Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2019–2020

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 674

BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 april 2020

Hierbij informeer ik uw Kamer, mede namens de Minister van Justitie en Veiligheid (JenV), de Minister van Defensie en de Minister van Onderwijs, Cultuur en Wetenschap (OCW), over de aanpak voor kennisontwikkeling en innovatie op het gebied van cybersecurity.[1]

Aanleiding voor deze aanpak zijn de ambities uit het regeerakkoord (bijlage bij Kamerstuk 34 700, nr. 34), de Nederlandse Cybersecurity Agenda Kamerstuk 26 643, nr. 536), de Defensie Cyber Strategie (Kamerstuk 33 321, nr. 9) en de Nederlandse Digitaliseringsstrategie (Kamerstuk 26 643, nr. 623). Er is urgentie om de ontwikkeling en toepassing van kennis in Nederland op het gebied van cybersecurity te verdiepen en te verbreden. Ook uw Kamer[2] en vertegenwoordigers van de cybersecurity-onderzoeksgemeenschap wijzen op het belang hiervan. Dit is hard nodig om maatregelen te kunnen treffen tegen bestaande en nieuwe digitale dreigingen.[3] Bovendien voorkomt een hoogwaardige, autonome kennispositie een te grote afhankelijkheid van cybersecurity-expertise en cybersecurity-oplossingen uit andere landen.

Het versterken van zowel fundamenteel als toegepast cybersecurity-onderzoek en de toepassing van kennis is hiervoor cruciaal. Cybersecurity-kennisontwikkeling geldt niet alleen voor bètawetenschappen, maar ook voor alfa en gamma. Het gaat om zowel gericht als interdisciplinair onderzoek, waarbij wordt gekeken naar oplossingen en toepassingen voor de korte en de lange termijn. Een focus op de gehele kennis- en innovatieketen, inclusief de rol van de overheid als *launching customer*, is hierbij van het grootste belang.

[1] Kamerstuk 26 643, nrs. 544 en 586
[2] Kamerstuk 34 775 VI, nr. 68
[3] https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

kst-26643-674
ISSN 0921 - 7371
's-Gravenhage 2020

Het kabinet heeft inmiddels via diverse impulsen kennisontwikkeling in Nederland versterkt. Mede namens de Minister van OCW kan ik u melden dat er in de afgelopen twee jaar door verschillende departementen is samengewerkt in het kader van de Nationale Wetenschapsagenda (NWA). Hierin zijn de diverse cybersecurity-beleidskaders en ook de behoeften uit het veld meegenomen. Als gevolg van deze samenwerking is in december 2019 een *call* geopend van circa € 8 miljoen over cybersecurity-, governance- en cryptologievraagstukken. Specifieke aandacht gaat hierbij uit naar talentontwikkeling. Ook is in juni 2019 vanuit de NWA€ 8 miljoen gehonoreerd aan het onderzoeksproject INTERSECT. Dit onderzoeksproject richt zich op de mogelijkheden van een veilig Internet of Things door technisch onderzoek te combineren met juridische en criminologische benaderingen. In het INTERSECT-consortium doen 34 organisaties[4] mee. Verder heeft NWO eind 2019 ruim € 4 miljoen gehonoreerd aan 10 onderzoeksprojecten die binnen de *call* cybersecurity – digitale veiligheid & privacy zijn ingediend.[5] Hiermee is in het afgelopen jaar in totaal meer dan € 20 miljoen beschikbaar gekomen voor onderzoek en innovatie op het gebied van cybersecurity. De NWA levert daarmee ook een grote bijdrage aan het verbinden van het veld over de gehele kennis- en innovatieketen. Een aanvullende impuls zal naar verwachting uitgaan van het missie gedreven innovatie en topsectoren beleid. De missie cyberveiligheid is één van de meerjarige missie gedreven innovatieprogramma's van de Kennis en Innovatie Agenda Veiligheid.

Met deze acties zetten we in op het versterken van ketenbrede samenwerking en zowel fundamenteel als toegepast onderzoek. Zodoende vormen zij een eerste basis om de ambities uit het regeerakkoord en de Nederlandse Cybersecurity Agenda op het terrein van onderzoek en innovatie te realiseren.

Tegelijkertijd zijn door de betrokken departementen verkenningen uitgevoerd hoe de aanpak en samenwerking in Nederland verder versterkt kan worden. Met deze brief informeer ik uw Kamer over de uitkomsten van deze verkenningen en over de vervolgacties. Op die manier geeft het kabinet ook uitvoering aan de motie van de leden Verhoeven en Arno Rutte.[6]

De kern van deze nieuwe aanpak is dat het kabinet de ambities uit de verschillende beleidskaders voor cybersecurity wil realiseren door verschillende instrumenten, waaronder de Nationale Wetenschapsagenda en het missiegedreven topsectoren- en innovatiebeleid, in te zetten. Dit doet het kabinet ter versterking van onderzoek, onderwijs en innovatie en samenwerking over de hele kennis- en innovatieketen heen.

