

Vergaderjaar 2020–2021

26 643

Informatie- en communicatietechnologie (ICT)

Nr. 723

**BRIEF VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN
EN KLIMAAT**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 9 december 2020

Begin dit jaar heb ik uw Kamer geïnformeerd over de oprichting van een nieuw publiek-privaat samenwerkingsplatform voor kennis en innovatie op het gebied van cybersecurity (Kamerstuk 26 643, nr. 674). Mede namens de Minister van Justitie en Veiligheid, de Minister van Defensie, de Minister van Onderwijs, Cultuur en Wetenschap (OCW) en de Minister van Binnenlandse Zaken en Koninkrijksrelaties informeer ik uw Kamer over de stand van zaken.

Ontwikkelingen in het digitale domein volgen elkaar in een hoog tempo op. Nederland moet nu en in de toekomst maatregelen kunnen nemen tegen bekende en nog onbekende digitale dreigingen. Hiervoor is het essentieel dat de ontwikkeling en toepassing van Nederlandse kennis en kunde meebeweegt met de snelle ontwikkelingen in het digitale en technologische domein. Dit kan onder meer bereikt worden door middel van intensieve samenwerking tussen overheid, bedrijfsleven en kennisinstellingen.¹ Een hoogwaardige en autonome Nederlandse kennispositie op het gebied van cybersecurity vermindert ongewenste afhankelijkheid van expertise en oplossingen uit het buitenland. Bovendien stelt een solide kennisbasis op het terrein van cybersecurity Nederland in staat om op een veilige wijze de economische en maatschappelijke kansen van digitalisering te verzilveren.²

In deze context heeft het kabinet verkenningen laten uitvoeren door TNO, NWO en cyberveilig NL naar de mogelijkheden en aanknopingspunten voor een vernieuwde aanpak (Kamerstuk 26 643, nr. 674). Uit deze verkenningen blijkt dat samenwerking over de gehele cybersecurity kennis- en innovatieketen versterkt moet worden. Een belangrijk onderdeel van deze benodigde versterking is het beter verbinden van vraag en aanbod van cyberkennis en het beter coördineren van dit proces.

¹ Missies voor topsectoren- en innovatiebeleid, Thema Veiligheid.

² Kennis en Innovatieagenda (KIA) Veiligheid, Missie: Cyberveiligheid.

Het kabinet heeft daarom voorgesteld om een nieuw publiek-privaat samenwerkingsplatform op te richten dat de maatschappelijke krachten op het terrein van onderzoek, innovatie en onderwijs moet bundelen (Kamerstuk 26 643, nr. 674).

Het platform dient relevante partijen, expertise, instrumenten en middelen uit het cybersecurity domein bij elkaar te brengen in een thematische en ketengeoriënteerde aanpak. Daarmee bouwt het platform voort op het werk van Dcypher, met een bredere scope en meer slagkracht. Dcypher is per 1 oktober 2020 beëindigd en de transitie naar het nieuwe platform wordt zo spoedig mogelijk afgerond. Over de vormgeving van het nieuwe platform is recent advies uitgebracht door vijf kwartiermakers uit wetenschap, onderwijs, bedrijfsleven en overheid.

Advies kwartiermakers

In vervolg op de hierboven genoemde verkenningen en een informatie-bijeenkomst met betrokken maatschappelijke partners, zijn vóór de zomer vijf kwartiermakers gevraagd om advies uit te brengen over de vormgeving van het nieuwe samenwerkingsplatform. Medio augustus jl. is het definitieve adviesrapport opgeleverd. Hierin worden voorstellen gedaan voor een strategisch narratief, een thematische werkwijze, de organisatie en de financiering (zie bijlage)³.

De kwartiermakers hebben onder andere geadviseerd om zo spoedig mogelijk te starten met de inrichting van het platform. Conform het advies van de kwartiermakers zal er een bestuur moeten aantreden en een platformbureau worden opgericht, met onderwijs-, onderzoeks- en innovatiemakelaars, om de verbinding te leggen tussen het veld, experts en het platform. Daarnaast moeten er inhoudelijke thema's worden bepaald en er moet verbinding worden gelegd met het beschikbare instrumentarium van de deelnemende partijen.

