Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

3862

Vragen van de leden **Wiersma** en **Yesilgöz-Zegerius** (beiden VVD) aan de Ministers van Onderwijs, Cultuur en Wetenschap en van Justitie en Veiligheid over *het bericht «Spionnen op de loer: «vooral China aast op vaccinkennis»»* (ingezonden 17 juni 2020).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Minister van Onderwijs, Cultuur en Wetenschap (ontvangen 26 augustus 2020).

Vraag 1
Bent u bekend met het bericht «Spionnen op de loer: «vooral China aast op vaccinkennis»?[1]

Antwoord 1
Ja.

Vraag 2
Deelt u de mening dat deze signalen zorgelijk zijn? Zijn er bij u signalen bekend vanuit onderzoeksinstituten waarbij verdenking is van (Chinese) digitale spionage? Zo ja, wat gebeurt er met deze signalen? Zo nee, bent u bereid hier actief navraag naar te doen? Wordt er voor kennisinstellingen in kaart gebracht hoe en op welke schaal deze spionage plaatsvindt, zodat zij zich hiertegen kunnen beschermen?

Antwoord 2
Uit het Cybersecuritybeeld Nederland 2020 en de jaarverslagen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en Militaire Inlichtingen- en Veiligheidsdienst (MIVD) blijkt dat sprake is van een permanente digitale dreiging vanuit statelijke actoren en dat deze dreiging blijft groeien. Digitale spionage wordt door deze statelijke actoren veelvuldig ingezet om onder meer geopolitieke en economische belangen van deze staten te dienen. Mochten er signalen zijn van digitale activiteiten richting kennisinstellingen of onderwijsinstellingen dan worden deze hierover geïnformeerd. In het

[1] De Telegraaf, https://www.telegraaf.nl/nieuws/1428327228/spionnen-op-de-loer-vooral-china-aast-op-vaccinkennis?utm_campaign=seeding-telegraaf&utm_medium=social&utm_source=facebook, 12 juni 2020.

ah-tk-20192020-3862
ISSN 0921 - 7398
's-Gravenhage 2020

openbaar worden echter geen concrete uitspraken gedaan over specifieke casuïstiek.
Het kabinet deelt uw zorg en werkt daarom aan maatregelen om ongewenste kennisoverdracht langs de weg van academisch onderwijs en onderzoek te voorkomen. Het kabinet spreekt geregeld met onderwijs- en onderzoeksinstellingen. Binnenkort wordt gestart met een nieuwe gespreksronde over veiligheidsbeleid en risico's van internationale samenwerking op instellingen (zie ook het antwoord op vraag zes).

Vraag 3
Zijn de onderzoeksinstituten waarbij verdenking is van Chinese digitale spionage actief geïnformeerd door sectorale toezichthouders over deze risico's? Zo ja, welke maatregelen zijn genomen? Zo nee, waarom niet? Wat doet u eraan om de Nederlandse wetenschap te beschermen tegen (digitale) spionage? Herinnert u nog dat u vorig jaar op soortgelijke berichtgeving[2] aangaf om te kijken of er onderzoek moet komen om uit te zoeken of er een brede kennisregeling moet komen met betrekking tot risicolanden? Welke stappen heeft u na deze berichtgeving genomen?

