samenwerkingen toegevoegd. In lijn met het eerste deel van de motie Rooderkerk en Paternotte[7] beschikken inmiddels alle universiteiten over deze overzichten en worden ze intern gebruikt in het kennisveiligheids-beleid.

Ten vierde heb ik 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. Deze set is als bijlage bij deze brief opgenomen en vormt een appendix bij de Leidraad Kennisveiligheid. Hiermee heb ik uitvoering gegeven aan het tweede deel van de motie Rooderkerk en Paternotte.[8]

Ik heb met de sector afgesproken om dit jaar ook de rest van de Leidraad Kennisveiligheid te actualiseren. De huidige versie stamt uit 2022, en kwam tot stand vanuit de theorie. Inmiddels zitten we midden in de praktijk en heeft de eerste fase van de herziening laten zien dat er voor meer onderdelen een kans ligt om concrete kennis en ervaring voor de Leidraad Kennisveiligheid te benutten. Daarmee zorgen we er samen voor dat de Leidraad Kennisveiligheid ook op de rest van de onderdelen blijft aansluiten bij de ontwikkelingen en uitdagingen waar instellingen dagelijks aan werken. Ik verwacht voor het einde van dit jaar de voortgezette actualisatie af te ronden en een geheel vernieuwde versie te kunnen publiceren.

2. Stroomschema kennisveiligheid

Tijdens het commissiedebat kennisveiligheid van 30 januari 2025 ben ik door het lid Martens-America gevraagd naar de mogelijkheden om in te grijpen wanneer er door wetenschappelijke samenwerking toch een gevaar zou ontstaan voor de nationale

---

[6] Kamerstuk 31 288 nr. 1134
[7] Kamerstuk 31 288 nr. 1134
[8] Kamerstuk 31 288, nr. 1134

veiligheid. Ik heb daarop toegezegd om uw Kamer te informeren over de stappen die ik in dat geval kan zetten. In deze brief zal ik daar op ingaan. Ter ondersteuning heb ik in de bijlage een schematische weergave opgenomen. Ik beschrijf de feitelijke situatie op dit moment en de situatie zodra de voorgenomen Wet screening kennisveiligheid in werking is getreden.[9,10]

De dreiging op het gebied van kennisveiligheid blijft onverminderd groot is. Er zijn nog steeds verschillende statelijke actoren die kennis en technologie als strategisch machtsmiddel inzetten en openlijk of heimelijk in Nederland kennis proberen te verwerven. Hiermee proberen zij hun eigen positie te verbeteren en strategische afhankelijkheden te verminderen. Met de kabinetsbrede aanpak van kennisveiligheid hebben we samen met het kennisveld de afgelopen jaren veel stappen gezet om weerbaar te zijn tegen deze dreiging, en onze wetenschap tegelijkertijd zo open mogelijk te houden.

Ons hoger onderwijs- en wetenschapsstelsel kent een hoge mate aan institutionele autonomie. Ook in de aanpak van kennisveiligheid is én blijft dit een belangrijk uitgangspunt. Kennisinstellingen zijn zelf verantwoordelijk voor hun beleid en keuzes op het gebied van kennisveiligheid. De instelling is bij uitstek de plek waar per casus een bewuste afweging gemaakt kan worden tussen de kansen én risico’s van een internationale samenwerking. Zo worden zoveel mogelijk kansen benut en dragen kennisinstellingen optimaal bij aan de samenleving. Kennisinstellingen hebben hiervoor adviesteams ingesteld, beleid ontwikkeld en bestuurlijk portefeuillehouders aangewezen. Ik zie bovendien dat het risicomanagementsysteem van kennisinstellingen steeds meer is ingericht op specifieke vraagstukken op het gebied van kennisveiligheid.[11] Kennis-instellingen kunnen ervoor kiezen om gebruik te maken van expertise van de Rijksoverheid via het Loket Kennisveiligheid. Het is aan de kennisinstelling om, eventueel aan de hand van advies van het Loket Kennisveiligheid, te besluiten of de internationale samenwerking kan worden aangegaan en welke mitigerende maatregelen daarbij zo nodig genomen moeten worden.

