Regels ter uitvoering van Verordening (EU) 2019/881 (Uitvoeringswet cyberbeveiligingsverordening)

NOTA NAAR AANLEIDING VAN HET VERSLAG

I. ALGEMEEN

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel Uitvoeringswet cyberbeveiligingsverordening. Cyberveiligheid vereist gezien haar grensoverschrijdende karakter, naast een nationale aanpak, ook Europese inspanningen. Deze leden hebben nog enkele vragen over dit wetsvoorstel.

De leden van de D66-fractie hebben met interesse kennisgenomen van de Uitvoeringswet cyberbeveiligingsverordening en onderstrepen het belang van een geharmoniseerde certificatiesystematiek om de cyberbeveiliging in de Europese Unie te vergroten en versterken. Deze leden hebben nog enkele vragen.

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Zij hebben hierover verschillende vragen en opmerkingen.

De leden van de SP-fractie hebben kennisgenomen van het wetsvoorstel en hebben hierover nog enkele vragen.

De leden van de GroenLinks-fractie hebben met belangstelling kennisgenomen van het voorliggende wetsvoorstel. De coronacrisis heeft de reeds bestaande trend van snelle digitalisering nog verder aangezet en de voordelen van digitalisering eens te meer duidelijk gemaakt. Aan de andere kant brengt digitalisering ook kwetsbaarheden met zich mee. Het is van groot belang dat de cyberbeveiliging van digitale producten, diensten en processen goed op orde is.

De leden van de ChristenUnie-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel. Deze leden constateren dat dit wetsvoorstel tot doel heeft cyberbeveiliging op Europees niveau vast te stellen door middel van cyberbeveiligingscertificeringsregelingen. Zij onderschrijven dit doel. Zij hebben hierover nog wel enkele vragen.

Met belangstelling heb ik kennisgenomen van de vragen van de leden van de vaste commissie voor Economische Zaken en Klimaat over het wetsvoorstel uitvoeringswet cyberbeveiligingsverordening (Kamerstukken 35 838, hierna: het wetsvoorstel). Hieronder ga ik graag in op de vragen en opmerkingen van de leden van de fracties van de VVD, D66, het CDA, SP, GroenLinks en de ChristenUnie. Daarbij volg ik de inhoudsopgave van het verslag waarbij in een aantal gevallen naar antwoorden op samenhangende vragen wordt verwezen.

1. De hoofdlijnen van de cyberbeveiligingsverordening

a) Reikwijdte

De leden van de VVD-fractie vinden het onduidelijk welke ICT-producten, -diensten en -processen gemoeid zijn met dit wetsvoorstel. Zij vragen de regering meer duidelijkheid te geven over welke producten en diensten dit wetsvoorstel beoogt te certificeren? Wat is hierin het aandeel van slimme apparaten?

Met het wetsvoorstel wordt uitvoering gegeven aan enkele bepalingen van Verordening (EU) nr. 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (hierna: de cyberbeveiligingsverordening). Deze verordening biedt een kader om op Europees niveau cyberveiligheidscertificeringsregelingen te ontwikkelen en certificering uit te voeren. Dit kader kent een brede reikwijdte inzake de categorieën van ICT-producten, - diensten en - processen die gecertificeerd kunnen worden. Hiermee kan de Europese Commissie voor een breed segment van ICT-producten, -diensten en processen Europese cyberbeveiligingscertificeringsregelingen opstellen.
Momenteel worden er twee Europese cyberbeveiligingscertificeringsregelingen ontwikkeld. Het gaat om een cyberbeveiligingscertificeringsregeling voor ICT-beveiligingsproducten (EUCC) en een cyberbeveiligingscertificeringsregeling voor clouddiensten. In het werkprogramma van de Europese Commissie zijn de eerste categorieën van ICT-producten, -diensten en –processen genoemd waarvoor Europese cyberbeveiligingscertificeringsregelingen worden ontwikkeld. In het werkprogramma kondigt de Europese Commissie aan dat het de intentie heeft om een Europese cyberbeveiligingscertificeringsregeling voor slimme apparaten voor consumenten te ontwikkelen.

Daarnaast is de Europese Commissie voornemens om Europese cyberbeveiligingscertificeringsregelingen te ontwikkelen voor 5G-netwerkapparatuur en geautomatiseerde industriële controlesystemen.

De leden van de VVD-fractie vragen hoe het mandaat van het Europees Agentschap voor netwerk- en informatiebeveiliging (Enisa) zich verhoudt tot dat van het Computer Emergency Response Team for the EU Institutions, bodies and agencies (CERT-EU).
Het mandaat van Enisa is vastgelegd in de cyberbeveiligingsverordening. De verantwoordelijkheden van Enisa op grond van deze verordening beslaan onder andere het bijdragen aan Europees cyberbeleid, het verhogen van de betrouwbaarheid van ICT-producten, -diensten en -processen door middel van certificering en het adviseren over uitdagingen op het gebied van cybersecurity voor de toekomst. Enisa vervult deze rol door het delen van kennis, het verhogen van bewustzijn en capaciteitsopbouw. Enisa is dus het expertisecentrum op het gebied van cybersecurity voor de EU en haar lidstaten.
CERT-EU is het Computer Emergency Response Team (CERT) voor de EU-instellingen, agentschappen en lichamen. Dit betekent dat CERT-EU op grond van de Europese NIB-richtlijn[1] deze doelgroepen kan adviseren en bijstand kan leveren op het gebied van preventie, detectie en respons tegen cyberaanvallen. In tegenstelling tot Enisa heeft CERT-EU daarbij een operationele rol.

De leden van de VVD-fractie lezen in de memorie van toelichting dat de Europese Commissie bevoegd wordt om Europese cyberbeveiligingscertificeringsregelingen voor ICT-producten, -diensten en -processen vast te stellen. Op basis van welke indicatoren gaat de Europese Commissie deze regelingen vaststellen? Hoe zijn deze indicatoren tot stand gekomen?
De cyberbeveiligingsverordening biedt een kader op grond waarvan er Europese cyberbeveiligingscertificeringsregelingen vastgesteld kunnen worden. In het antwoord van een eerdere vraag van de VVD fractie hierover is toegelicht dat de Europese Commissie onder meer in het voortschrijdend werkprogramma van de Unie een aantal prioriteiten voor de ontwikkeling van cyberbeveiligingscertificeringsregelingen heeft geïdentificeerd, gebaseerd op de criteria genoemd in artikel 47, derde lid, van de cyberbeveiligingsverordening, waaronder voor clouddiensten. De lidstaten zijn betrokken bij de het tot stand komen van het genoemde werkprogramma, middels de Europese Groep voor cyberbeveiligingscertificering (de „EGC", een adviesgremium bestaande uit de lidstaten). Daarnaast adviseert een adviserend gremium bestaande uit stakeholders de Europese Commissie hierbij.
De cyberbeveiligingsverordening stelt eisen aan de ontwikkeling en inhoud waaraan elke Europese cyberbeveiligingscertificeringsregeling moet voldoen. Een aantal minimumeisen staat in artikel 54 van de cyberbeveiligingsverordening genoemd.

De leden van de CDA-fractie lezen dat de cyberbeveiligingsverordening lidstaten vrijlaat om aanvullende maatregelen te nemen om het gebruik van de in beginsel voor de commerciële markt bedoelde gecertificeerde ICT-producten, -diensten en -processen in de voornoemde domeinen te beperken, te verbieden of hieraan aanvullende eisen te stellen. Zij vragen of de regering voornemens is dit te doen.
De regering is op dit moment niet voornemens om op nationaal niveau aanvullende maatregelen op het gebied van openbare beveiliging, defensie, nationale veiligheid en activiteiten van de staat op het gebied van het strafrecht te nemen welke leiden tot het beperken, verbieden of stellen van aanvullende eisen.

