

SCHRIFTELIJKE VRAAG

nr. 103

van **KARL VANLOUWE**

datum: 1 december 2023

aan **JO BROUNS**

VLAAMS MINISTER VAN ECONOMIE, INNOVATIE, WERK, SOCIALE ECONOMIE EN LANDBOUW

Open strategische autonomie en kennisveiligheid - Plannen

Door de geopolitieke en economische uitdagingen van de afgelopen jaren zet de Europese Unie na veel aandringen in op een open strategische autonomie ten opzichte van het wereldtoneel. De oorlog in Oekraïne heeft pijnlijk blootgelegd hoe sterk de EU afhankelijk is van Rusland op het vlak van energie. Tegelijk zien we zeer duidelijk hoe China onze openheid misbruikt om onze strategische voordelen, ons academisch potentieel en hoogtechnologische industrie te ondergraven.

De voorbeelden van de sluipende dreiging van Chinese inmenging zijn niet meer te overzien: drie vierde van de lopende EU-onderzoeken van dumping is tegen China, het land mengt zich ongewenst in onze havens, universiteiten en hoogtechnologische bedrijven. Om die reden zet de Vlaamse Regering extra in op een sterker kennisveiligheidsbeleid. De Vlaamse troeven - onze intellectuele eigendommen, economisch en wetenschappelijk potentieel - mogen ons niet ontnomen worden door China, noch door enige andere buitenlandse mogendheid.

Met het zicht op deze strategische bedreigingen zetten minister-president Jambon en minister Weyts het Beleidskader Kennisveiligheid op poten. Dat beleidskader moet acties coördineren om kennisveiligheid te garanderen in samenwerking met bedrijven, kenniscentra en administraties.

Hieronder een opsomming van alle acties die door de Vlaamse Regering in antwoorden op schriftelijke vragen en vragen om uitleg zijn gegeven:

- In het kader van de Europese verordening over buitenlandse directe investeringen en buitenlandse inmenging is een intern Belgisch samenwerkingsakkoord bereikt waarin eind 2022 werd beslist om een interfederaal screeningsmechanisme op te richten. In de laatste beleids- en begrotingstoelichting (BBT) werd toegelicht dat de Vlaamse diensten op het Departement Kanselarij en Buitenlands Beleid zich voorbereiden tot dit federaal is opgesteld.
- Naar het Nederlandse voorbeeld zou een loket voor kennisveiligheid worden opgericht. Dat zou moeten zorgen voor informatiedoorstroming van en naar veiligheids- en overheidscentra naar en van kennisinstellingen. Dat zou normaliter na de interministeriële commissie voor wetenschapsbeleid worden opgezet. De bedoeling zou zijn om extra experts rond kennisveiligheid aan te stellen.
- Daarnaast zouden er brochures en sensibiliseringsprogramma's worden opgezet om kennisinstellingen bewust te maken van de potentiële samenwerkingen met buitenlandse instellingen op het vlak van kennisveiligheid. In juni 2022 is er binnen de Vlaamse Interuniversitaire Raad (VLIR) een dergelijke visietekst opgemaakt door de



**Vlaams
Parlement**

universiteiten om problemen rond kennisveiligheid aan te pakken met betrekking tot de zogenaamde 'Seven sons of National Defense'-instellingen. Ook heeft het Departement Kanselarij en Buitenlands Beleid een bilateraal traject opgezet met de Vlaamse universiteiten in 2020 om samenwerking met Chinese instellingen verder op te volgen.