---

[9] Kamerstuk 31 288, nr. 1187

[10] Het stroomschema en de beschrijving in deze brief is van toepassing op alle kennisinstellingen die onder de stelselverantwoordelijkheid van de Minister van Onderwijs, Cultuur en Wetenschap vallen.

[11] Uit de sectorbeelden kennisveiligheid voor universiteiten (2023), hogescholen (2024) en NWO-I en KNAW (2024) blijkt dat kennisinstellingen belangrijke stappen hebben gezet om de Nationale Leidraad Kennisveiligheid te implementeren. De meting wordt in 2025 en 2026 herhaald.

Het kan voorkomen dat een kennisinstelling een internationale samenwerking wil aangaan waarbij het kabinet toch een risico ziet voor de nationale veiligheid. Bijvoorbeeld wanneer de inlichtingen- en veiligheidsdiensten hierop wijzen of wanneer het kabinet zorgen heeft over iets wat wordt waargenomen bij een instelling. Academische vrijheid en institutionele autonomie zijn niet onbegrensd wanneer het de veiligheid raakt. In dat geval ga ik, vanuit mijn stelselverantwoordelijkheid en in lijn met de bestuurlijke verhoudingen, hierover in gesprek met het bestuur van de kennis-instelling. Ik zal dan aangeven welke risico's het kabinet ziet, vragen naar de risico-inschatting van de instelling en bespreken welke maatregelen de kennisinstelling voornemens is te nemen om risico's te mitigeren. Het kan gebeuren dat een instellingsbestuur na dergelijke gesprekken zou vasthouden aan een risicovolle internationale samenwerking en het gesprek de zorgen niet wegneemt. In dat geval zijn er afhankelijk van de situatie verschillende (formele) vervolgstappen denkbaar waarin het risico en mogelijke maatregelen verder kunnen worden onderzocht.

In de specifieke situatie dat er een vermoeden is van spionage, zoals neergelegd in het Wetboek van Strafrecht, zal ik het Openbaar Ministerie informeren. Als er sprake is van een vermoeden van overtreding van internationale sancties kan ik de betreffende handhavende autoriteit (bijvoorbeeld de FIOD) op de hoogte brengen. Zij beslissen vervolgens eigenstandig over de eventueel te nemen verdere stappen. In andere gevallen bespreek ik de zorgen van het kabinet met de raad van toezicht van de kennisinstelling, als zijnde werkgever van het instellingsbestuur.

Op basis van specifieke sanctiewet- en regelgeving heb ik rechtstreekse eigen bevoegdheden als het gaat om de toelating van personen. Als een vakgroep valt onder het verscherpt toezicht is een kennisinstelling verplicht om voor alle studenten, onderzoekers en ander personeel, van die betreffende vakgroep, te verzoeken om een ontheffingsbesluit of een advies te krijgen van de taskforce verscherpt toezicht Kennisembargo. Als een ontheffingsbesluit wordt geweigerd, mag de kennisinstelling de betreffende persoon geen toegang geven. Zodra de voorgenomen Wet screening kennisveiligheid in werking treedt, wordt een screening vooraf verplicht gesteld voor een groter aantal vakgebieden dan in het huidige verscherpt toezicht. Mijn bevoegdheden worden daarmee uitgebreid, omdat ik dan voor alle personen die toegang willen tot een hoog-risico onderdeel binnen een sensitief vakgebied een bindend besluit neem over de toegang.

In het hiervoor beschreven stroomschema is de eigen verantwoordelijkheid van de kennisinstelling het leidende principe. In mijn ervaring volstaat dat uitgangspunt. Het bewustzijn en de

zelfregulering van kennisinstellingen op het gebied van kennisveiligheid is aantoonbaar gegroeid in de afgelopen jaren.[12] Instellingen laten zien dat zij bewust zijn van het feit dat vrijheid zonder verantwoordelijkheid niet bestaat.[13] Daarmee vertrouw ik er op dat instellingen daadkrachtig en adequaat handelen wanneer zij op risico's voor de nationale veiligheid worden gewezen. Het blijft noodzakelijk om samen met de kennisinstellingen op te trekken in de aanpak van kennisveiligheid, daarbij zo scherp mogelijk risicogericht te werk te gaan en afhankelijk van de casus te bekijken of het nodig is de in het stroomschema beschreven mogelijke stappen te zetten.

