SCHRIFTELIJKE VRAAG

nr. 74
van **KARL VANLOUWE**
datum: 22 november 2024

---

aan **MATTHIAS DIEPENDAELE**
MINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN ECONOMIE, INNOVATIE EN INDUSTRIE, BUITENLANDSE ZAKEN, DIGITALISERING EN FACILITAIR MANAGEMENT

Vlaamse universiteiten en risicovolle Chinese universiteiten - Toenemende samenwerking

Op 10 oktober lazen we op de voorpagina van De Tijd dat volgens een studie van de Koninklijke Militaire School (KMS) Vlaamse onderzoekers steeds meer gevoelige onderzoeken doen met risicovolle universiteiten in China. Die universiteiten hebben links met bijvoorbeeld het Volksbevrijdingsleger of de Chinese inlichtingendiensten en op die manier worden Vlaams-Chinese onderzoeken misbruikt voor spionage, kernwapenprogramma's tot zelfs het ontwikkelen van technologie waarmee China controle uitoefent op etnische minderheden.

Het is niet enkel problematisch dat dit soort onderzoeken plaatsvindt, maar ook dat hun aantal ook nog eens toeneemt: het afgelopen jaar zijn de publicaties met Chinese universiteiten die een 'hoog' of 'zeer hoog' risico vormen, verdubbeld ten opzichte van 2016. Het aantal onderzoeken naar technologie die volgens de normen van de Europese Commissie als 'kritiek' bestempeld worden, steeg van 145 in 2016 naar 373 afgelopen jaar.

Dat soort onderzoeken laat jammer genoeg niets aan de verbeelding over. Zo verscheen vorig jaar een gezamenlijk onderzoek over manieren om turbines robuuster te maken. Dat onderzoek vond plaats met het Harbin Institute of Technology, een van de zeven 'Seven Sons of National Defense'-universiteiten. Deze Chinese universiteiten spenderen minstens de helft van hun onderzoeksbudgetten aan militaire toepassingen en onderzoekers van de KMS waarschuwen dat dit onderzoek misbruikt zal worden om efficiëntere straalmotoren te maken voor gevechtsvliegtuigen. Een ander voorbeeld is een samenwerking van dit jaar met de Beihang University, een andere 'Seven Sons of National Defense'-universiteit,naar drones met onder andere een techniek die kan worden misbruikt om vijandige luchtafweerverdediging te detecteren.

Gelukkig staat Vlaanderen niet stil: door de groeiende, geopolitieke veranderingen startte twee jaar geleden onder het Departement Economie, Wetenschap en Innovatie (EWI) een nieuwe werkgroep Kennisveiligheid die een concreet beleidskader moet uitwerken rond kennisveiligheidsbeleid. Op 1 december 2023 liet de Vlaamse Regering weten dat het niet langer nieuwe samenwerkingen met de Chinese 'Sevens Sons of Defense' toelaat.

Bij de parlementaire vragen over kennisveiligheid in de vorige regeerperiode kwam de uitbouw van een kennisveiligheidsloket steeds meer ter sprake. Dat loket zou moeten dienen om bijvoorbeeld kenniscentra te helpen met de analyse en inschatting van de balans tussen opportuniteit en risico van een specifieke samenwerking met een buitenlands kenniscentrum. Een concrete uitwerking van het loket bleef vorige zittingsperiode uit, maar

de uitbouw van een kennisveiligheidsloket werd opnieuw bevestigd in het Vlaamse regeerakkoord.

Gezien de alarmerende vaststelling van toenemende samenwerking met risicovolle universiteiten, wil ik de minister-president een aantal vragen stellen.

1. Hoe ver staat de werkgroep Kennisveiligheid met de uitbouw van een Vlaams kennisveiligheidsbeleid dat ondertussen twee jaar geleden van start ging? Ondanks het verbod op nieuwe samenwerkingen met de 'Seven Sons of Defense'-universiteiten, blijven er samenwerkingen plaatsvinden met die universiteiten die kwalijke gevolgen kunnen hebben.

   Zouden alle samenwerkingen met dat soort universiteiten niet gescreend moeten worden en eventueel verboden om dat soort zaken te voorkomen?

2. De functionele invulling van het kennisveiligheidsloket werd vorige legislatuur vertraagd door de intra-Belgische overleggroep.

   Vond er al een overleg plaats dat klaarheid schept over deze invulling? Kan er een stand van zaken gegeven worden over het kennisveiligheidsloket?