De leden van de SP-fractie lezen dat met de verordening de Europese Commissie bevoegd wordt om Europese cyberbeveiligingscertificeringsregelingen voor categorieën van ICT-producten, -diensten en processen vast te stellen. Zij vragen waar de behoefte voor deze soevereiniteitsoverdracht vandaan komt. Immers, de verordening heeft geen betrekking op bevoegdheden van lidstaten betreffende activiteiten inzake openbare beveiliging, defensie, nationale veiligheid en strafrecht aangezien deze thema's onder de nationale competentie van lidstaten vallen. De leden vragen wat de verordening effectief zal betekenen in het bevorderen van cyberveiligheid, of dat zij met name de markt voor cyberveiligheidsproducten zal bevorderen?
De regering is positief ten aanzien van de subsidiariteit van de cyberbeveiligingsverordening, gezien het inherent grensoverschrijdende karakter van cyberbeveiliging en cyberdreiging. Ten aanzien van het certificeringsraamwerk zijn de voordelen van schaalvergroting het grootst wanneer certificaten EU-breed gelden en de Digitale Interne Markt wordt hierdoor versterkt. De Europese

[1] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194)

cyberbeveiligingscertificeringsregelingen hebben immers een EU brede werkingssfeer en bevatten beveiligings- en beschermingsvoorschriften ten aanzien van ICT-producten, -diensten en -processen, hierdoor ontstaat meer uniformiteit inzake de cyberbeveiliging, wordt het gelijke speelveld in de digitale interne markt behouden en de concurrentiepositie van Nederlandse bedrijven versterkt. Daarnaast blijft de mogelijkheid bestaan om in het kader van de nationale veiligheid aanvullende nationale maatregelen te treffen.
De cyberbeveiligingsverordening levert tevens een bijdrage aan het versterken van vertrouwen van burgers en bedrijven in de veiligheid van producten en diensten. Op dit moment is deze markt sterk versnipperd en functioneert daardoor niet effectief. De schaalvergroting die optreedt door ontwikkeling van Europees geharmoniseerde certificeringsregelingen kan certificering op EU-niveau efficiënter maken. Deze effecten kunnen niet door de lidstaten afzonderlijk worden bereikt.

De leden van de GroenLinks-fractie lezen in de memorie van toelichting dat de verordening voorziet in de harmonisatie van de vereisten die worden gesteld aan certificaten. Waarom is er niet gekozen voor harmonisatie van de certificaten zelf? Leidt de huidige opzet niet alsnog tot een grote proliferatie aan verschillende certificaten, waardoor eindgebruikers alsnog het overzicht verliezen? Leidt het bovendien niet ertoe dat bedrijven kunnen inzetten op certificatieshopping, waarbij ze certificaten aanvragen bij beoordelingsinstanties in lidstaten die makkelijker zijn in het afgeven van certificaten? Op welke manier wordt dit risico beperkt? Is het niet duidelijker en effectiever om tot een Europees certificaat te komen?
Inderdaad voorziet de cyberbeveiligingsverordening in de harmonisatie van de vereisten die worden gesteld aan de Europese cyberbeveiligingscertificaten. De verordening voorziet in het creëren van een geharmoniseerd Europees certificatiestelsel, waarbij in verschillende EU landen certificaten voor ICT-producten, -diensten, en -processen op dezelfde wijze worden uitgegeven, aan de hand van een specifieke Europese cyberbeveiligingscertificeringsregeling. In die zin is er dus sprake van een Europees cyberbeveiligingscertificaat, en van harmonisatie van de certificaten zelf.

De leden van de GroenLinks-fractie vragen of het cyberbeveiligingscertificeringskader enkel toeziet op certificatieschema's van lidstaten, of ook op schema's die worden beheerd door particuliere organisaties.
Het cyberbeveiligingscertificeringskader ziet toe op Europese cyberbeveiligingscertificeringsregelingen die op grond van de cyberbeveiligingsverordening zijn vastgesteld. Het heeft geen betrekking op private initiatieven. Met de inwerkingtreding van een nieuwe Europese cyberbeveiligingscertificeringsregeling onder de cyberbeveiligingsverordening, vervallen eventuele publieke nationale certificeringsregelingen. Eventuele private initiatieven kunnen hiernaast blijven bestaan.

De leden van de ChristenUnie-fractie lezen in de memorie van toelichting dat met dit wetsvoorstel wordt gestreefd naar een geharmoniseerd kader voor het ontwikkelen van certificeringsregelingen. Deze leden onderschrijven het belang van het voorkomen van fragmentatie van de Europese digitale interne markt. Toch lezen zij ook in het advies van de Afdeling advisering van de Raad van State dat verplichte certificering op Europees niveau mogelijk pas over enkele jaren wordt verwacht. De regering zal tot die tijd de markt stimuleren om gebruik te maken van de bestaande certificeringstrajecten. Deze leden vragen of er problemen kunnen ontstaan in de transitie van de bestaande nationale certificeringsregelingen naar de nog te verwachten Europese cyberbeveiligingscertificeringsregelingen die pas over enkele jaren verwacht worden. Deze leden vragen de regering hoe deze transitie vormgegeven wordt om het doel van voorkomen van fragmentatie van de Europese digitale interne markt te bewerkstelligen.
Nederland kent momenteel één nationale cyberbeveiligingscertificeringsregeling, namelijk het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB). De Europese markt is op dit moment gefragmenteerd. De inwerkingtreding van de Europese cyberbeveiligingscertificeringsregelingen zal tot verdere harmonisering leiden. Bij de ontwikkeling van de Europese cyberbeveiligingscertificeringsregelingen is er specifiek aandacht voor het borgen van een goede transitie. De insteek van de Europese Commissie en de EGC z(Europese Groep voor cyberbeveiligingscertificering, een adviesgremium bestaande uit de lidstaten) is ervoor te zorgen dat er geen situaties ontstaan waarbij zowel de nationale cyberbeveiligingscertificeringsregeling als de Europese cyberbeveiligingscertificeringsregelingen tegelijkertijd niet meer van toepassing zijn. Het dient dan ook mogelijk te blijven voor fabrikanten en aanbieders om te laten certificeren.

b) Nationale cyberbeveiligingscertificeringsautoriteit
De leden van de VVD-fractie stellen vragen over het feit dat binnen deze wet de mogelijkheid bestaat van conformiteitszelfbeoordeling waarbij een fabrikant of aanbieder zelf in plaats van een onafhankelijke instantie, bepaalt of er aan voorschriften van de certificeringsregeling is voldaan.

Hoe beoordeelt de regering deze mogelijkheid in het kader van onafhankelijke toetsing en daarmee ook de doelmatigheid van dit wetsvoorstel?
De regering juicht het toe dat fabrikanten of aanbieders een conformiteitszelfbeoordeling kunnen doen. Bij een conformiteitszelfbeoordeling voert de fabrikant of de aanbieder van ICT-producten, -diensten of -processen zelf alle inspecties uit om te zorgen dat de ICT-producten, -diensten of -processen in overeenstemming zijn met de Europese cyberbeveiligingscertificeringsregeling. Dit betreft een efficiënte mogelijkheid voor fabrikanten of aanbieders om aan te tonen dat is voldaan aan de eisen van de betreffende cyberbeveiligingscertificeringsregeling. Om de doelmatigheid van het wetsvoorstel te behouden, is een aantal voorwaarden gesteld aan de conformiteitszelfbeoordeling. De mogelijkheid van conformiteitszelfbeoordeling dient expliciet te zijn bepaald in de desbetreffende Europese cyberbeveiligingscertificeringsregeling en wordt enkel geschikt geacht voor ICT-producten, -diensten en -processen met een geringe complexiteit (eenvoudig ontwerp- en productiemechanismen) die een laag risico voor het openbaar belang opleveren. Voorts dient conformiteitszelfbeoordeling ten aanzien van ICT-producten, -diensten of -processen alleen te worden toegestaan wanneer deze zekerheidsniveau „basis" hebben. Bovendien is het toezichthoudende kader onverkort van toepassing op de EU-conformiteitsverklaringen die is afgegeven na de conformiteitszelfbeoordeling.