Antwoord 3
Het borgen van de veiligheid inclusief digitale veiligheid is in eerste instantie een verantwoordelijkheid van onderzoeksinstituten zelf. Afhankelijk van het onderzoeksinstituut kunnen er specifieke aanvullende eisen aan de (cyber-)veiligheid gesteld worden. Bijvoorbeeld voor instituten die zich bezighouden met defensie-gerelateerd onderzoek.
Onderwijsinstellingen nemen vanuit hun eigen verantwoordelijkheid ook actie om hun (digitale) veiligheid te vergroten en risico's in te dammen. Daarbij worden ze geholpen door organisaties als SURF, de ICT-coöperatie van onderwijs en onderzoek, waarin hoger onderwijs- en onderzoeksinstellingen samenwerken op het gebied van cybersecurity en het cybersecurity expertisecentrum Z-CERT voor academische ziekenhuizen met onderzoekafdelingen. Als het gaat om onderzoeksinstituten die verbonden zijn aan instellingen uit het hoger onderwijs is er ook het Platform Integrale Veiligheid Hoger Onderwijs. Instellingen volgen actief de ontwikkelingen over kennisveiligheid. Ook hebben ze richtlijnen opgesteld, zoals integriteitscodes en gedragscodes als het gaat om internationale samenwerking. Tevens is de checklist van het The Hague Center for Strategic Studies over het aangaan van academische samenwerking met Chinese partners is onder de aandacht gebracht bij instellingen.[3]
De internationale oriëntatie van kennisinstellingen is een groot goed. Tegelijkertijd kan het ongewenst overdragen van (wetenschappelijke) kennis naar andere landen risico's met zich meebrengen voor de nationale veiligheid en de positie van kennisinstellingen. Om de digitale weerbaarheid van onderzoekscentra die zich bezighouden van vaccinonderzoek gedurende de Covid-19-uitbraak te verhogen, heeft het kabinet een spoedwetsvoorstel ingediend waarmee het Nationaal Cybersecurity Centrum (NCSC) de mogelijkheid krijgt om bijstand aan deze centra te verlenen. Deze bijstand bestaat uit het informeren en adviseren van deze organisaties, het bijstaan in het treffen van maatregelen bij dreigingen en incidenten, waaronder ook digitale spionage, en het verrichten van analyses en technisch onderzoek hiernaar.
Daarnaast werkt het kabinet aan maatregelen ter voorkoming van ongewenste kennisoverdracht, onder de werknaam brede kennisregeling. De focus ligt daarbij op dit moment onder andere op bewustwordingsverhoging, informatievoorziening en veiligheidsbeleid. Ook onderzoekt het kabinet wat de eventuele mogelijkheden zijn voor het toetsen van studenten en onderzoekers. Instellingen in het hoger onderwijs, onderzoeksinstellingen, sectororganisaties en het Platform Integraal Veilig Hoger onderwijs worden betrokken bij de uitvoering van de maatregelen. In het najaar wordt uw Kamer over de voortgang van dit traject geïnformeerd.

---

[2] NOS, https://nos.nl/nieuwsuur/artikel/2290313-falend-toezicht-op-chinese-militaire-wetenschappers-in-nederland.html, 23 juni 2019.
[3] https://hcss.nl/sites/default/files/files/reports/BZ127566%20HCSS%20Checklist%20for%20collaboration%20with%20Chinese%20Universities.pdf

Concreet is de Minister van Economische Zaken en Klimaat (EZK) naar aanleiding van de incidenten bij de Universiteit Maastricht en Wetsus in gesprek gegaan met de TO2-federatie om het veiligheidsbewustzijn te vergroten en de samenwerking op het gebied van cyberveiligheid bij de TO2 instellingen te verbeteren. Hierbij is ter ondersteuning ook het Digital Trust Center betrokken.

Vraag 4
Valt het onderzoek naar het coronavaccin onder «onderzoeksgebieden waar zeer specifieke technische kennis kan worden opgedaan»? Zo nee, waarom niet? Zo ja, moeten er dan op zeer korte termijn geen kaders worden geschapen voor kennisinstellingen hoe om te gaan met invloeden uit risicolanden? Kunt u dit uitleggen?

Antwoord 4
Op dit moment wordt i.s.m. experts onderzocht welke kennisgebieden zouden moeten worden aangemerkt als risicovolle kennisgebieden. In het najaar wordt u hierover geïnformeerd.
Wat betreft het onderzoek naar het vaccin tegen de ziekte Covid-19, staat het kabinet een gezamenlijke, internationale aanpak voor. Waarin we uitgangspunten als open science (betreft onder meer open access van publicaties en onderzoeksdata), gelijkwaardigheid, wederkerigheid en academische vrijheid hanteren. Tegelijkertijd weten we dat deze uitgangspunten niet voor alle landen vanzelfsprekend zijn. Daarom is het belangrijk dat onderzoeksinstituten goed nadenken met wie ze samenwerken, de data delen, wederkerige afspraken maken en hoe ze hun onderzoek beschermen. Daarbij geldt het motto «zo open als mogelijk, zo gesloten als nodig», zoals dat in 2016 onder Nederlands voorzitterschap van de Raad van de Europese Unie is afgesproken.
Op de korte termijn zet het kabinet in op het verder vergroten van het bewustzijn van betrokken onderzoeksinstellingen onder meer door nader met hen in gesprek te gaan en het nog meer onder de aandacht brengen van het belang van (digitaal) veiligheidsbeleid.