3. Zijn er naast het uitbouwen van een Vlaams kennisveiligheidsloket andere zaken gepland rond kennisveiligheid? Zo werd deze zomer de 'Corporate Sustainable Due Diligence'-richtlijn (CS3D) aangenomen in het Europees Parlement, die grote bedrijven verplicht een 'gepaste voorzichtigheid' te hanteren voor kennis en technologie die gebruikt worden voor militaire of 'dual use'-producten.

   Zal de Vlaamse Regering het kennisveiligheidsbeleid ook uitbreiden naar de private sector? Wordt kennisveiligheid een transversaal thema dat in meerdere beleidsdomeinen zal worden opgenomen?

4. In het regeerakkoord wordt de CS3D-richtlijn vermeld als een uitdaging om niet te hervallen in toenemende regeldruk.

   Hoe wil de minister door de omzetting van de richtlijn de 'gepaste voorzichtigheid' in bedrijven doen toenemen zonder de regeldruk te doen toenemen?

MATTHIAS DIEPENDAELE
MINISTER-PRESIDENT VAN DE VLAAMSE REGERING, VLAAMS MINISTER VAN ECONOMIE, INNOVATIE EN INDUSTRIE, BUITENLANDSE ZAKEN, DIGITALISERING EN FACILITAIR MANAGEMENT

ANTWOORD
op vraag nr. 74 van 22 november 2024
van **KARL VANLOUWE**

---

1. Vooraf dit: de KMS-studie, die zeker waardevol is, vergt toch enige nuancering waardoor de zaken toch minder dramatisch zijn als nu ze overkomen. Cijfers over publicaties komen met een vertraging van een jaar of twee. Ook het schrijven van een wetenschappelijk artikel en het publicatieproces op zich nemen niet zelden een jaar (of zelfs langer) in beslag. Dit betekent dat de samenwerkingen waarover de KMS-studie spreekt al enkele jaren achter ons liggen, toen samenwerkingen met China nog als positief beschouwd werden en kennisveiligheid nog niet of maar nauwelijks op de politieke radar stond. We mogen dus niet de fout maken om een eerdere periode, toen de zaken anders lagen, te beoordelen van het huidige perspectief. De studie is evenwel een uitstekende referentie om vanaf nu de evolutie van de samenwerkingen te monitoren.

   Wat de uitrol van het Vlaams kennisveiligheidsbeleid op het terrein betreft, waarvoor de werkgroep kennisveiligheid werd opgericht, wil ik wijzen op de vier belangrijke initiatieven inzake kennisveiligheid die het Fonds Wetenschappelijk Onderzoek (FWO) intussen heeft ontwikkeld:
   - Ten eerste zet het FWO zelf in op verantwoorde partnerschappen en voert het een grondige risicoanalyse uit wanneer het nieuwe partnerschappen met onderzoeksfinancierders in het buitenland afsluit.
   - Ten tweede zet het FWO maximaal in op sensibilisering door iedere aanvrager een beknopte risicoanalyse te laten invullen waarbij enerzijds de potentiële veiligheidsrisico's worden ingeschat en anderzijds, indien nodig, mitigerende maatregelen worden geformuleerd.
   - Ten derde zal er in de interim en ex-post rapportering van gefinancierd FWO-onderzoek gepolst worden naar mogelijke inbreuken inzake kennisveiligheid zodat het FWO dit kan monitoren en waar nodig het FWO-kennisveiligheidsbeleid kan bijsturen.
   - Het vierde luik omvat een solide cyberveiligheid-strategie conform de CCB visie (Centrum Cyberveiligheid België). Het FWO behaalde in het licht van deze strategie recent het ISO 27001-certificaat.

   Met dit beleid is het FWO één van de eerste onderzoeksfinancierders in Europa die voldoet aan de richtlijnen die de Europese Commissie in mei 2024 uitbracht. De Commissie beveelt namelijk aan dat kennisveiligheid integraal deel dient uit te maken van de aanvraagprocedure voor financiering zodat de aanvragers aangezet worden na te denken over de mogelijke risico's die hun onderzoek en/of samenwerkingen mogelijks met zich meebrengen en hierop gepast anticiperen. Gezien bovenstaande aanbeveling, is het Vlaamse beleid er dan ook op gericht om de kennisinstellingen gericht te ondersteunen in de uitbouw van hun eigen kennisveiligheidsbeleid, mede omdat de kennisinstellingen met fondsen zoals het BOF en IOF ook zelf instaan voor de toewijzing van een belangrijk deel van de onderzoeksmiddelen.