Het kabinet is de kwartiermakers zeer erkentelijk voor het vele werk dat zij in korte tijd verricht hebben, en het gedegen en gedragen eindresultaat. Met het advies is een stevige basis gelegd voor de vervolgstappen die noodzakelijk zijn om te komen tot een breed gedragen publiek-privaat samenwerkingsplatform. Het advies onderstreept de doelstellingen die het kabinet wenst te bereiken met het vernieuwde platform en wij herkennen het belang van een thematische, inhoudelijk gedreven aanpak, alsmede de noodzaak om partners over de hele keten van onderwijs, onderzoek en innovatie te betrekken.

Vervolgstappen

Op basis van het advies van de kwartiermakers hebben de betrokken ministeries een aantal vervolgstappen in gang gezet.

Inrichting van het platform

Er wordt gezocht naar kandidaten voor een bestuursfunctie binnen het nieuwe platform. Doelstelling voor het bestuur is het stimuleren van bottom-up samenwerking tussen de publieke en private partijen op een thematische en ketengeoriënteerde wijze. Het bestuur stelt in samenwerking met de betrokken partners de strategie van het platform vast en ziet erop toe dat de missie en visie van het samenwerkingsplatform gerealiseerd worden. Daarnaast stelt het bestuur de activiteiten van het platform vast in het jaarlijkse werkplan, op basis van relevante

³ Raadpleegbaar via www.tweedekamer.nl.

(beleids)agenda's en overige relevante instrumenten. Betrokken partners uit het veld adviseren aan zowel bestuur als platformbureau over de operationele invulling van programma's en projecten.

Bij de invulling van het bestuur wordt toegezien op een evenredige vertegenwoordiging vanuit kennisinstellingen, bedrijfsleven en overheid, gespreid over de gebieden onderwijs, onderzoek en innovatie. Daarbij is diversiteit van het bestuur een belangrijk uitgangspunt.

De functionele leiding van het platformbureau wordt belegd bij een platformmanager. Op korte termijn zal de wervingsprocedure worden gestart voor deze functie en voor de overige bemensing van het platformbureau. Het platform wordt ondergebracht bij de Rijksdienst voor Ondernemend Nederland (RVO.nl). RVO.nl heeft veel ervaring in het ondersteunen van publiek-private samenwerking en heeft goed zicht op relevant instrumentarium voor de beoogde samenwerking.

Inhoudelijke agendering en programmering

Sinds 1 oktober 2020 wordt gewerkt aan de processen rondom de agendering en programmering van de inhoudelijke thema's. Samen met verschillende kennisinstellingen en een aantal partners uit bedrijfsleven en overheid wordt gewerkt aan concrete thematische routekaarten. Naarmate de agenderings- en programmeringsprocessen vorderen zal het platformbureau zich verder ontwikkelen. Over twee jaar zal het functioneren van het samenwerkingsplatform geëvalueerd worden.

Op dit moment is er een budget van € 5 miljoen voor onderwijs, onderzoek en innovatie op het gebied van cybersecurity.⁴ Deze middelen zullen worden ingezet voor de hierboven genoemde routekaarten op het gebied van onderwijs, onderzoek, en innovatie, en voor het platform.

Uit dit budget heeft het Ministerie van Economische Zaken en Klimaat recent de Nationale Wetenschapsagenda call «*Cybersecurity-, governance- en cryptologievraagstukken*» opgehoogd met € 1,5 miljoen. Deze onderzoekscall van in totaal circa € 9,5 miljoen wordt door zeven verschillende ministeries gefinancierd. NWO heeft, met middelen van OCW, ook € 3 miljoen bijgedragen. Het grote aantal inschrijvingen op deze call onderstreept de relevantie van het onderwerp en de betrokkenheid van de cyber community.

Tot slot

Het kabinet acht het van groot belang dat het nieuwe platform *de* plek zal worden waar onderwijs, onderzoek en innovatie op het gebied van cybersecurity effectief bij elkaar komen. Door de krachten te bundelen kan Nederland een volgende stap zetten naar een digitaal veiliger Nederland en het verzilveren van de daaraan verbonden economische kansen. Ik zal uw Kamer medio 2021 informeren over de verdere vormgeving van het samenwerkingsplatform.

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

⁴ 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-%202020191016%20definitief.pdf>.