De leden van de VVD-fractie vragen hoe en door welke instantie wordt bepaald welk zekerheidsniveau (basis, substantieel en hoog) geldt voor welk product, dienst of proces. Op basis van welke parameters wordt dit gedaan?
Per Europese cyberbeveiligingscertificeringsregeling worden de betreffende categorieën van ICT-producten, -diensten of -processen op welke de regeling van toepassing is, vastgelegd. Daarbij gaat de Europese cyberbeveiligingscertificeringsregeling ook in op de zekerheidsniveaus die van toepassing kunnen zijn, en welke eisen gelden per zekerheidsniveau. De desbetreffende aanbieder kan dan bij een aanvraag voor een certificaat zelf kiezen voor welk zekerheidsniveau het ICT-product, dienst of proces gecertificeerd moet worden.
De Europese cyberbeveiligingscertificeringsregelingen worden door de Europese Commissie vastgesteld. De Europese Commissie doet voor het opstellen van een certificeringsregeling een verzoek aan Enisa. Bij de uitwerking van de certificeringsregelingen vindt nauwe samenwerking plaats met de Europese Groep voor cyberbeveiligingscertificering. Ook wordt bij de ontwikkeling van een certificeringsregeling een ad-hoc werkgroep ingericht. Vervolgens stelt de Europese Commissie de certificeringsregelingen vast door middel van uitvoeringshandelingen.

De leden van de VVD-fractie lezen dat de nationale autoriteit de mogelijkheid heeft om sancties op te leggen aan aanbieders en producenten wanneer zij hun verplichtingen niet nakomen. In hoeverre wordt bij het opleggen van deze sancties rekening gehouden met het zekerheidsniveau van de aangeboden producten/diensten/processen?
Het zekerheidsniveau is op zichzelf geen factor waar rekening mee moet worden gehouden bij het opleggen van sancties. Het zekerheidsniveau is gekoppeld aan de eisen voor het behalen van een certificaat.
Bij cyberbeveiligingscertificering gaat het in de kern om het waarborgen van het publieke vertrouwen in het certificaat. Dat vertrouwen staat los van het zekerheidsniveau van het certificaat, ook de afnemers van ICT-producten, -processen of -diensten van certificaten (o.a. bedrijven, consumenten, overheidsorganisaties) op een lager zekerheidsniveau moeten kunnen vertrouwen op de kwaliteit van het certificaat. In dat opzicht worden alle certificaten gelijk behandeld.

De leden van de VVD-fractie lezen verder dat de nationale autoriteit het mandaat krijgt om cyberbeveiligingscertificaten met zekerheidsniveau hoog weer in te trekken indien het certificaat niet blijkt te voldoen aan de voorliggende certificeringsregeling. Ligt er een bepaalde overweging ten grondslag aan de mogelijkheid om louter certificaten met zekerheidsniveau hoog in te trekken? Zo ja, welke analyse ligt hieronder? Welke (juridische) mogelijkheden hebben fabrikanten of aanbieders in het geval van intrekking van certificaten nog?
Een intrekkingsbesluit is een besluit in de zin van de Algemene wet bestuursrecht waartegen bezwaar en beroep open staan. Belanghebbenden, zoals fabrikanten of aanbieders, kunnen volgens de gebruikelijke procedures bezwaar aantekenen tegen een intrekkingsbesluit van de nationale autoriteit.

De leden van de CDA-fractie lezen in de memorie van toelichting dat de cyberbeveiligingsverordening stelt dat iedere lidstaat een (of meerdere) nationale cyberbeveiligingscertificeringsautoriteit(en) moet aanwijzen die met toezichthoudende taken wordt belast. Onder andere Cyberveilig Nederland merkt in reactie op het wetsvoorstel op dat de nationale autoriteit over voldoende personele middelen dient te beschikken. Deze leden vragen of

dit op tijd gaat lukken, gelet op de schaarste aan ICT-personeel die dikwijls eerder hun weg vinden naar het bedrijfsleven in plaats van naar de overheid. Welke wervingsacties worden op dit terrein ondernomen? Waarom is er niet voor gekozen het Nationaal Cyber Security Centrum als nationale autoriteit aan te wijzen? Onderkent de regering dat het toezicht op cyberveiligheid nu heel gefragmenteerd is, terwijl er steeds vaker bevoegdheden/taken op dit terrein vanuit Europa geïmplementeerd zullen moeten worden, zonder dat er een echt geschikte toezichthouder is?
Vanuit het oogpunt van effectiviteit en efficiëntie wordt de nationale cyberbeveiligingscertificeringsautoriteit ondergebracht bij een bestaande organisatie, zijnde het Agentschap Telecom, die geruime ervaring heeft met zowel uitvoerende als, afdoende daarvan gescheiden, toezichthoudende werkzaamheden binnen het digitale domein. Zo houdt AT niet alleen toezicht op de zorgplicht van aanbieders van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten maar ook op de wetgeving inzake elektronische handtekeningen. Ook is AT de toezichthouder op de Wet beveiliging netwerk- en informatiesystemen (Wbni) voor de energiesector, digitale infrastructuur en digitale diensten. AT is daarom al enige jaren actief en succesvol met het uitbreiden van de expertise inzake cyberbeveiliging.
Het Nationaal Cyber Security Centrum (NCSC) is het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. Op grond van de Wbni heeft het NCSC onder andere de taak de rijksoverheid en vitale aanbieders te informeren, te adviseren en waar nodig te ondersteunen bij dreigingen en incidenten met betrekking tot netwerk- en informatiesystemen. Het NCSC draagt bij aan het vergroten van de digitale weerbaarheid van de Nederlandse samenleving, en is daarbij geen toezichthouder. De rol als nationale cyberbeveiligingscertificeringsautoriteit past daarom niet bij het NCSC.
Cybersecurity is een vraagstuk wat in alle sectoren speelt en ook onder de verantwoordelijkheid valt van elke minister. Bij het implementeren van Europese (sectorale) wet- en regelgeving is het van belang om ook het toezicht te beleggen bij de toezichthouder met kennis en ervaring van de desbetreffende sector. Het aanwijzen van AT als nationale cyberbeveiligingscertificeringsautoriteit past bij de bestaande verantwoordelijkheden, kennis en ervaring.