---

[4] TU Eindhoven (H), VU Amsterdam, Radboud Universiteit Nijmegen, TU Delft, Universiteit Twente, Tilburg University, Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, Fontys Hogeschool, Hogeschool Leiden, TNO, Hogeschool van Amsterdam, BDO Advisory B.V., Brainport Development N.V., Bosch Security Systems B.V., Centric Netherlands B.V., Compumatica secure networks B.V., Consumentenbond, Fourtress BV, ICT Automatisering B.V., Ministerie van BZK, Océ-Technologies B.V., Omron Europe B.V., Oracle Nederland B.V., Koninklijke Philips N.V., Qbit Cyber Security, Secura B.V., Stichting Internet Domeinregistratie Nederland, Siemens Nederland N.V., Signify Netherlands B.V., Simac Techniek N.V., SURFnet B.V., Synopsys Netherlands B.V., Technolution B.V., Verum Software Tools B.V.

[5] https://www.nwo.nl/actueel/nieuws/2019/12/ruim-vier-miljoen-euro-voor-10-projecten-in-derde-nwo-national-cybersecurity-call.html

[6] Kamerstuk 34 775 VI, nr. 68

Resultaten oriëntatiefase verkenning cybersecurity kennisontwikkeling en innovatie

Medio 2018 heeft de Minister van JenV[7] een verkenning aangekondigd naar de mogelijkheden voor versterking van de kennis- en innovatieketen, de opzet van een kennis- en innovatie-agenda en hoe een duurzame samenwerking tussen publieke en private partijen over de hele keten heen kan worden georganiseerd.

De oriëntatiefase van de verkenning, onder leiding van ABD Topconsult, had tot doel inzichtelijk te maken wat hierbij de belangrijkste knelpunten zijn. In deze fase is ten eerste gebleken dat een duidelijker beeld nodig is van het functioneren van de kennis- en innovatieketen voor cybersecurity in Nederland. Ten tweede is uit een internationale vergelijking geconcludeerd dat er geen eenduidig model of werkwijze is voor de opzet en inrichting van een kennis- en innovatieketen voor cybersecurity. In de derde plaats is geconstateerd dat meerdere ministeries een eigen rol hebben bij de vormgeving van de kennisontwikkeling op het gebied van cybersecurity. Het verbinden van deze eigen rollen naar een gezamenlijke aanpak is complex.

De uitkomsten van de oriëntatiefase maakten duidelijk dat verdere analyse nodig was om tot een concrete en gezamenlijke aanpak te komen. Hierbij ging het onder meer om het inrichten van een samenhangende governance voor de realisatie van de ambities op het terrein van kennis en innovatie cybersecurity zoals gesteld in de Nederlandse Cybersecurity Agenda, de Defensie Cyber Strategie, de Nederlandse Digitaliseringsstrategie en in de missie cyberveiligheid van het Missiegedreven Topsectoren- en Innovatiebeleid. Het Ministerie van Economische Zaken en Klimaat (EZK) heeft daarom, met betrokkenheid van de ministeries van Defensie, OCW en JenV, opdracht gegeven voor een verdiepende verkenning.

Naast een verdere verdieping van de verkenningsfase, is besloten om waar mogelijk de ambities uit verschillende cybersecurity-beleidskaders op het terrein van kennis en innovatie, de behoeften van het bedrijfsleven, agenda's van kennisinstellingen, het vernieuwde Missiegedreven Topsectoren- en Innovatiebeleid en de NWA te verbinden. Op die manier kunnen onderzoekers, ondernemers en overheden krachten bundelen waar het kan en versterken ze de samenwerking op het gebied van kennis en innovatie cybersecurity waar het moet.

Resultaten verdiepende fase verkenning cybersecurity kennisontwikkeling en innovatie

Het doel van deze verdieping was het verkrijgen van meer inzicht in de sterktes en zwaktes van het cybersecurity kennis- en innovatie-ecosysteem in Nederland. Hiertoe zijn in samenwerking met private partijen, NWO en TNO een viertal analyses uitgevoerd[8]. Het gaat daarbij om:

1. Een sterkte-zwakte analyse van het Nederlandse kennisveld op het gebied van cybersecurity (door NWO en TNO gezamenlijk),
2. Analyse van de valorisatieketen op het gebied van cybersecurity in Nederland (door TNO),
3. Behoefte analyse van het Nederlandse cybersecurity-bedrijfsleven (door Cyberveilig Nederland),

[7] Kamerstuk 26 643, nr. 544

[8] Raadpleegbaar via www.tweedekamer.nl.