- Het gebruik van een ASPI-tracker zou worden gepromoot in alle betrokken Vlaamse instellingen. Die tracker, uitgebracht door het Australian Strategic Policy Institute, geeft aan welke Chinese instellingen allemaal gelinkt zijn aan militaire en politieke instituties. Op die manier moeten we voorkomen dat onze technologie en kennis tegen ons gebruikt zouden worden.
- Er zouden ook extra regels komen ten opzichte van zogenaamde dualuseproducten: de term duidt op producten maar ook kennis die zowel voor civiele als militaire doeleinden gebruikt kunnen worden. Rechtstreekse export van deze dualuseproducten naar China wordt gecontroleerd, maar dat is nog niet het geval voor meer indirecte stromingen en deze regels zouden worden verstrengd.
- Er zou een verbindingsofficier worden aangesteld bij de politie om Chinese studenten in onze kennisinstellingen die militair actief zijn beter en sneller te detecteren. Ook moet dat ertoe leiden dat er sneller informatie wordt uitgewisseld tussen de betrokken instellingen en moet het de samenwerking tussen de diensten op het vlak van kennisveiligheid helpen optimaliseren.
- Ten slotte zetten de Vlaamse diensten in op Internal Compliance Programma's (ICP's). Deze ICP's zijn interne nalevingsprogramma's die bedrijven en instellingen moeten opvolgen om conform te zijn met de actuele regelgeving. Door deze programma's proberen te implementeren in bedrijven, probeert de Vlaamse overheid onze weerbaarheid tegen diefstal en misbruik van kennis te verhogen.

De initiatieven van de Vlaamse Regering zijn dus talrijk en doelgericht.

1. Kan de minister een stand van zaken geven van al die initiatieven?
2. Hoe evalueert hij die stand van zaken?
3. Zijn er nog bijkomende initiatieven gepland dan wel nodig? Ziet de minister nog bijkomende uitdagingen op dat vlak?
4. De bovenvermelde initiatieven en programma's gaan in op verschillende aspecten van kennisveiligheid en worden allemaal uitgevoerd in het beleidskader dat de minister-president en minister Weyts hebben opgesteld.

Heeft het beleidskader tot doel om al die initiatieven en programma's te bundelen in een duidelijk programma rond kennisveiligheid?

ANTWOORD

op vraag nr. 103 van 1 december 2023
van **KARL VANLOUWE**

Ik kan u enkel een antwoord geven over de zaken die gebeuren in het beleidsdomein Economie, Wetenschap en Innovatie en die ook aangehaald werden in de gezamenlijke Mededeling aan de Vlaamse Regering over kennisveiligheid die ingediend werd door mezelf, de minister-president en collega Weyts in oktober 2022.

Een belangrijk element in deze mededeling betreft inderdaad de oprichting van een loket voor kennisveiligheid naar Nederlands voorbeeld. Om een dergelijk loket op te richten is het nodig de medewerking te krijgen van een aantal federale diensten, waarvan de Veiligheid van de Staat de voornaamste is. Anderzijds wenst deze laatste te vermijden dat individuele onderzoekers uit gans België bij hen komen. Vandaar dat alle Belgische entiteiten onderling moeten overeenkomen over hoe met bv. de Veiligheid van de Staat samen te werken.

Vlaanderen wenst zelf in te staan voor de aanvragen, opvolging en verdere verwerking van vragen naar informatie omtrent potentiële risico's rond internationale samenwerking met partners buiten Europa. Of anders gesteld, Vlaanderen ziet geen meerwaarde in een uniek federaal loket dat alle aanvragen groepeerd, samen doorstuurt en dan de antwoorden weer verder verdeelt. Dit was de kern van de beslissing door de interministeriële conferentie voor wetenschapsbeleid die op 11 december jongstleden. Vlaanderen zal deelnemen aan een nieuwe interfederale werkgroep om tot werkafspraken te komen, en kan nu tevens ook zelf verder initiatieven nemen om tot een kennisveiligheidsloket te komen.