c) Europese cyberbeveiligingscertificeringsregelingen
De leden van de VVD-fractie constateren dat Enisa om de vijf jaar elke vastgestelde Europese cyberbeveiligingscertificeringsregeling evalueert. Op basis van welke analyse is deze termijn vastgesteld? Hoe verhoudt deze termijn zich tot de driejarige termijn van de Europese Commissie om bepaalde certificeringsregelingen verplicht te stellen? Ziet de regering ruimte om deze termijnen samen te brengen om verplichting logischer te laten volgen op evaluatie?
Europese cyberbeveiligingscertificeringsregelingen zullen op verschillende momenten in de tijd gereed zijn en kennen vanaf het moment van de publicatie een eigen evaluatiecyclus van vijf jaar. Deze evaluatie heeft betrekking op de inhoud van de regeling - de cyberbeveiligingsnormen, evaluatiemethoden en accreditatievoorwaarden. De periode van maximaal vijf jaar is gekozen omdat aan de ene kant technologie en cyberdreigingen voortdurend in beweging zijn, en aan de andere kant certificeringsregelingen hanteerbaar moeten zijn voor aanbieders, certificerende instelling en testlaboratoria en dus niet kort cyclisch kunnen veranderen. In de certificeringsregelingen zullen de eisen daarom zo zijn gesteld dat bij de toetsing en gedurende de levenscyclus van producten, diensten en processen er rekening gehouden moet worden met de actuele cyberdreigingen en kwetsbaarheden.
De periodieke inhoudelijke evaluatie van de Europese cyberbeveiligingscertificeringsregelingen heeft een andere focus dan de beoordeling van de Europese Commissie voor eind 2023 of er verplichtingen ten aanzien van certificering noodzakelijk zijn. Overigens zullen in de meeste gevallen eventuele verplichtingen tot certificering of gebruik van gecertificeerde producten, diensten en processen worden opgenomen in andere Europese regelgeving (bijvoorbeeld in het voorstel van de herziening van de NIB-richtlijn).
De regering ziet op dit moment nog geen aanleiding om de evaluatietermijnen samen te brengen.

De leden van de VVD-fractie constateren tevens dat reeds bestaande nationale certificeringsregelingen voor ICT-producten, -diensten en –processen zal komen te vervallen en zal worden vervangen door Europese cyberbeveiligingscertificeringsregelingen. In hoeverre brengen de Europese regelingen een aanscherping aan op de nationale regeling?
Het is op voorhand niet te zeggen of Europese cyberbeveiligingscertificeringsregelingen die nog moeten worden ontwikkeld een aanscherping zullen betekenen van nationale regelingen. Voor zover bekend is de enige nationale regeling die zal komen te vervallen het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB). Dit internationaal multilaterale schema wordt voor de EU ondergebracht in het stelsel van de cyberbeveiligingsverordening. De eerste Europese cyberbeveiligingscertificeringsregeling voor ICT-beveiligingsproducten (EUCC) die dit jaar

wordt verwacht, kent een beperkt aantal verschillen en aanscherpingen voor de partijen die de conformiteitsbeoordeling uitvoeren en laat het lage zekerheidsniveau buiten beschouwing. Dit verschilt met het huidige NSCIB dat is opgesteld naar de internationale SOG-IS criteria (waar een aantal EU landen waaronder Nederland aan deelneemt).

De leden van de CDA-fractie lezen in de memorie van toelichting dat nationale cyberbeveiligingscertificeringsregelingen die hetzelfde onderwerp regelen als een Europese cyberbeveiligingscertificeringsregelingen vanaf een bij de certificeringsregeling vastgestelde datum zullen vervallen. Begrijpen deze leden correct dat op dit moment nog niet kan worden vastgesteld welke nationale cyberbeveiligingscertificeringsregelingen dit zijn?
Voor zover bekend zal door de ontwikkeling van een Europese cyberbeveiligingscertificeringsregeling voor ICT-beveiligingsproducten (EUCC), het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB) komen te vervallen en worden vervangen voor de EUCC.

De leden van de GroenLinks-fractie zijn van mening dat het, om vertrouwen en veiligheid in de digitale economie te borgen, een helder kader voor de certificering van digitale producten, diensten en processen essentieel is. Deze leden juichen dan ook toe dat de cyberbeveiligingsverordening werk maakt van verduidelijking en harmonisatie van dit kader. Zij vragen echter of de huidige opzet, gestoeld op vrijwillige certificering, ver genoeg gaat. Deze leden begrijpen dat een duidelijk kader voor vrijwillige certificering een marktdynamiek in gang kan zetten waarbij steeds meer fabrikanten hun producten vrijwillig laten certificeren. De ervaring leert echter dat er vaak een groep is die zich daar juist aan onttrekt, en wellicht een bewuste keuze maakt voor goedkopere, maar ook onveiligere producten, waar de eindgebruiker, en uiteindelijk de samenleving als geheel, de negatieve gevolgen van dragen. Waarom is er in de verordening niet gekozen voor een meer verplichtend karakter van cyberbeveiligingscertificering? Is de regering bereid om zich hiervoor in te spannen?
De cyberbeveiligingsverordening biedt marktpartijen in eerste instantie de mogelijkheid om op vrijwillige basis te certificeren.
De regering deelt uw beeld dat een duidelijk kader voor vrijwillige certificering een marktdynamiek in gang kan zetten waarbij steeds meer fabrikanten hun producten vrijwillig laten certificeren. Hiermee kunnen aanbieders en fabrikanten zich onderscheiden.
De regering zal daarnaast conform motie Paternotte c.s.[2] blijven pleiten voor verplichte cybersecurity certificering op Europees niveau. In de cyberbeveiligingsverordening is opgenomen dat de Europese Commissie voor eind 2023 aan zal geven of bepaalde Europese cyberbeveiligingscertificeringsregelingen alsnog in de EU verplicht worden via aanvullende wet- en regelgeving.

De leden van de GroenLinks-fractie vragen waarom de regering er met het wetsvoorstel voor heeft gekozen om geen gebruik te maken van de mogelijkheid onder artikel 56 om certificering verplicht te stellen.
De regering is er voorstander van dat op Europees niveau besloten wordt om cyberbeveiligingscertificering te verplichten en niet op nationaal niveau. Hiermee ontstaat meer uniformiteit inzake de cyberbeveiliging, wordt het gelijke speelveld in de digitale interne markt behouden en de concurrentiepositie van Nederlandse bedrijven versterkt.

De leden van de GroenLinks-fractie lezen dat bij de uitwerking van specifieke certificeringsregelingen nader ingegaan zal worden op de wijze waarop voorheen onopgemerkte kwetsbaarheden moeten worden aangepakt, door middel van passende regels inzake updates, hacks of patches. Klopt het dat de wijze waarop dat wordt gedaan niet verder wordt ingevuld en dat het daarmee mogelijk blijft dat een certificeringsregeling slechts lichte vereisten stelt op dit gebied? In hoeverre vormt dat een risico? Waarom zijn de minimumvereisten ten aanzien van de omgang met updates, hacks of patches niet opgenomen in de verordening, en in de uitvoeringswet daarvan, zelf?
De cyberbeveiligingsverordening biedt een kader om Europese cyberbeveiligingscertificeringsregelingen te ontwikkelen voor ICT-producten, ICT-diensten en ICT-processen. De regels omtrent het beschikbaar stellen en uitvoeren van updates en de wijze waarop voorheen onopgemerkte kwetsbaarheden in de cyberbeveiliging, zoals bijvoorbeeld een hack, moeten worden aangepakt zijn inderdaad niet in de cyberbeveiligingsverordening zelf opgenomen maar zullen een onderdeel zijn van iedere Europese cyberbeveiligingscertificeringsregeling (artikel 51, aanhef en onder j, respectievelijk artikel 54, eerste lid, aanhef en onder m, van de