4. Inventarisatie van de kennis- en innovatiebehoeften bij de departementen JenV, Defensie en EZK in het kader van de missie cyberveiligheid.[9]

Ad 1)

De gezamenlijke sterkte-zwakte-analyse van NWO en TNO naar het kennisaanbod op het terrein van cybersecurity in Nederland, wijst uit dat de totale onderzoekscapaciteit in Nederland bescheiden is te noemen, zeker in vergelijking met een land als Duitsland. Als de onderzoekscapaciteit wordt uitgesplitst naar specifieke onderwerpen, blijkt zowel voor de academische instellingen als TNO de onderzoekscapaciteit bescheiden te zijn.
Op basis van patenten en citatie-analyse blijkt echter dat Nederland internationaal tot de landen met de grootste bijdrage aan het aantal wetenschappelijke publicaties op het gebied van cybersecurity behoort.

Ad 2)

Parallel aan deze sterkte-zwakte-analyse heeft TNO een onderzoek uitgevoerd naar de mogelijkheden om de keten te versterken. Dit betreft een beschrijving en analyse van de gehele kennis- en innovatieketen. De belangrijkste conclusie van dit onderzoek is dat er onvoldoende kennisontwikkeling en -uitwisseling plaatsvindt binnen en tussen de bedrijven en kennisinstellingen. Hierdoor wordt in Nederland ontwikkelde kennis nog onvoldoende benut. Tegelijkertijd geven alle betrokken partijen aan wel een sterke behoefte te hebben aan meer interactie en uitwisseling van kennis.

Ad 3)

Aan de brancheverenigingen voor het cybersecurity-bedrijfsleven in Nederland, Cyberveilig Nederland, is gevraagd om onder haar leden de behoeften en aandachtspunten op het gebied van kennisontwikkeling en innovatie te inventariseren. Hieruit blijkt dat het cybersecurity-bedrijfsleven vooral behoefte heeft aan duidelijke coördinatie. Het cybersecurity-bedrijfsleven wil innoveren, maar ervaart geen systematiek waar vraag en aanbod van kennis- en innovatiebehoeften bij elkaar komen. Met name het kennisintensieve cybersecurity-mkb heeft moeite met de complexiteit en vormgeving van door de overheid ontwikkelde instrumenten om onderzoek en innovatie te stimuleren.

Ad 4)

Tot slot hebben de ministeries van JenV, Defensie en EZK een inventarisatie gemaakt van de inhoudelijke vraagstukken die voor hen prioritair zijn.[10] Samen met de inventarisatie van kennisbehoeften van het cybersecurity-bedrijfsleven is er nu een eerste basispakket aan prioritaire onderwerpen uitgewerkt.

Vervolgaanpak

De uitkomsten van de analyses en de knelpunten die door de betrokkenen zijn aangedragen herken ik. De essentie die ik uit al deze onderzoeken haal, is de noodzaak om samenwerking over de hele keten heen te

---

[9] Kamerstuk 33 009, nr. 81

[10] Zie missie cyberveiligheid in het kader van het missiegedreven topsectoren- en innovatiebeleid https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/KIA%20Veiligheid%20-%2020191016%20definitief.pdf

stimuleren door onder andere vraag en aanbod van kennis beter aan elkaar te verbinden en beter te coördineren. Een ander element betreft het beter benutten van de diverse beleidsinstrumenten. Door deze instrumenten te verbinden met de cybersecurityketen, is de verwachting dat er positieve effecten zullen ontstaan ten aanzien van de gehele kennis- en innovatieketen.

Om samenwerking te versterken zijn in de afgelopen jaren verschillende initiatieven gestart, waaronder het Dutch Cybersecurity Platform for Higher Education and Research (dcypher). Hiermee zijn belangrijke stappen gezet in onder andere het agenderen en het betrekken van verschillende departementen bij het formuleren van specifieke kennisvraagstukken, en het verenigen en bijeenbrengen van diverse partijen zoals overheden, bedrijven en kennisinstellingen. Een vervolgaanpak, voortbouwend op de ervaringen met en activiteiten van dcypher, moet voorzien in een bredere, ketengeoriënteerde aanpak waarin bedrijven, kennisinstellingen en de overheid gezamenlijk inzetten op onderwijs, onderzoek en innovatie.

