Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

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

3108

Vragen van de leden **Yesilgöz-Zegerius** en **Rajkowski** (beiden VVD) aan de Minister van Justitie en Veiligheid en de Staatssecretaris van Economische Zaken en Klimaat over *het bericht «Nederland verliest controle op beveiliging van het internet»* (ingezonden 19 mei 2021).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens Staatssecretaris van Economische Zaken en Klimaat (Keijzer) (ontvangen 8 juni 2021).

Vraag 1
Bent u bekend met het artikel «Nederland verliest controle op beveiliging van het internet?»[1]

Antwoord 1
Ja.

Vraag 2 en 3
Hoe beoordeelt u het advies van de Cyber Security Raad dat het kabinet dringend moet ingrijpen om te voorkomen dat onze economie te afhankelijk wordt van buitenlandse technologie? Kunt u uw analyse toelichten?
Hoe beoordeelt u de onderliggende waarschuwing van de Cyber Security Raad dat Nederland haar greep op de beveiliging van het internet anders dreigt kwijt te krijgen? Kunt u uw analyse toelichten?

Antwoorden 2 en 3
Op 14 mei jl. heeft de Cyber Security Raad (CSR) het advies «Nederlandse Digitale Autonomie en Cybersecurity» uitgebracht. Het vraagstuk van digitale autonomie en het verhogen van onze digitale weerbaarheid heeft de nadrukkelijke aandacht van het kabinet. Digitale autonomie is echter geen vanzelfsprekendheid.
Nederland is verweven met de mondiale economie die bestaat uit een veelheid aan onderlinge, wederzijdse afhankelijkheden. Dat betekent dat leveranciers van over de hele wereld als onderdeel van complexe waardeketens producten en diensten leveren in het digitale domein. Deze verweven-

[1] Het Financieele Dagblad, 14 mei 2021, «Nederland verliest controle op beveiliging van het internet», https://fd.nl/economie-politiek/1383703/adviesraad-kabinet-nederland-verliest-controle-op-beveiliging-internet

ah-tk-20202021-3108
ISSN 0921 - 7398
's-Gravenhage 2021

heid biedt in algemene zin zeer grote economische voordelen, is in een open en gespecialiseerde economie onvermijdelijk en kan bijdragen aan een weerbare internationale economische positie van Nederland. Door deze verwevenheid kunnen er in het digitale domein echter ook ongewenste afhankelijkheidsrelaties met partijen van buiten EU ontstaan. Dit kan onze publieke belangen, waaronder onze (nationale) digitale veiligheid, in het geding brengen. De CSR wijst er in zijn advies op dat ongewenste (digitale) afhankelijkheden een bedreiging kunnen vormen die geadresseerd moeten worden. Tegelijkertijd onderschrijft de CSR dat naast de dreiging die uitgaat van deze afhankelijkheidsrelaties, globalisering enorme voordelen voor Nederland heeft gebracht. Balkanisering (versplintering) van technologie en protectionisme kan wereldwijde handel belemmeren en daarmee ook welvaart en banen kosten in Nederland, aldus de CSR.
Bij het adresseren van ongewenste afhankelijkheidsrelaties moeten protectionisme en fragmentatie dan ook zo veel mogelijk worden vermeden. In dat licht ziet het kabinet digitale autonomie niet als doel op zich maar als middel. Dit moet, in samenspraak met onze Europese partners, zorgvuldig en proportioneel worden bezien zodat Nederland het vermogen heeft om voldoende voor de eigen publieke belangen, waaronder onze (nationale) digitale veiligheid, op te komen en deze belangen zeker te stellen.
Het is nodig voor onze digitale autonomie dat we open, eerlijke en duurzame internationale relaties aangaan, waarbij onze normen en waarden zijn beschermd. De voordelen van internationale handel en investeringen, toegang tot wereldwijde waardeketens en internationale concurrentie moeten zoveel mogelijk behouden blijven.
Tegelijkertijd is het zaak dat we actief blijven investeren in de weerbaarheid van onze digitale infrastructuur. Waar nodig en wenselijk moeten we maatregelen nemen om ongewenste strategische afhankelijkheden weg te nemen of te voorkomen. Om tot effectieve en proportionele maatregelen te komen dient een zorgvuldige analyse van en afweging tussen de risico's en de verwachte (veiligheids)baten en de verwachte kosten van de mogelijke maatregelen.
Er lopen al acties die concreet bijdragen aan onze digitale autonomie. Zo wordt binnen het nieuwe samenwerkingsplatform voor kennis en innovatie cybersecurity (dcypher) gewerkt aan een routekaart voor cryptocommunicatie. Het kabinet werkt daarnaast voortdurend aan de versterking van de digitale weerbaarheid via het beleid dat is uiteengezet in de Nederlandse Cybersecurity Agenda (NCSA). Bij de beoordeling van risico's ten aanzien van spionage, beïnvloeding of sabotage door statelijke actoren of andere partijen bij digitale producten hanteert het kabinet de overwegingen die zijn vermeld in de brief aan de Tweede Kamer over C2000.[2] Meer specifiek voor de telecommunicatiesector heeft het kabinet op 1 juli 2019 aanvullende beschermingsmaatregelen aangekondigd op basis van een risicoanalyse die is uitgevoerd door de Taskforce Economische Veiligheid[3]. Dit heeft er onder andere toe geleid dat mobiele netwerk operators in kritieke onderdelen alleen gebruik mogen maken van vertrouwde leveranciers.
Daarnaast overweegt Nederland deelname aan een Important Project of Common European Interest voor Cloudinfrastructuur en services (IPCEI CIS), een concreet Europees project wat als doel heeft om nieuwe generatie cloud-oplossingen in Europa te ontwikkelen en de waardeketen in Europa te versterken. Ook kijkt Nederland naar deelname aan een Important Project of Common European Interest voor de semiconductorsector (IPCEI Microelektronica 2, IPCEI ME2). De resultaten om onder het Nederlandse bedrijfsleven en kennisinstellingen de belangstelling te identificeren volgen in de zomer.
Het is essentieel dat we nu en in de toekomst blijven inzetten op digitale autonomie en cybersecurity.