[2] Kamerstuk 21 501-30, nr. 422

cyberbeveiligingsverordening). Omdat deze regels geen deel uitmaken van de cyberbeveiligingsverordening, zijn die niet in het onderhavige wetsvoorstel opgenomen.
De op grond van de cyberbeveiligingsverordening vastgestelde certificeringsregelingen hebben onder meer als doelstelling dat ICT-producten, -diensten en – processen worden geleverd met actuele software en hardware die geen algemeen bekende kwetsbaarheden bevatten, en met mechanismen voor beveiligde updates (artikel 51, aanhef en onder j, van de cyberbeveiligingsverordening).
De passende regels inzake updates, hacks of patches en de gevolgen van de updates, hacks of patches voor het zekerheidsniveau en het afgegeven certificaat zullen dus per afzonderlijke Europese cyberveiligheidscertificeringsregeling moeten worden bepaald. Deze en andere regels kunnen per certificeringsregeling verschillen, aangezien deze betrekking zullen hebben op verschillende categorieën van ICT-producten, -diensten en -processen en zullen sterk verbonden zijn aan het betreffende zekerheidsniveau, zodat er tegemoet wordt gekomen aan de verschillende onderlinge eigenschappen van ICT-producten, -diensten en -processen.
De regering zal bij de uitwerking van specifieke Europese cyberbeveiligingscertificeringsregelingen erop toezien dat de regels inzake updates, hacks of patches voldoende zijn.

d) Verstrekking van Europese cyberbeveiligingscertificaten en EU-conformiteitsverklaringen
De leden van de D66-fractie horen graag of verwacht wordt dat een evaluatie om de vijf jaar op vastgestelde Europese cyberbeveiligingscertificeringsregeling, door ENISA, voldoende recht doet aan de snel veranderende sector waar de verordening op toeziet. Deze leden horen graag of de regels bij cyberbeveiligingscertificeringsregling omtrent het beschikbaar stellen van updates universeel zullen zijn en welke termijnen momenteel hiertoe overwogen worden.
Op grond van de cyberbeveiligingsverordening worden de Europese cyberbeveiligingscertificeringsregelingen in elk geval om de vijf jaar geëvalueerd. Zoals eerder aangegeven in antwoord op een vraag van de leden van de VVD-fractie, zal deze evaluatie betrekking hebben op de inhoud van de regeling - de cyberbeveiligingsnormen, evaluatiemethoden en accreditatievoorwaarden. De periode van maximaal vijf jaar is gekozen omdat aan de ene kant technologie en cyberdreigingen voortdurend in beweging zijn en, aan de andere kant, certificeringsregelingen hanteerbaar moeten zijn voor aanbieders, certificerende instelling en testlaboratoria en dus niet kort cyclisch kunnen veranderen.
Het is echter ook van belang dat de Europese cyberveiligheidscertificeringsregeling zelf voldoende mogelijkheid biedt om recht te doen aan de snel veranderende sector. In de certificeringsregelingen zullen de eisen daarom zo zijn opgesteld dat bij de toetsing en gedurende de levenscyclus van producten, diensten en processen er rekening gehouden moet worden met de actuele cyberdreigingen en kwetsbaarheden. De bedoelde regels zullen per certificeringsregeling zijn aangepast op de producten, diensten en processen waarvoor de regeling is bedoeld. Er is dan ook per Europese cyberbeveiligingscertificeringsregeling de noodzaak voor maatwerk.

De leden van de CDA-fractie constateren dat de cyberbeveiligingscertificeringsregelingen de basis vormen van de uitgifte van de cyberbeveiligingscertificaten en Europese Unie-conformiteitsverklaringen. Deze uitgifte geschiedt nationaal, door ofwel een conformiteitsbeoordelingsinstantie (zekerheidsniveaus 'basis' en 'substantieel') ofwel de nationale cyberbeveiligingscertificeringsautoriteit (zekerheidsniveau 'hoog'). Kan de regering deze verschillende zekerheidsniveaus met voorbeelden toelichten?
Het aantal eisen en de zwaarte van de eisen in een Europese cyberbeveiligingscertificeringsregeling neemt toe naarmate het zekerheidsniveau stijgt en dit kan eveneens gelden voor de zwaarte van de toetsing in het kader van de certificering.
Zolang de specifieke certificeringsregelingen niet beschikbaar zijn, zijn de verschillen in zekerheidsniveau alleen op een generieke wijze aan te geven.
Een Europees cyberbeveiligingscertificaat of EU-conformiteitsverklaring voor het zekerheidsniveau „basis" biedt de zekerheid dat de ICT-producten, -diensten en -processen waarvoor dat certificaat of die EU-conformiteitsverklaring is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op het niveau dat bedoeld is om de bekende basisrisico's van cyberincidenten en cyberaanvallen tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste een toetsing van technische documenten. Indien een dergelijke toetsing niet geschikt is, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.
Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau „substantieel", biedt de zekerheid dat de ICT-producten, -diensten en -processen waarvoor dat certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om de bekende cyberbeveiligingsrisico's, en het risico op cyberincidenten en cyberaanvallen door actoren met beperkte vaardigheden en middelen, tot een minimum te beperken. De te ondernemen evaluatiewerkzaamheden behelzen ten minste

het volgende: verifiëren dat er geen algemeen bekende kwetsbaarheden zijn, en testen of bij de ICT-producten, -diensten of -processen de benodigde beveiligingsfuncties correct worden toegepast. Indien dergelijke evaluatiewerkzaamheden niet geschikt zijn, worden vervangende gelijkwaardige evaluatiewerkzaamheden ondernomen.
Een Europees cyberbeveiligingscertificaat voor het zekerheidsniveau „hoog" biedt de zekerheid dat de ICT-producten, -diensten en -processen waarvoor dat certificaat is afgegeven, voldoen aan de overeenkomstige beveiligingsvoorschriften, waaronder beveiligingsfuncties, en dat zij geëvalueerd zijn op een niveau dat bedoeld is om het risico van geavanceerde cyberaanvallen door actoren met aanzienlijke vaardigheden en middelen, tot een minimum te beperken.

De leden van de SP-fractie vragen in welke mate lidstaten kiezen voor het laten verstrekken van nationale cyberbeveiligingscertificaten voor zekerheidsniveau hoog door de nationale cyberbeveiligingscertificeringsautoriteit dan wel door een conformiteitsbeoordelingsinstantie. Welke gevolgen heeft het gebruik van verschillende regimes voor de wederzijdse erkenning?
Op dit moment is nog onvoldoende duidelijk in welke mate lidstaten kiezen voor het laten verstrekken van nationale cyberbeveiligingscertificaten voor zekerheidsniveau hoog door de nationale cyberbeveiligingscertificeringsautoriteit dan wel door een conformiteitsbeoordelingsinstantie. Het gebruik van verschillende regimes voor de uitgifte van Europese cyberbeveiligingscertificaten met zekerheidsniveau hoog heeft geen gevolgen voor de wederzijdse erkenning van deze certificaten. Het maakt voor wederzijdse erkenning dus niet uit of een certificaat met zekerheidsniveau hoog wordt afgegeven door een nationale cyberbeveiligingscertificeringsautoriteit dan wel door een conformiteitsbeoordelingsinstantie.

