

Vergaderjaar 2023–2024

26 643

Informatie- en communicatietechnologie (ICT)

33 009

Innovatiebeleid

Nr. 1183

BRIEF VAN DE MINISTER VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 7 juni 2024

Hierbij bied ik u namens het kabinet de agenda voor *Cybersecurity Technologies* aan, zoals aangekondigd in de Kamerbrief Nationale Technologiestrategie van 19 januari 2024 (Kamerstuk 33 009, nr. 140).

Deze uitgewerkte agenda gaat over één van de prioritaire sleuteltechnologieën onder de Nationale Technologiestrategie (NTS). De NTS is opgesteld om de Nederlandse uitgangspositie in de mondiale concurrentiestrijd te verstevigen en om ongewenste afhankelijkheden te beperken, en schetst de keuze om te investeren in tien prioritaire sleuteltechnologieën. Deze prioritaire sleuteltechnologieën kenmerken zich door een sterke basis in Nederland, een grote bijdrage aan ons verdienvermogen, een grote bijdrage aan het oplossen van maatschappelijke uitdagingen en een groot belang voor de nationale veiligheid. De prioritaire sleuteltechnologieën worden uitgewerkt in agenda's, waarin we onze positie in het internationale speelveld beschrijven, en ambities voor het verder ontwikkelen van onze positie op deze sleuteltechnologieën. De agenda's zijn door het Ministerie van Economische Zaken en Klimaat (EZK) ontwikkeld, in samenwerking met andere departementen en met inbreng van deskundigen uit het onderzoeks- en innovatie-ecosysteem.

Technologische innovaties rondom cybersecurity zijn essentieel voor een digitaal veilig, weerbaar, open, autonoom en welvarend Nederland. Om de toenemende digitale dreiging tegen te gaan en de afhankelijkheid van anderen te beperken is technologisch leiderschap belangrijk voor Nederland. Het doel van een sterke cybersecuritykennis- en innovatieketen is daarom opgenomen onder Pijler 2 van de kabinetsbrede Nederlandse Cybersecuritystrategie 2022 – 2028 (NLCS).¹ Het belang van een sterke positie op cybersecurity en het voorkomen van ongewenste afhankelijkheden op Nederlands en Europees niveau, wordt ook

¹ Kamerstuk 26 643, nr. 925

benadrukt in de agenda Digitale Open Strategische Autonomie (DOSA).² Cybersecuritytechnologie raakt alle sectoren en technologieën en zou in de basis moeten worden meegenomen in de ontwikkeling van operationele en digitale systemen in alle sectoren (*security-by-design*). Andere sleuteltechnologieën, zoals kunstmatige intelligentie, kunnen worden ingezet om systemen automater en veiliger te maken. Ook is aandacht nodig voor de risico's van deze sleuteltechnologieën, zoals de impact van de kwantumcomputer op versleutelde data. De noodzaak voor gerichte investeringen in kennis en innovatie op het gebied van cybersecuritytechnologie is daarom groot.

Deze agenda beschrijft het belang van cybersecuritytechnologieën in een voortdurend digitaliserende samenleving en snel veranderend cyberdreigingslandschap. Ook wordt het nationale en internationale speelveld beschreven, inclusief de kansen en uitdagingen voor het opschalen en ontwikkelen van cybersecuritytechnologieën in Nederland. Op basis van de ronde-tafelgesprekken met partijen uit het onderzoeks- en innovatie-ecosysteem zijn voorstellen gedaan voor de hoofd- en deelambities voor cybersecuritytechnologie.

In de Kamerbrief van 19 januari 2024 is aangegeven dat de NTS een volgend kabinet helpt om nadere invulling te geven aan het strategisch technologie-, innovatie- industrie- en ondernemerschapsbeleid. In lijn met de andere agenda's voor de NTS kunnen ook voor het cybersecuritygedeelte publiek-private samenwerking, samenwerking met de regio's, Europese samenwerking en het vrijmaken van voldoende (financiële) middelen belangrijk zijn. Keuzes hieromtrent zijn aan een volgend kabinet. Later dit jaar zal uw Kamer nader geïnformeerd worden over de verdere uitwerking van de NTS.

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

² Kamerstuk 36 259, nr. 21.