2. Voor de uitwerking van een Vlaams kennisveiligheidsbeleid, met inbegrip van de uitbouw van een Vlaams kennisveiligheidsloket, is een nauwe samenwerking vereist met de federale overheid, die nog steeds de volheid van bevoegdheid heeft inzake openbare orde en nationale veiligheid, en die over heel wat meer expertise, mensen en

middelen hieromtrent beschikt. Deze samenwerking is in volle opbouw binnen de ambtelijke werkgroep CIS-Kennisveiligheid, waarvan de oprichting door de Interministeriële Conferentie inzake Wetenschapsbeleid (IMCWB) is beslist, maar verloopt tot op heden nog maar bij mondjesmaat, gelet op onderliggende politieke gevoeligheden en vooral op de recente vertragingen bij de federale regeringsvorming.

3. Wat de uitbouw van het Vlaams kennisveiligheidsbeleid betreft, is er inderdaad niet alleen sprake van de oprichting van het kennisveiligheidsloket ter ondersteuning van de Vlaamse onderzoeksinstellingen dat in nauwe samenwerking met de federale overheid zal worden opgericht. In mijn beleidsnota komen nog drie andere initiatieven naar voor. Ten eerste zal de Vlaamse overheid samenwerkingsafspraken met de Vlaamse kennisinstellingen opstellen. Ten tweede bekijken mijn diensten of de strategie en aanpak die voor aanvragen van onderzoeksfinanciering bij het Fonds voor Wetenschappelijk onderzoek werd uitgetekend, ook breder binnen de Vlaamse kennisinstellingen kan worden uitgerold. Tot slot onderzoekt deze Regering een algemene zorgplicht inzake kennisveiligheid voor de kennisinstellingen in te voeren om hen in staat te stellen hieromtrent zelf rechtshandelingen te stellen en beschermingsmaatregelen te nemen, ook ten aanzien van derde (private) partijen waarmee nu wordt samengewerkt.

   Ook moet er hier op gewezen worden dat kennisveiligheid al één van de criteria uitmaakt om buitenlandse directe investeringen in Vlaamse bedrijven te screenen, zoals beschreven in het wetgevend samenwerkingsakkoord hieromtrent, en waarvan de toepassing in de praktijk een taak vormt waaraan de Vlaamse overheid actief deelneemt.

   Er bestaat reeds een algemene zorgvuldigheidplicht voor alle bedrijven en kennisinstellingen op vlak militaire en dualuse-exportcontrole. Voor dualusegoederen gelden deze verplichtingen binnen bepalingen van Verordening (EU) 2021/821 uiteraard voor gecontroleerde dual use technologieën, waarbij elke gecontroleerde kennisoverdracht een geldige vergunning vereist. Maar ook voor niet-gecontroleerde dual use producten, inclusief kennis en verlenen van technische bijstand kunnen vergunningsplichten gelden in de door de verordening voorziene gevallen. Dit omvat de situatie er relevante redelijke vermoedens (zouden moeten) gedetecteerd worden onder de normale uitoefening van de zorgvuldigheidsplicht onder artikel 4, 5 en 8 van Verordening 2021/821.

   Europese richtlijnen omtrent interne nalevingsprogramma's in het algemeen en specifiek in het kader van onderzoek werden reeds ter beschikking gesteld:
   - Aanbeveling (EU) 2019/1318 van de Commissie van 30 juli 2019 inzake interne nalevingsprogramma's voor controles op de handel in producten voor tweeërlei gebruik uit hoofde van Verordening (EG) nr. 428/2009;
   - Aanbeveling (EU) 2021/1700 van de Commissie van 15 september 2021 inzake interne nalevingsprogramma's voor controles op onderzoek met betrekking tot producten voor tweeërlei gebruik uit hoofde van Verordening (EU) 2021/821 van het Europees Parlement en de Raad 2021 tot instelling van een Unieregeling voor controle op de uitvoer, de tussenhandel, de technische bijstand, de doorvoer en de overbrenging van producten voor tweeërlei gebruik.

   De dienst controle Strategische goederen (dCSG) zet actief in op bewustmaking van zowel industrie als kennisinstellingen, zowel op vlak van militaire als dual use regelgeving en zorgvuldigheidsplichten.

   Richtlijn (EU) 2024/1760 (de 'de CS3D-richtlijn') veroorzaakt op dit vlak geen wijzigingen, zoals ook toelicht in overweging 25 van deze richtlijn. Hierin wordt de complementariteit van de richtlijn met de bestaande verplichtingen onder Verordening 2021/821 benadrukt.

4. De omzetting van de CS3D richtlijn valt onder de verantwoordelijkheid van de federale overheid. Het is dus aan hen om dit op zo'n manier om te zetten, dat de regeldruk zo weinig mogelijk toeneemt. En zoals in het regeerakkoord staat, pleiten we voor administratieve eenvoud en zullen we waar mogelijk de nodige ondersteuning proberen bieden aan kmo's die geconfronteerd worden met de effecten van deze wetgeving.