De leden van de GroenLinks-fractie lezen dat de verordening ruimte biedt voor conformiteitszelfbeoordelingen door fabrikanten waar het gaat om ICT-producten, -diensten en –processen met een laag risico. Waarom is deze mogelijkheid geboden, zo vragen deze leden? Erkent de regering dat de gevolgen van een cybersecurity incident rond een product met laag risico alsnog serieus kunnen zijn? Wat zijn de risico's van de mogelijkheid tot zelfbeoordeling, en op welke wijze worden die gemitigeerd?
De regering erkent dat er ook risico's zijn verbonden aan producten met een laag risico. Deze risico's zijn echter meer beperkt en hebben naar verwachting een minder ontwrichtend karakter. Het gaat immers om producten met een geringe complexiteit. Om de risico's bij conformiteitszelfbeoordeling te beperken, is een aantal voorwaarden gesteld aan de conformiteitszelfbeoordeling. De mogelijkheid van conformiteitszelfbeoordeling dient expliciet te zijn bepaald in de desbetreffende Europese cyberbeveiligingscertificeringsregeling en wordt enkel geschikt geacht voor ICT-producten, -diensten en -processen met een geringe complexiteit (eenvoudig ontwerp- en productiemechanismen) die een laag risico voor het openbaar belang opleveren. Voorts dient conformiteitszelfbeoordeling ten aanzien van ICT-producten, -diensten of -processen alleen te worden toegestaan wanneer deze zekerheidsniveau „basis" hebben. Bovendien is het toezichthoudende kader onverkort van toepassing op de EU-conformiteitsverklaringen die zijn afgegeven na de conformiteitszelfbeoordeling.
Bij het opstellen van de cyberbeveiligingsverordening hebben de lidstaten de mogelijkheid voor conformiteitszelfbeoordeling niet willen uitsluiten omwille van de volledigheid en toepasselijkheid van het zekerheidsmodel. Per Europese cyberbeveiligingscertificeringsregeling wordt echter bepaald of een conformiteitzelfbeoordeling afhankelijk van de risico's kan worden toegepast.

e) Conformiteitsbeoordelingsinstanties

De leden van de CDA-fractie lezen in een bijlage bij de cyberbeveiligingsverordening de vereisten waaraan een conformiteitsbeoordelingsinstantie moet voldoen om te worden geaccrediteerd om Europese cyberbeveiligingscertificaten te kunnen verstrekken. Hoeveel van deze instanties zijn er momenteel in Nederland?
Conformiteitsbeoordelingsinstanties kunnen voor een Europese cyberbeveiligingscertificeringsregeling worden geaccrediteerd op het moment dat die regeling beschikbaar is. Dat is op dit moment nog niet het geval. De markt van conformiteitsbeoordelingsinstanties is in beweging met fusies en overnames. Er zijn meer dan twintig conformiteitsbeoordelingsinstanties in Nederland actief. Een deel daarvan is op dit moment al actief op het terrein van cybersecurity, een ander deel mogelijk in de toekomst. De keuze om zich te laten accrediteren is aan de conformiteitsbeoordelingsinstantie zelf en afhankelijk van eigen zakelijke afwegingen.

De leden van de SP-fractie vragen welke belangen conformiteitsbeoordelingsinstanties hebben bij het verstrekken van cyberbeveiligingscertificaten.
De onafhankelijkheid van conformiteitsbeoordelingsinstanties is een kernvoorwaarde van het accreditatiestelsel. Een conformiteitsbeoordelingsinstantie heeft geen belang bij het verstrekken van een certificaat. Het verdienmodel van de conformiteitsbeoordelingsinstantie is gebaseerd op de aanvraag van een certificaat en niet op afgifte. De Raad voor Accreditatie houdt toezicht op de geaccrediteerde conformiteitsbeoordelingsinstanties. De accreditatie ziet toe op onpartijdigheid, competentie en consistente bedrijfsvoering.

f) Fabrikanten/aanbieders
De leden van de CDA-fractie lezen in de memorie van toelichting dat fabrikanten of aanbieders van ICT-producten, -diensten of -processen middels de cyberbeveiligingsverordening worden aangespoord om beveiligingsmaatregelen te nemen. De cyberbeveiligingsverordening gaat in eerste instantie uit van certificering op basis van vrijwilligheid, met een eigen keuze voor bedrijven om ervoor te kiezen hun ICT-producten, -diensten en -processen te laten certificeren. Kan de regering ingaan op de keuze voor vrijwillige in plaats van voor verplichtende certificering? Welke criteria liggen hieraan ten grondslag? Wat wordt gedaan wanneer te weinig bedrijven zich certificeren, en op welk moment?
De cyberbeveiligingsverordening gaat uit van certificering op basis van vrijwilligheid. Zoals eerder vermeld is de regering voorstander van verplichte certificering, dit dient wat betreft de regering afgedwongen te worden via Europese wet- en regelgeving. De regering zal tussentijds fabrikanten en aanbieders stimuleren om hun producten en diensten te laten certificeren.

2. Hoofdlijnen van het wetsvoorstel
De leden van de CDA-fractie vragen op welke datum de cyberbeveiligingsverordening moet zijn geïmplementeerd in nationale wetgeving en of de verwachting is dat zowel Nederland als andere lidstaten deze deadline zullen halen.
Op 27 juni 2019 is de Europese cyberbeveiligingsverordening grotendeels in werking getreden. Een aantal bepalingen dient uiterlijk op 28 juni 2021 geïmplementeerd te zijn. Het onderhavige wetsvoorstel geeft uitvoering aan deze verordening. Gezien de fase waarin het wetsvoorstel zich thans bevindt, zal de implementatiedatum licht worden overschreden. De verwachting is dat het grote merendeel van de lidstaten de deadline niet zal halen.

De leden van de CDA-fractie vragen de regering of zij de overeenkomsten en verschillen met de huidige CE-markering kan schetsen. Deze leden vragen tevens of de regering kan aangeven hoe de cyberbeveiligingscertificering in de Verenigde Staten is georganiseerd. Zijn er parallellen met wat nu in Europa wordt voorgesteld?
De CE-markering is onderdeel van het Europese raamwerk van richtlijnen voor productveiligheid, het zogenaamde Nieuwe wetgevingskader (NWK). De richtlijnen reguleren de productveiligheidseisen voor toegang tot de Europese interne markt, inclusief toezicht. De Radioapparatenrichtlijn is een voorbeeld van een richtlijn uit dit raamwerk. De cyberbeveiligingsverordening staat naast het systeem van de CE-markering en kent een aantal verschillen. De cyberbeveiligingsverordening heeft een bredere scope dan fysieke producten, namelijk ICT-producten, -diensten en -processen en de Europese cyberbeveiligingscertificeringsregelingen kunnen meerdere veiligheidsniveaus bevatten. Daarnaast is de cyberbeveiligingsverordening een vrijwillig systeem van certificering die geen betrekking heeft op markttoegang tot de Europese interne markt. Op basis van de Roadmap Digitaal Veilige Hard- en Software zet Nederland in op zowel cybersecurity certificering van ICT-producten, diensten en processen via de cyberbeveiligingsverordening als op het realiseren van cybersecurity minimumeisen voor *Internet of Things* (IoT)-apparaten via de Europese Radioapparatenrichtlijn[3]. Beide maatregelen kunnen op het gebied van IoT-apparaten complementair aan elkaar worden ingevuld.
De aanpak in de Verenigde Staten (VS) lijkt op die van de Europese Unie, ondanks de constitutionele verschillen, want de verhouding van de Staten in de VS tot het Federale niveau is niet volledig vergelijkbaar met de verhouding tussen de EU en de soevereine lidstaten.
De VS beschikt over een federaal standaardisatie instituut, NIST, dat op ook op het terrein van cybersecurity standaarden uitbrengt. Deze standaarden worden in federale regelgeving opgenomen als richtinggevend voor federale en statelijke -organisaties die zich over de naleving moeten verantwoorden. De private organisaties die onderhevig zijn aan de regelgeving, bijvoorbeeld als

[3] Richtlijn nr. 2014/53/EU van het Europees Parlement en de Raad van 16 april 2014 betreffende de harmonisatie van de wetgevingen van de lidstaten inzake het op de markt aanbieden van radioapparatuur en tot intrekking van Richtlijn 1999/5/EG (PbEU L 153/62)

onderdeel van een vitale infrastructuur in een staat moeten zich over de naleving verantwoorden naar hun 'ministerie'. Bij een dergelijke verantwoording door organisaties worden veelal onafhankelijke private auditbedrijven ingehuurd die aan de hand van de NIST-standaarden een toetsing uitvoeren en daarover een conformiteitsverklaring afgegeven. Het gebruik van het specifieke construct van ISO-certificatie is in de VS niet heel breed verbreidt.

a) Nationale cyberbeveiligingscertificeringsautoriteit

De leden van de VVD-fractie achten het positief dat het Agentschap Telecom (AT) wordt aangewezen als nationale autoriteit van deze cyberbeveiligingsverordening gezien de geruime ervaring op het gebied van toezichthoudende werkzaamheden op het digitale domein. Echter, deze leden willen benadrukken dat het beleggen van deze taken bij de Agentschap Telecom een zekere mate van capaciteit vereist en dat andere, huidige taken niet in het geding mogen komen. Hoeveel fulltime equivalent (FTE) gaat de taak van nationale autoriteit naar uw inschatting vereisen? Beschikt het Agentschap Telecom over deze capaciteit?