Vraag 5
Deelt u de mening dat juist in deze tijd de veiligheid van ons onderzoek zeker moet worden gesteld? Zijn kennisinstellingen naar uw mening voldoende op de hoogte van de risico's en handelen zij hier ook voldoende naar? Hebben de kennisinstellingen voldoende vaardigheden en kennis in huis om zich te beschermen tegen digitale spionage? Waar zitten de kwetsbaarheden bij de kennisinstellingen?

Antwoord 5
Zoals ook vermeld bij het antwoord onder vraag drie is veiligheid van onderzoek altijd van belang. Door het hiervoor genoemde spoedwetsvoorstel dat het kabinet heeft ingediend krijgt het Nationaal Cybersecurity Centrum (NCSC) de mogelijkheid om bijstand aan deze centra die zich op dit moment bezighouden met het vaccinonderzoek te verlenen. Op die manier kunnen deze organisaties door het NCSC actief worden geïnformeerd en geadviseerd. Ook kan het NCSC bijstand verlenen in het treffen van maatregelen bij dreigingen en incidenten, o.a. op het gebied van digitale spionage.

Vraag 6
Is het Ministerie van Justitie & Veiligheid bereid om met sectorale toezichthouders van dit soort vitale onderzoeksinstituten in gesprek te gaan en daar waar mogelijk te ondersteunen en hun informatiepositie te versterken? Zo nee, waarom niet? Zo ja, kunt u de Kamer informeren over de uitkomsten van deze gesprekken?

Antwoord 6
Het kabinet spreekt geregeld met instellingen in onderwijs en onderzoek. Zoals hierboven aangegeven start het kabinet binnenkort met een nieuwe gespreksronde om het bewustzijn van de risico's van internationale samenwerking te vergroten en om met instellingen en sectororganisaties te komen tot afspraken in het kader van het borgen van veiligheidsbeleid op de instellingen, inclusief digitale veiligheid. Het grootste gedeelte van de

gesprekken komt voor rekening van de Minister van Onderwijs, Cultuur en Wetenschap. Maar ook de Minister van Volksgezondheid, Welzijn en Sport en de Staatssecretaris van Economische Zaken en Klimaat zullen betrokken zijn bij de gesprekken met de voor hen relevante onderzoeksinstellingen. Bij de gesprekken zal het Ministerie van Justitie en Veiligheid ondersteuning bieden. Ook zal het Platform Integrale Veiligheid Hoger Onderwijs, naast de sectororganisaties, betrokken worden.

Vraag 7
Op welke manier garandeert u de uitgangspunten van «open science» in de zoektocht naar een vaccin voor het Coronavirus, maar zorgt u er eveneens voor dat deze wetenschappelijke onderzoeksinstituten beschermd worden tegen Chinese digitale spionage? En op welke manier vraagt u hierin aandacht voor binnen de Europese wetenschappelijke samenwerkingsverbanden?

Antwoord 7
Het kabinet is voorstander van een internationale samenwerking in onderzoek en wetenschap. Voor ons belangrijke uitgangspunten zijn open science en open access. Waarden als gelijkwaardigheid, wederkerigheid en academische vrijheid hebben we hoog in het vaandel staan.
Nederland heeft, ook in Europees verband, nadrukkelijk aangeven dat het belangrijk is dat onderzoek omtrent de Covid-19-uitbraak volgens de principes van open science gedeeld zal worden. Dankzij deze internationale samenwerking staan we sterker in de zoektocht naar een vaccin en behandeling. De crisis toont het belang aan van breed en snel beschikbaar stellen van onderzoeksresultaten.
Niet alle landen hanteren dezelfde waarden over gelijkwaardigheid, wederkerigheid, academische vrijheid en open science. Daarom geldt dat we zo open mogelijk zijn, maar zo gesloten als het moet. Dat betekent dat ook wordt gevraagd aan onderzoekers om zich zo bewust mogelijk te zijn van met wie en op welke manier onderzoeksdata worden gedeeld en met wie men samenwerkt. Ook op grond van dual-use exportcontrole kunnen er beperkingen van toepassing zijn op het delen van technologie gerelateerd aan biologische agentia zoals virussen.
Dit vraagstuk komt ook aan bod op de Europese overlegtafels, waar ook het kabinet bij betrokken is. Als het gaat om de aanpak van de Covid-19-pandemie, maar ook in het algemeen als het gaat over onderzoek, wetenschap en innovatie. Lidstaten onderschrijven het belang van samenwerking om ongewenste overdacht van kennis en technologie tegen te gaan. De Europese Commissie werkt daarom op een aantal vlakken aan het voorkomen van ongewenste kennisoverdracht.