Vraag 4
Wat is de status van de uitvoering van de motie van de leden Buitenweg en Yesilgöz-Zegerius over inzicht verkrijgen in de afhankelijkheid van digitale processen en diensten bij vitale processen? In hoeverre zijn processen van

[2] Kamerstuk 25 124, nr. 96
[3] Kamerstuk 30 821, nr. 92.

onze vitale infrastructuur ondergebracht en afhankelijk van buitenlandse aanbieders? In hoeveel van deze gevallen is het beheer van deze digitale processen uitbesteed aan buitenlandse aanbieders? Hoeveel van deze aanbieders zijn gevestigd in staten die een offensief cyberprogramma kennen?[4]

Antwoord 4
Met de brief «Beleidsreactie op het Dreigingsbeeld Statelijke Actoren (DBSA) en voortgang aanpak statelijke dreigingen» gaf het kabinet invulling aan de motie Buitenweg/Yesilgöz-Zegerius over het inzichtelijk maken van cyberafhankelijkheden in vitale processen.[5] Hierin wordt de opzet van een structurele aanpak voor de telecomsector benoemd. Ook staat hierin aangegeven dat in de komende periode in kaart wordt gebracht wat er nodig is qua mensen, middelen en expertise om deze aanpak te verbreden naar andere vitale processen.
Er wordt niet integraal bijgehouden in hoeverre de dienstverlening binnen vitale processen plaatsvindt door of afhankelijk is van buitenlandse aanbieders, en daarmee ook niet in hoeveel gevallen het beheer van digitale processen wordt uitbesteed aan buitenlandse aanbieders. Dit is, gezien het grote aantal leveranciers van producten en diensten van vitale processen, ook niet realistisch. Uitgangspunt is een risicogestuurde aanpak, zodat dreigingen en kwetsbaarheden gericht kunnen worden geadresseerd. Zo zijn binnen de aanpak tegengaan statelijke dreigingen verschillende instrumenten ontwikkeld en maatregelen genomen om nationale veiligheidsrisico's te adresseren, zoals de voorbereiding van wetgeving ten behoeve van het stelsel van investeringstoetsing en de herziening en beschikbaarstelling van het instrumentarium voor inkoop en aanbesteding.[6]

Vraag 5
Bent u het met de mening eens dat het uit nationale veiligheidsoverwegingen, onwenselijk is om digitale technologieën die wij gebruiken voor vitale processen zoals energievoorziening en betalingsverkeer af te nemen van staten met een offensief cyberprogramma? Zo ja, waar liggen volgens u mogelijkheden om meer grip te krijgen op de digitale processen van onze vitale infrastructuur? Zo nee, waarom niet?

Antwoord 5
Zoals in het Dreigingsbeeld Statelijke Actoren (DBSA) beschreven is een toenemende afhankelijkheid van buitenlandse technologie een gegeven, aangezien geen land beschikt over alle kennis en productiemiddelen om technologisch onafhankelijk te opereren.[7]
Tegelijkertijd bestaan er risico's op digitale spionage en -sabotage, die kunnen leiden tot verstoring van de continuïteit van de vitale infrastructuur en aantasting van de integriteit of exclusiviteit van gevoelige kennis en informatie. Een aanvullend risico kan ontstaan als er betrokkenheid is van leveranciers die afkomstig zijn, of onder controle staan van bedrijven, uit een land met wetgeving die commerciële partijen dwingt tot samenwerking met de overheid van dat land. De risico's voor de nationale veiligheid worden verder vergroot als het land in laatstbedoelde zin een offensief inlichtingenprogramma voert dat gericht is op Nederlandse belangen. Van belang is het juist ook met betrekking tot deze risico's telkens te bepalen of en welke beheersmaatregelen mogelijk, wenselijk, en realiseerbaar zijn om voldoende bescherming hiertegen te bieden.
Versterking van de weerbaarheid van netwerk- en informatiesystemen is dan ook van groot belang. Het kabinet werkt hieraan via de aanpak statelijke dreigingen, de versterkte aanpak vitaal en de aanpak zoals beschreven in de Nederlandse Cybersecurity Agenda (NCSA). Het in kaart brengen van de te beschermen belangen en de daarop betrekking hebbende dreigingen, alsmede het nemen van maatregelen om die belangen te beschermen, staan daarbij steeds centraal. De combinatie van technologische ontwikkelingen en