Daar waar de risico's voor de nationale veiligheid het grootst zijn, zijn extra bevoegdheden voor de overheid nodig. In het eerder genoemde Dreigingsbeeld Statelijke Actoren wordt de dreiging van de *insider threat* voor de kennisveiligheid benoemd: de overdracht van sensitieve kennis en technologie via onderzoekers of andere medewerkers en studenten die studeren of werken binnen Nederlandse kennisinstellingen. Daarom geef ik prioriteit aan een zorgvuldige invoering van het wetsvoorstel screening kennisveiligheid, dat als doel heeft om deze overdracht zoveel mogelijk te voorkomen. Ik doe dit in aanvulling op de blijvende inzet om bewustwording van kennisveiligheidsrisico's en zelfregulering in de kennissector te stimuleren en ondersteunen.

Ik heb onlangs ook met uw Kamer gesproken over (sociale) veiligheid op kennisinstellingen.[14] In aanvulling op dit stroomschema voor kennisveiligheid heeft het lid Martens-America mij gevraagd een soortgelijk overzicht te geven in het geval van een bedreiging van de veiligheid van studenten en personeel, zoals in het geval van protesten. Bijvoorbeeld wie er verantwoordelijk is en wie er kan ingrijpen wanneer een protest escaleert. Voor de zomer zal ik uw Kamer per brief informeren over de uitvoering van diverse moties en toezeggingen op het gebied van veiligheid. Daarin zal ik ook ingaan op escalatiemechanismes bij protesten.

3. Stand van zaken verscherpt toezicht

De ongewenste overdracht van kennis en technologie speelt niet alleen een rol binnen de kabinetsbrede Aanpak Kennisveiligheid. Op het gebied van sanctienaleving hebben kennisinstellingen daar al

---

[12] Sectorbeelden kennisveiligheid voor universiteiten (2023), hogescholen (2024) en NWO-I en KNAW (2024).
[13] Verklaring over Academische Vrijheid – De rectoren van de Nederlandse universiteiten (2025).
[14] Bijvoorbeeld tijdens het plenair debat over de veiligheid op universiteiten van 23 januari 2025 en tijdens het commissiedebat over hoger onderwijs en DUO van 23 april 2025.

langer mee te maken. Op grond van internationale sancties is het verboden om bepaalde kennis en technologie over te dragen naar gesanctioneerde landen, in tegenstelling tot de aanpak kennisveiligheid spelen kansen geen rol. Het naleven van deze verboden is de eigen verantwoordelijkheid van de instellingen.

Voor een drietal sanctieregelingen (Iran, Noord-Korea en Rusland) ondersteunt de overheid kennisinstellingen bij de naleving. Dit is een samenwerking van de ministers van Buitenlandse Zaken (BZ) en Onderwijs, Cultuur en Wetenschap. In 2019 is de taskforce verscherpt toezicht kennisembargo in het leven geroepen om vorm te geven aan het verscherpen van toezicht op studenten en onderzoekers in gevoelige onderwijs- en onderzoeksgebieden. Doel is om bepaalde gevoelige kennis te beschermen.

De basis van dit verscherpte toezicht zijn de sanctieverordeningen van Iran (EU Vo. 2012/267) en Noord-Korea (EU Vo. 2017/1509). Sinds 1 augustus 2024 valt ook de sanctieverordening Rusland (EU VO. 833/2014) onder verscherpt toezicht. De reikwijdte van deze toetsing is daarmee niet uitgebreid, het zijn nog steeds dezelfde onderwijs- en onderzoeksgebieden. De taskforce ondersteunt kennisinstellingen door een deel van de taken over te nemen bij het naleven van de verboden van de hierboven genoemde sanctieverordeningen. Dit betekent dat vooraf wordt onderzocht of er met de toegang van een specifiek persoon een risico bestaat dat de kennisinstelling daarmee direct of indirect verboden technische bijstand levert. Bij Noord-Korea en Rusland levert de taskforce een besluit af dat bindend is, bij Iran betreft het een advies, daar er geen kennisembargo op Iran bestaat.

