Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

# 30 821 Nationale Veiligheid

**Nr. 99**

## BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 20 december 2019)

Hierbij ontvangt u, mede namens de Minister van OCW, de reactie op het rapport van het Rathenau Instituut *«Kennis in het vizier: de gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur»* [1], zoals verzocht door de commissie voor Onderwijs, Cultuur en Wetenschap.

*Rapport «Kennis in het vizier»: Conclusies en aanbevelingen*

Het Rathenau Instituut brengt in het rapport *Kennis in het vizier* in kaart wat de belangrijkste gevolgen zijn van de recente geopolitieke, economische en maatschappelijke ontwikkelingen, en de digitalisering van de samenleving voor de Nederlandse publieke kennisinfrastructuur – bestaande uit universiteiten, wetenschappelijke instituten en publieke kennisorganisaties. Hierbij ziet het Rathenau Instituut twee belangrijke ontwikkelingen:

Het vervagen van het onderscheid tussen kennisontwikkeling voor civiele en militaire doelen, met name door digitalisering;
Het internationaliseren van kennisontwikkeling en innovatie, in het bijzonder die gericht op defensie en veiligheid.

De genoemde ontwikkelingen dwingen de partijen in de militaire kennisecosystemen tot meer verbindingen met civiele kennisecosystemen, omdat militaire technologieontwikkeling steeds meer voortbouwt op civiele technologie. Daarnaast werken publieke kennisinstellingen steeds meer in internationale samenwerkingsverbanden om hun kennisbasis te verbreden en hun positie in de wereld te versterken. Meer samenwerking roept de vraag op in hoeverre Nederlandse kennisinstellingen, bekeken vanuit veiligheidsbelangen, bepaalde kennis zelf in huis moeten hebben en in welke mate ze afhankelijk kunnen zijn van de kennisbasis van nieuwe, soms buitenlandse, partners.

[1] Raadpleegbaar via www.tweedekamer.nl

kst-30821-99
ISSN 0921 - 7371
's-Gravenhage 2019

Het Rathenau Instituut concludeert dat gezamenlijk beleid nodig is van overheid en kennisinstellingen om maatschappelijk verantwoord vorm te geven aan kennisontwikkeling die raakt aan defensie en veiligheid. De belangrijkste opgaven liggen hierbij op het gebied van beleidsontwikkeling, verdeling en aanvaarding van verantwoordelijkheden, afweging van belangen en bescherming van gekoesterde waarden, en van institutionalisering van manieren om met de ontwikkelingen om te gaan. Tot slot roept het Rathenau Instituut de betrokken partijen op om gezamenlijk invulling en uitwerking te gaan geven aan dit beleid.

*Reactie op de belangrijkste conclusies en aanbevelingen van het Rathenau Instituut*

Het kabinet dankt het Rathenau Instituut voor het uitbrengen van deze verkenning over deze actuele ontwikkelingen en de gevolgen daarvan voor publieke kennisinstellingen ten aanzien van hun betrokkenheid bij defensie- en veiligheidsvraagstukken. Het rapport laat zien dat er behoefte is aan duidelijke beleidskaders hoe hiermee om te gaan, waarbij het van belang is dat overheid en kennisinstellingen – vanuit ieders eigen verantwoordelijkheid – zoveel mogelijk gezamenlijk optrekken. Het kabinet onderschrijft dit, maar benadrukt tevens dat we in Nederland niet aan het begin staan van deze discussie, en dat er al belangrijke voortuitgang is geboekt. Hierover informeer ik u nader in deze brief.

*Kennisinstellingen werken samen aan het verbeteren van de veiligheid*

Bestuurders van hoger onderwijs- en onderzoeksinstellingen in Nederland zijn verantwoordelijk voor de integrale veiligheid, waaronder ook de digitale veiligheid, van hun instelling. Het stimuleren van het bewustzijn van veiligheidsrisico's onder bestuurders, wetenschappers en studenten is hiervan een belangrijk onderdeel. De VSNU en de VH hebben, met steun van het Ministerie van OCW, daarom het Platform Integrale Veiligheid Hoger Onderwijs ingericht.[2] Hierin werken bestuurders en veiligheidsexperts van hoger onderwijsinstellingen samen aan het stimuleren van veiligheidsbewustzijn door het uitwisselen van kennis en kunde en het ontwikkelen van tools en handreikingen.