De basis voor de gezamenlijke vervolgaanpak zal bestaan uit een nieuw samenwerkingsplatform dat de krachten op het terrein van onderzoek, innovatie en onderwijs moet bundelen. Binnen dit samenwerkingsplatform komen alle relevante partijen, expertise, instrumenten en middelen uit het cybersecuritydomein bij elkaar.

Het platform zal zich richten op het bij elkaar brengen van kennisvragen en -aanbod. Ook zal het informatie over (financierings- en innovatie-) instrumenten beschikbaar stellen voor kennisinstellingen, het bedrijfsleven en medeoverheden. Hierbij valt te denken aan instrumenten zoals thematische calls uit de Nationale Wetenschapsagenda, toeslagen uit het missiegedreven topsectoren- en innovatiebeleid, Small Business Innovation Research (SBIR) en instrumenten uit Europese onderzoeksprogramma's als Horizon Europe en Digital Europe.

Zoals hierboven beschreven (zie ad 4) is in 2019 een eerste aanzet tot gezamenlijke prioritering verricht. Als vervolgstap zal de verbinding worden gelegd met het beschikbare nationale en internationale instrumentarium. Er is € 5,5 miljoen geoormerkt voor onderzoek, onderwijs en innovatie op het gebied van cybersecurity.

Dit bedrag wil ik inzetten voor het financieren van het samenwerkingsplatform en als hefboom voor cybersecurity-onderzoek, -onderwijs en -innovatie. Onder andere het hierboven beschreven instrumentarium kan voor de realisatie van programma's ingezet worden. De ketengeoriënteerde, programmatische aanpak voorziet in de specifieke inzet van instrumenten, waarbij per geval wordt afgewogen welk instrument het beste past bij het op te lossen vraagstuk. Het kan hierbij gaan om fundamenteel onderzoek, toegepast onderzoek, onderwijs en de valorisatie van ontwikkelde kennis. Op die manier bundelen we als overheid de krachten met het bedrijfsleven en de wetenschap en versterken we onderzoek, onderwijs en innovatie over de hele kennis- en innovatieketen heen.

Het samenwerkingsplatform zal door mij verder uitgewerkt worden in samenwerking met de relevante departementen, kennisinstellingen en het bedrijfsleven. In de tussentijd draagt NWO zorg voor continuering van een aantal activiteiten van dcypher tot 1 oktober 2020.

Verkenning specifiek kennisinstituut Cybersecurity

De motie van de leden Verhoeven en Arno Rutte[11] verzocht de mogelijkheid te onderzoeken om een instituut voor onderzoek op het gebied van cybersecurity op te richten. Het kabinet heeft conform de motie deze mogelijkheid onderzocht.

De vraag of er thema's van nationaal belang zijn die tot wijzigingen zouden moet leiden in het institutenportfolio, is meegenomen in de evaluatie van het institutenstelsel door KNAW en NWO. Hierover is uw Kamer eerder geïnformeerd.[12] Uit deze evaluatie kunnen geen conclusies worden getrokken met betrekking tot de noodzaak tot oprichting van een wetenschappelijk cybersecurity onderzoeksinstituut.

De verkenningen naar cybersecurity-kennis en -innovatie laten echter zien dat er in de Nederlandse context een uitdaging ligt om te komen tot meer samenhang tussen enerzijds fundamenteel en toegepast onderzoek en anderzijds valorisatie. Ook de genoemde motie wijst hier op. Verder beschrijven de verkenningen dat er onvoldoende kennisontwikkeling en -uitwisseling plaatsvindt tussen bedrijven en kennisinstellingen. Hierdoor wordt kennis die in Nederland ontwikkeld wordt nog onvoldoende benut. Tegelijkertijd geven alle betrokken partijen aan wel een sterke behoefte te hebben aan meer interactie en uitwisseling van kennis.

Gezien deze bevindingen en de overwegingen van uw Kamer, zie ik een essentiële rol weggelegd voor het nieuwe samenwerkingsplatform om partijen, expertise, instrumenten en middelen op één plek bij elkaar te brengen. Bijvoorbeeld door kennisvragen en -aanbod van partijen centraal te inventariseren. Maar ook door de diverse (financierings- en innovatie-)instrumenten en de informatievoorziening hierover beter te ontsluiten voor kennisinstellingen, het bedrijfsleven en medeoverheden. Zodoende versterken we, in lijn met wat de motie vraagt, de kennispositie en samenwerking rond cybersecurity-onderzoek en -innovatie in Nederland. Ik zal uw Kamer rond de zomer informeren over de verdere vormgeving van het samenwerkingsplatform.

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

[11] Kamerstuk 34 775 VI, nr. 68
[12] Kamerstuk 29 338, nrs. 187 en 205