[4] Kamerstuk 35 570 VI, nr. 38
[5] Kamerstuk 30 821, nr. 125
[6] Kamerstuk 30 821, nr. 125
[7] Kamerstuk 30 821, nr. 125

geopolitieke veranderingen vraagt erom met een andere blik te kijken naar welke belangen we willen beschermen. Hiervoor wordt nauw samengewerkt met onder meer bedrijven en kennisinstellingen. Met een geactualiseerd instrumentarium worden deze veranderende omstandigheden integraal meegewogen in het beoordelen van risico's en bij het naar aanleiding daarvan waar nodig nemen van weerbaarheidsverhogende maatregelen. Hierbij wordt digitale en fysieke weerbaarheid in zijn geheel bezien. Ketenafhankelijkheden worden daarbij beter in kaart gebracht, omdat vitale processen onderling sterk verweven zijn en sterk afhankelijk zijn van toeleveranciers.

Vraag 6
Hoeveel geld ontvangt Nederland jaarlijks uit het EU Resilience and Recovery Fund om te investeren in digitale innovaties? Hoe groot is dit bedrag ten opzichte van andere lidstaten? Op basis van welke voorwaarden wordt dit geld verdeeld onder lidstaten?

Antwoord 6
Nederland ontvangt naar verwachting € 5,96 mld. aan middelen uit de Recovery and Resilience Facility. Om aanspraak te maken op de RRF-middelen moet Nederland een Recovery and Resilience plan (RRP) indienen met ambitieuze hervormingen en investeringen die invulling geven aan de landspecifieke aanbevelingen die de Europese Commissie voor Nederland heeft geïdentificeerd. Deze middelen moeten ingezet worden voor het bevorderen van economisch herstel en het aanjagen van de groene en digitale transitie. Minstens 20% van de middelen moeten ten goede komen aan de digitale transitie. Hiernaast moet minstens 37% bijdragen aan de groene transitie. De middelen worden in tranches uitgekeerd op basis van het behalen van vooraf geformuleerde mijlpalen en doelen die voor 31 augustus 2026 moeten zijn afgerond. Dezelfde voorwaarden zijn van toepassing op andere lidstaten. Het staat lidstaten verder vrij om binnen de criteria uit de RRF-verordening meer focus te leggen op de digitale transitie in hun eigen RRP's.
De allocaties uit de RRF worden op twee momenten vastgesteld. De allocatie voor 2021–2022 is gebaseerd op werkloosheidscijfers (2015–2019), de omvang van de bevolking (2019) en het bbp per capita (2019). Voor de allocatie in 2023 geldt een aangepaste verdeelsleutel waarbij de factor werkloosheid wordt vervangen door (in gelijke delen) het bbp-verlies in 2020 en het cumulatieve bbp-verlies over de periode 2020–21 op basis van de cijfers die eind juni 2022 beschikbaar zijn. Op de website van de Europese Commissie vindt u de allocatie van de RRF-middelen per lidstaat[8]. Lidstaten worden geacht een RRP in te dienen voor 100% van de verwachte allocatie. Naar aanleiding van de definitieve vaststelling kunnen lidstaten hun RRP's wijzigen voor zover de definitieve allocatie is gewijzigd.

Vraag 7
Bent u het met de mening eens dat het voor Nederland, zowel uit veiligheids- als innovatieoogpunt van groot belang is dat wordt geïnvesteerd in Nederlandse technologie? Zo ja, hoe beoordeelt u het bedrag dat Nederland jaarlijks ontvangt uit het EU Resilience and Recovery Fund? Zo nee, waarom niet?

Antwoord 7
Ja, vanuit zowel veiligheids- als innovatieoogpunt is het van groot belang dat wij blijven investeren in technologische ontwikkeling. Het bedrag dat Nederland zal ontvangen vanuit de Resilience and Recovery Facility is een welkome aanvulling. De RRF-middelen betreft echter een incidentele impuls en is daarmee van beperkte meerwaarde voor de uitdagingen waar Nederland voor staat. Het is voor onze brede welvaart van groot belang dat wij ook structureel blijven investeren in het versterken van onze lange termijn verdienvermogen.

Vraag 8
Kunt u deze vragen binnen de gestelde termijn beantwoorden?

[8] https://ec.europa.eu/info/files/recovery-and-resilience-facility-grants-allocation-member-state_nl

Antwoord 8
Ja.