Op het gebied van cybersecurity werken hoger onderwijs- en onderzoeksinstellingen in Nederland samen via SURF, de ICT-coöperatie van onderwijs en onderzoek. SURF onderzoekt de behoeften en de kansen, ontwikkelt een gezamenlijke visie en investeert in innovatie en kennis die nodig is om te kunnen anticiperen op de soms ontregelende effecten en veiligheidsrisico's die gepaard gaan met ICT-innovatie.[3]

*Veiligheidsbelang onderdeel van nieuwe Nederlandse Code Wetenschappelijke Integriteit*

In Europees verband zijn onder Nederlands EU-voorzitterschap afspraken gemaakt over het optimaal hergebruiken van onderzoeksdata voortkomend uit onderzoek gefinancierd met publieke middelen, en hoe veiligheidsbelangen hierin meegewogen kunnen worden.[4] Hierbij is het principe leidend «zo open als mogelijk is en zo gesloten als noodzakelijk» (Raadsconclusies 2016, Artikel 14, 15). Dit principe is vorig jaar ook vastgelegd in de Nederlandse Code Wetenschappelijke Integriteit (Onderdeel «Ontwerp» en «Verslaglegging», norm 11, 45). De code wordt onderschreven door KNAW, NFU, NWO, de TO2-federatie, de Vereniging

[2] https://www.integraalveilig-ho.nl/
[3] Kamerstuk 30 821, nr. 87.
[4] Kamerstuk 34 139, nr. 18.

Hogescholen (VH) en de Vereniging van Nederlandse Universiteiten (VSNU).[5]

*Bescherming van kennis/technologie die raakt aan de nationale veiligheid*

Nationale veiligheid is een kerntaak van de overheid. Waar zich dreigingen of risico's voordoen, spant de overheid zich in om Nederland weerbaar(der) te maken. Omdat deze inspanningen mogelijk gevolgen kunnen hebben voor de openheid van onze samenleving en open economie, vindt steeds een weging plaats tussen het benutten van kansen enerzijds en het beschermen van nationale veiligheidsbelangen anderzijds. Het open karakter van onze samenleving vormt de grondslag voor de inrichting van onze maatschappij en de basis voor onze welvaart. We zijn zo open mogelijk en beschermen waar noodzakelijk.[6] Het kabinet werkt aan maatregelen om haar handelingsperspectief te vergroten bij de ongewenste overdracht van kennis/technologie die raakt aan de nationale veiligheid. Hieraan gerelateerd is de uitdaging om kennis- en technologiegebieden te identificeren waarop Nederland nu afhankelijk is van het buitenland, maar waarop in de toekomst een grotere mate van (digitale) autonomie gewenst is.

Er is een traject gestart om te onderzoeken in hoeverre aanvullende maatregelen gewenst zijn met betrekking tot de risico's voor de (nationale) veiligheid van ongewenste kennis- en technologieoverdracht via de weg van (academisch) onderwijs en onderzoek. In dit traject wordt onderzocht op welke manier een brede kennisregeling kan worden opgezet waarmee onderzoeks- en onderwijsgebieden met een veiligheidsrelevantie effectief beschermd worden. Daarnaast heeft het kabinet uw Kamer op 14 maart 2019 geïnformeerd over het verscherpt toezicht op studenten en onderzoekers die een link kunnen hebben met het Iraanse ballistische raketprogramma.[7]