Daartoe werd al een basis gelegd door de werkzaamheden van een werkgroep Kennisveiligheid gefaciliteerd door het departement EWI, o.a. door een bevraging te organiseren over de gewenste functies en diensten dat zo'n loket zou moeten aanbieden. De eerstvolgende stap is het opstellen van eigen richtlijnen (of leidraad of gedragscode) waarop kennisinstellingen zich kunnen baseren om eigen interne procedures in te stellen of aan te passen. De vraag naar richtlijnen kwam overigens vanuit de vermelde werkgroep. Vele kennisinstellingen zijn ondertussen al bezig met interne processen uit te tekenen. Een recent aangetrokken EWI-medewerker zal instaan voor het opstellen van dergelijke richtlijnen (en het verdere traject naar de oprichting van een loket).

Vanuit het perspectief van bewustwording is het FWO een elektronische toepassing aan het ontwikkelen, in samenspraak met de Vliir, waardoor elke aanvrager doorheen een reeks vragen geloodst wordt om uiteindelijk aanwijzingen te ontvangen over het mogelijke risicogehalte van de geplande samenwerking en hoe daarmee om te gaan. Zo worden nu nieuwe samenwerkingen met de Chinese "Seven Sons of Defense" niet meer toegelaten. Een volgende stap – of uitdaging als u wil – is dan deze toepassing aan de praktijk te toetsen en waar nodig bij te sturen. Daarnaast is het wenselijk dat binnen de kennisinstellingen zelf een soortgelijke toepassing voorzien wordt die volgens dezelfde achterliggende logica functioneert. Het loket wordt dan als het ware het sluitstuk van deze toepassingen: daar waar de instellingen zelf over onvoldoende informatie of inzicht beschikken kunnen ze beroep doen op het kennisveiligheidsloket. Daarbij hoort wel de bedenking dat zelfs zo'n kennisveiligheidsloket op sommige vragen en aspecten van risico-inschatting het antwoord schuldig zal moeten blijven, maar wel suggesties zal kunnen leveren om het risico te beperken.

Daarnaast blijft het departement de evoluties rond dit thema opvolgen op Europees niveau door deelname in verschillende Europese werkgroepen en aan een zogenaamde "mutual learning exercise" (dit laatste samen met een medewerkster van het FWO). Tijdens zo'n mutual learning exercise stellen de lidstaten hun praktijkvoorbeelden voor aan elkaar en zorgen externe experts voor breder (en theoretisch) perspectief. Vooral de Nederlandse presentaties zijn zeer leerrijk en hebben ook tot bijkomende bilaterale contacten geleid.

Vandaar dat het departement ook voorstander is om het thema "kennisveiligheid" op te nemen als nieuwe actie van de vernieuwde beleidsagenda van de Europese onderzoeksruimte (niet toevallig met Nederland als initiatiefnemer). Deze problematiek overstijgt immers de landsgrenzen. Internationale afstemming onder nationale administraties is een pluspunt. Tijdens het Belgisch voorzitterschap zal de Commissie een zogenaamde Raadsaanbeveling voorstellen waarover de lidstaten dan verder zullen debatteren. Dankzij onze sterke betrokkenheid bij de relevante Europese werkgroepen biedt de Europese Commissie ons de kans om informeel suggesties en reacties te door te spelen nog tijdens het voorbereiding van de ontwerp tekst voor Raadsaanbevelingen.

Kortom, meer dan werk genoeg op de plank en meer dan voldoende uitdagingen om op te pakken, zowel lokaal als internationaal. We vorderen traag maar gestaag. Met de nieuwe medewerker op post en de IMCWB achter de rug kunnen we een versnelling hoger schakelen, te beginnen met de richtlijnen, zoals ik al eerder vermeldde. De werkgroep rond kennisveiligheid, waaraan ook vertegenwoordigers van het departement Onderwijs en het departement Kanselarij en Buitenlands Bestuur deelnemen, zal volgend jaar opnieuw samenkomen waarbij ook zal ingegaan worden op hun initiatieven, die u vermeld hebt in uw vraagstelling, en hoe deze te combineren met hetgeen door het departement EWI nagestreefd wordt, in het bijzonder rond dual use. Maar ik verwijs naar het antwoord van de collega's voor een stand van zaken rond de initiatieven in hun beleidsdomein.