Uitvoering verscherpt toezicht gaat op in wet screening kennisveiligheid

Het verscherpt toezicht zal als zelfstandig uitvoeringsinstrument ophouden te bestaan zodra het opgaat in de uitvoering van de screening kennisveiligheid. Op

7 april jl. heb ik uw Kamer geïnformeerd over de stand van zaken van het wetsvoorstel dat deze screening introduceert.[15] De uitvoering van de screening kennisveiligheid is daarmee naar verwachting ook een efficiënte en effectieve manier om uitvoering te geven aan het Verscherpt toezicht.

Proces verscherpt toezicht afgelopen jaren verbeterd

[15] Kamerstuk 31 288, nr. 1187.

In 2021 is uw Kamer geïnformeerd over de eerste evaluatie van de taskforce verscherpt toezicht kennisembargo.[16] Daarmee is de professionalisering van het verscherpt toezicht ingezet. Zo is de doorlooptijd verkort van 5,2 weken in 2020 naar 2,8 weken in 2024. In de periode 2019-2024 zijn 2019 aanvragen gedaan voor een ontheffing van het kennisembargo. Dit heeft in twee gevallen geleid tot een afwijzing of andere reden om niet tot ontheffing te komen. Ten aanzien van de Iran-sanctieverordening wordt geen ontheffing verleend, maar een advies gegeven aan de kennisinstelling. In 13 van de 2019 aanvragen heeft dit geleid tot een verhoogd risicoadvies.

Per 1 november 2023 heb ik het gecoördineerd opdrachtgeverschap overgenomen van de minister van Buitenlandse Zaken.[17] Daarmee zijn de taken uitgevoerd door het OCW-loket Kennisembargo en de taskforce verscherpt toezicht kennisembargo onder mijn uitvoeringsverantwoordelijkheid komen te vallen. Daarbij blijft de inzet van BZ noodzakelijk om deze verantwoordelijkheid te vervullen. Bij de overdracht van het opdrachtgeverschap zijn hierover afspraken vastgelegd.

Dat verscherpt toezicht instellingen ondersteunt, betekent niet dat sanctienaleving voor kennisinstellingen eenvoudig is. Kennisinstellingen geven aan dat het stelsel van sanctieverordeningen erg complex is en dat het van hen aanzienlijke deskundigheid vergt om de sanctieverordeningen effectief te implementeren. Instellingen geven aan dat informatievoorziening, versimpeling en harmonisatie cruciaal zijn voor een uitvoerbare en effectieve sanctienaleving. Deze behoefte begrijp ik. Ik ben daarom blij dat deze knelpunten onderdeel zijn van de toonzettende Nederlandse inzet op het gebied van sanctienaleving in Europees verband.[18]

Met de kennisinstellingen die vallen onder het verscherpt toezicht[19] ben ik bovendien in gesprek over de doorontwikkeling van het verscherpt toezicht zelf. Dit gesprek draagt er aan bij de ervaring van instellingen met sancties en het verscherpt toezicht zichtbaar te

---

[16] Evaluatie Taskforce ongewenste kennisoverdracht, 6 juli 2021, ABD TOPConsult.
[17] Kamerstuk 30 821, nr. 152.
[18] Strengthening European cooperation to reinforce national efforts on the implementation and enforcement of EU restrictive measures. Non-paper by the Netherlands, November 2024. Bijlage bij Kamerstukken 36 600 V, 2024/25 “Vaststelling van de begrotingsstaat van het Ministerie van Buitenlandse Zaken (V) voor het jaar 2025”
[19] https://www.rijksoverheid.nl/onderwerpen/hoger-onderwijs/vraag-en-antwoord/waarom-heb-ik-een-ontheffing-nodig-voor-bepaalde-technische-nucleaire-studies

maken en te begrijpen, en om verbeterpunten te identificeren. Een belangrijk thema in de gesprekken is de herziening van de lijst van instellingsonderdelen die onder het verscherpt toezicht vallen. De komende tijd onderzoek ik samen met BZ en de betrokken kennisinstellingen hoe dit kan worden vormgegeven.

De minister van Onderwijs, Cultuur en Wetenschap,
E.E.W. Bruins