De ontwikkeling van hoogwaardige technologie die raakt aan de nationale veiligheid loopt het risico onderbroken te worden wanneer er sprake is van ongewenste overnames en/of investeringen.
Het gaat met name om risico's van het ontstaan van strategische afhankelijkheden, aantasting van de continuïteit van dienstverlening van vitale processen of aantasting van de integriteit en exclusiviteit van kennis en informatie. Een van de maatregelen die het kabinet neemt is een stelsel van investeringstoetsing op nationale veiligheidsrisico's, hierover is uw Kamer op 12 november 2019 geïnformeerd.[8] In het kader van de Defensie Industrie Strategie (DIS) is eveneens een ex ante analyse van de Nederlandse Defensie technologische en industriële basis (NLDTIB) uitgevoerd. Met deze analyse is in kaart gebracht of, en zo ja, welke beschermende maatregelen nodig zijn wanneer overnames en investeringen in de NLDTIB risico's voor de nationale veiligheid opleveren. Dit heeft in het bijzonder betrekking op kennis van en informatie over de uitvoering van de essentiële militaire taken door onze Defensie. Uw Kamer wordt over de uitkomsten hiervan vóór de jaarwisseling geïnformeerd.

*Exportcontrole strategische goederen*

Een relevant juridisch kader wordt gevormd door wetgeving op gebied van exportcontrole en sancties. Dat kader is ook van toepassing op kennisinstellingen. Zowel het EU Gemeenschappelijk Standpunt inzake

---

[5] https://www.vsnu.nl/wetenschappelijke_integriteit.html
[6] Kamerstuk 30 821, nr. 72
[7] Kamerstuk 30 821, nr. 70
[8] Kamerstuk 30 821, nr. 97

wapenexport als de Europese Dual-use[9] verordening stellen beperkingen aan het internationaal delen van kennis en technologie over gecontroleerde producten.[10] Voor de export van technologie of kennis gerelateerd aan die producten is een vergunning noodzakelijk. Op grond van verschillende Europese sancties[11] kunnen ook beperkingen bestaan ten aanzien van kennisoverdracht. Het Ministerie van Buitenlandse Zaken (BZ) is verantwoordelijk voor het exportcontrolebeleid en de implementatie daarvan met verschillende ketenpartners.

Het kabinet is in gesprek met de wijze waarop kennisinstellingen deze wetgeving naleven. BZ organiseert regelmatig voorlichtingsbijeenkomsten waaraan ook kennisinstellingen deelnemen. Daarbij is specifieke aandacht voor internationale samenwerkingen in het onderzoeksveld en de niet-fysieke overdracht van technologie. Online[12] is veel praktische informatie beschikbaar en individuele voorlichting vindt, indien nodig, ook plaats. In Europees verband wordt gewerkt aan specifieke compliancerichtlijnen over dual-use exportcontrole voor kennisinstellingen. Nederland is actief bij dit proces betrokken en werkt daarbij samen met vertegenwoordigers van de academische sector.

*Tot slot*

Het rapport van het Rathenau Instituut maakt duidelijk dat de huidige geopolitieke ontwikkelingen gevolgen hebben voor de publieke kennisinfrastructuur, die zijn betrokkenheid bij defensie- en veiligheidsvraagstukken gestaag ziet toenemen. Met deze realiteit in het achterhoofd zullen – politiek, overheden en kennisinstellingen – samen moeten werken aan duidelijke afwegingskaders en procedures om maatschappelijk verantwoord vorm te geven aan kennisontwikkeling die raakt aan defensie en veiligheid. Het bovenstaande overzicht laat zien welke stappen reeds zijn gezet en hoe het kabinet hierin in (inter)nationaal verband opereert. Samen met kennispartners zet het kabinet de ingezette lijn de komende tijd voort. Bij deze en andere toekomstige beleidstrajecten zullen de aanbevelingen van het Rathenau Instituut steeds worden meegenomen.

De Staatssecretaris van Economische Zaken en Klimaat,
M.C.G. Keijzer

[9] Dual-use, oftewel voor tweeërlei gebruikt geschikt, d.w.z. zowel civiel als militair toepasbaar.
[10] De EU dual-use verordening definieert 10 controlecategorieën: nucleair, speciale materialen en aanverwante appatuur, materiaalverwerking, elektronica, computers, telecommunicatie en informatiebeveiliging, sensoren en lasers, navigatie en vliegtuigelektronica, zeeschepen en zeewezen, ruimtevaart en voortstuwing.
[11] www.sanctionsmap.eu
[12] www.rijksoverheid.nl/exportcontrole