De regering zet in op versterking en behoud van een relatief sterke cyberbeveiligingscertificeringsmarkt. De taken voor toezicht en uitvoering van de cyberbeveiligingsverordening zullen groeien met het aantal Europese cyberbeveiligingscertificeringsregelingen dat door de Europese Commissie wordt vastgesteld. AT is als nationale cybersecuritycertificeringsautoriteit vanaf de start betrokken bij de ontwikkeling van Europese cyberbeveiligingscertificeringsregelingen en maakt daarmee tijdig een dynamische inschatting van de benodigde extra kennis en capaciteit en van het moment waarop die capaciteit in huis moet zijn gehaald. De bijbehorende extra financiële middelen voor deze nieuwe taak worden aan AT beschikbaar gesteld en op de ontwikkeling aangepast. De extra taken gaan dus niet ten koste van de bestaande taken van AT.
De voorbereiding op deze taken loopt sinds de tweede helft van 2019. Het jaar 2021 moet worden gezien als de bouwfase. Naast de op te bouwen taken voor certificering en toezicht in het kader van de cyberbeveiligingsverordening is tevens capaciteit vrijgemaakt voor de noodzakelijke betrokkenheid bij de ontwikkelfase van lopende nieuwe Europese cyberbeveiligingscertificeringsregelingen. In de projectbegroting voor 2021 zijn in totaal 7 FTE opgenomen waarvan ongeveer 3FTE inzet van bestaand personeel betreft en 4 FTE al van buiten is aangetrokken of nog wordt aangetrokken. De verwachting is dat het aantal betrokken FTE zal groeien in de aankomende jaren met het aantal Europese cyberbeveiligingscertificeringsregelingen en certificeringen, echter het is op dit moment niet aan te geven in welke mate en tempo.

De leden van de CDA-fractie constateren dat volgens het wetsvoorstel de uitvoering van de taken van de Nationale cyberbeveiligingscertificeringsautoriteit berust bij het Agentschap Telecom. Het AT is in het digitale domein zowel uitvoerder als toezichthouder. Kan de regering de keuze voor het AT als uitvoerder nog eens beargumenteren? Vindt zij dit naast de meest effectieve/efficiënte ook de meeste wenselijke oplossing? Heeft het AT thans voldoende slagkracht om deze extra taken erbij te kunnen nemen? Indien niet, wat heeft het AT nodig om zowel haar nieuwe als bestaande taken optimaal te kunnen doen?

Zoals eerder vermeld in de beantwoording van een vraag van de leden van de CDA-fractie over aanwijzing van een nationale cyberbeveiligingscertificeringsautoriteit heeft de regering ervoor gekozen om de taken van de nationale cyberbeveiligingscertificeringsautoriteit bij Agentschap Telecom onder te brengen wegens de geruime ervaring die organisatie heeft met zowel uitvoerende als, afdoende daarvan gescheiden, toezichthoudende werkzaamheden binnen het digitale domein. Ik verwijs dan ook verder naar de eerdere beantwoording.
De slagkracht van Agentschap Telecom zal voldoende zijn en mee gaan groeien met het aantal Europese cybersecuritycertificeringsregelingen en aantal certificeringen. De organisatie wordt immers specifiek gefinancierd om de taken van nationale cyberbeveiligingscertificeringsautoriteit naar behoren uit te kunnen oefenen.

De leden van de GroenLinks-fractie begrijpen de keuze voor het AT als de Nederlandse uitvoerder van de taken die vallen onder de nationale cyberbeveiligingscertificeringsautoriteit. Wat betekent deze uitbreiding van het takenpakket voor de benodigde capaciteit bij het Agentschap Telecom? Ook vragen deze leden op welke wijze de relevante instanties die onder de minister van Justitie & Veiligheid vallen, zoals het Nationale Cybersecurity Centrum (NCSC), betrokken worden bij de uitvoering van deze taken?

De uitvoering van het takenpakket betekent dat Agentschap Telecom over meer personele en materiele middelen dient te beschikken. Hiermee wordt rekening gehouden in de financiering van de organisatie.
Om haar taken goed uit te kunnen oefenen zal Agentschap Telecom relaties onderhouden met andere relevante overheidsinstanties. De Nationaal Coördinator Terrorismebestrijding en Veiligheid

(NCTV) is bij dit dossier betrokken in het kader van zijn coördinerende rol op gebied van digitale weerbaarheid. AT kan eveneens een beroep doen op het NCSC vanuit diens operationele, adviserende rol op het gebied van cybersecurity. Ook zal er samenwerking plaatsvinden met de Algemene Inlichtingen- en Veiligheidsdienst wegens haar ervaring inzake certificering op het gebied van cyberbeveiliging.

b) Conformiteitsbeoordelingsinstantie en accreditatie

De leden van de CDA-fractie lezen in de memorie van toelichting dat fabrikanten en aanbieders gevestigd in andere lidstaten en derde landen een conformiteitsbeoordeling kunnen laten uitvoeren in Nederland. Geldt dit ook andersom, of zijn er ook (derde) landen waar een conformiteitsbeoordeling voor Nederlandse fabrikanten en aanbieders niet mogelijk is (wederkerigheid)?

Nederlandse fabrikanten en aanbieders kunnen in een andere lidstaat van de EU een conformiteitsbeoordeling laten verrichten. Aanbieders kunnen in derde landen geen Europees cyberbeveiligingscertificaat verkrijgen. De cyberbeveiligingsverordening en de Europese cyberbeveiligingscertificeringsregelingen zijn immers alleen in de EU van toepassing.

De leden van de CDA-fractie constateren dat Nederlandse conformiteitsbeoordelingsinstanties in Nederland geaccrediteerd moeten te zijn. Dienen zij ook uit Nederland afkomstig te zijn, of is het mogelijk dat een buitenlandse organisatie uit bijvoorbeeld China een accreditatie krijgt om in Nederland conformiteitsbeoordelingen te doen?

De regels voor accreditatie zijn wettelijk vastgelegd. De Raad voor Accreditatie heeft deze regels vervat in beleidsregels en op haar website gepubliceerd. Binnen de Europese Unie moet een conformiteitsbeoordelingsinstantie, op basis van verordening EU 765/2008[4], accreditatie aanvragen bij haar nationale accreditatie instantie. Om in Nederland een accreditatie te verkrijgen moet een organisatie een vestiging in Nederland hebben waarbij de eis is dat een substantieel deel van de activiteiten ook door die Nederlandse vestiging worden uitgevoerd.

c) Verstrekking van Europese cyberbeveiligingscertificaten met zekerheidsniveau hoog: het nationale stelsel

De leden van de VVD-fractie lezen in de memorie van toelichting dat deelname van fabrikanten en aanbieders aan de cyberbeveiligingscertificeringsregelingen vooralsnog vrijwillig is. Dit overwegende, hoe beoordeelt de regering deze mate van vrijwilligheid in het licht van de doelmatigheid van deze wet? Hoe beoordeelt de regering vrijwilligheid bij certificering van producten met een hoog zekerheidsniveau? Deelt de regering de mening dat een verplichtend karakter verstandig kan zijn bij certificering van producten met hoge zekerheidsniveaus in verband met de grote maatschappelijke en economische risico's die verbonden zijn aan deze categorie?

De regering deelt de mening dat een verplichte cybersecurity certificering wenselijk is en zal zich conform de motie Paternotte c.s. blijven inzetten voor verplichte cybersecuritycertificering op Europees niveau.[5]. Dit geldt ook voor verplichte certificering voor zekerheidsniveau hoog. Risico's, verplichtingen en zekerheidsniveaus staan inderdaad met elkaar in relatie. In de Europese besluitvorming over certificeringsverplichtingen zullen maatschappelijke en economische aspecten en risico's worden betrokken.

De leden van de CDA-fractie constateren dat de regering met dit wetsvoorstel kiest voor een goedkeuringsmodel, met voorafgaande goedkeuring door de nationale autoriteit, waarbij zowel de markt als de nationale autoriteit actief betrokken zijn bij de conformiteitsbeoordeling. Dit om efficiënt te kunnen inspelen op behoeftes van fabrikanten en leveranciers en wegens hun deskundigheid enerzijds en vanuit kostenoogpunt anderzijds. Zitten hier ook risico's aan, bijvoorbeeld in situaties wanneer de druk op overheidsbudgetten groot is?

De regering voorziet geen dergelijke risico's bij dit model. De inzet vanuit de overheid is vanuit het perspectief van kosten juist zo efficiënt mogelijk voorzien. Door middel van het voorgestelde marktgeoriënteerde nationale stelsel maken bedrijven gebruik van de capaciteit, expertise en schaalbaarheid van marktpartijen voor conformiteitbeoordelingen. De voorgestelde inrichting van het nationale stelsel biedt ook economische kansen voor Nederlandse cybersecurity bedrijven om zich te ontwikkelen als conformiteitsbeoordelingsinstantie onder de verordening. De regering is van mening dat deze inrichting van het nationale stelsel Nederland aantrekkelijker maakt voor bedrijven om hun ICT-producten, -diensten en -processen te laten certificeren in Nederland.

---

[4] Verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EEG) nr. 339/93 (PbEU L 218/30)

[5] Kamerstuk 21 501-30, nr. 422.

De leden van de CDA-fractie constateren dat een certificatietraject voor zekerheidsniveau 'hoog' doorgaans een langdurig en kostbaar traject is, waarbij aanzienlijke investeringen van de opdrachtgevers worden gevraagd. Hierom is gekozen voor een goedkeuringsmodel, met een hoge mate van zekerheid en voorspelbaarheid, bedoeld om onnodige kosten te beperken. Wordt de keuze voor dit model door opdrachtgevers en andere stakeholders gesteund?
Vanuit een aantal fabrikanten, aanbieders, conformiteitsbeoordelingsinstanties en evaluatielaboratoria is positief gereageerd op de keuze voor dit model. Dit kwam naar voren in contact met de overheid, onder andere tijdens het experiment voor de opkomende Europese cyberbeveiligingscertificeringsregeling voor clouddiensten.

De leden van de CDA-fractie lezen in de memorie van toelichting de schets van de goedkeuringsprocedure, die zal worden opgedeeld in meerdere stappen. De conformiteitsbeoordelingsinstantie doet melding bij de nationale autoriteit dat een certificeringstraject wordt gestart, legt het onderzoeksplan ter goedkeuring voor aan de nationale autoriteit, legt het onderzoeksrapport en het bijhorende Europese cyberbeveiligingscertificaat dat de conformiteitsbeoordelingsinstantie voornemens is af te geven ter goedkeuring voor aan de nationale autoriteit en geeft het Europese cyberbeveiligingscertificaat af na goedkeuring door de nationale autoriteit.
De leden van de CDA-fractie vragen of met deze procedure/dit model/deze werkwijze geoefend of ervaring opgedaan is. Indien ja, wat waren de uitkomsten daarvan? Waren alle stakeholders hierbij betrokken?
De optie van het goedkeuringsmodel is op aandringen van Nederland in de cyberbeveiligingsverordening opgenomen. Een van de redenen hiervoor was dat dit goedkeuringsmodel ruimte geeft om de huidige werkwijze onder het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB), waar goede ervaring mee was, voort te zetten, en optimaal gebruik te maken van de kracht, flexibiliteit en schaalbaarheid van de certificeringsmarkt.
De stakeholders worden nu ook betrokken bij de uitwerking van het goedkeuringsmodel bij de specifieke cyberbeveiligingsregelingen. Zo loopt nu ook een experiment (proof of concept) voor de opkomende Europese cyberbeveiligingscertificeringsregeling voor clouddiensten. De resultaten worden binnenkort met Enisa gedeeld.

De leden van de CDA-fractie vragen of de regering kan aangeven wat de (maximale) termijnen/doorlooptijden zijn voor eerdergenoemde stappen, zodat een beeld kan worden gevormd van hoe lang een certificeringstraject kan duren. Verwacht de regering dat een lang en kostbaar certificeringstraject opdrachtgevers kan afschrikken om aan vrijwillige certificering mee te doen, waardoor zowel de verordening als het wetsvoorstel hun doel voorbijschieten?
Aan de conformiteitsbeoordeling zijn reeds bepaalde doorlooptijden en kosten verbonden. Bij de ontwikkeling bij Europese cyberbeveiligingscertificeringsregelingen wordt nadrukkelijk aandacht besteed aan kosteneffectiviteit en uitvoerbaarheid van de regelingen.
Bij de afgifte van een cyberbeveiligingscertificaat met zekerheidsniveau 'hoog' voorziet het wetsvoorstel een rol voor de nationale cyberbeveiligingscertificeringsautoriteit. Het afgeven van formele goedkeuring door de nationale cyberbeveiligingscertificeringautoriteit bij certificaten met zekerheidsniveau hoog, aan het onderzoeksplan en de uitreiking van het certificaat is gebonden aan een wettelijke beslistermijn van acht weken met de mogelijkheid tot eenmalige verlenging tot zes weken.

De leden van de CDA-fractie constateren dat de nationale autoriteit ten behoeve van haar besluitvorming advies kan vragen van andere (overheids-)organisaties, zoals de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Dit advies is echter niet-bindend van aard. Waarom is hiervoor gekozen? Acht de regering het voorstelbaar dat de nationale autoriteit een advies van de AIVD naast haar neerlegt? In welke situaties? Zou dit geen veiligheidsrisico's met zich meebrengen?
Agentschap Telecom kan advies vragen van andere (overheids-)organisaties, zoals de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Dit kunnen ook andere (overheids-) organisaties zijn, zoals bijvoorbeeld het NCSC. Dit advies is niet-bindend van aard. Agentschap Telecom dient als nationale cyberbeveiligingscertificeringsautoriteit een zelfstandige afweging te maken om tot een besluit te komen, rekening houdend met alle relevante informatie. Uiteraard spelen veiligheidsrisico's hierbij een belangrijke rol.

De leden van de CDA-fractie lezen in de memorie van toelichting dat gegevens die de nationale autoriteit in het kader van het goedkeuringsproces en het uitoefenen van een beperkt aantal toezichthoudende taken verkrijgt voor zekerheidsniveau 'hoog' uitgezonderd zijn van de toepassing

van de Wet openbaarheid van bestuur, ter bescherming van de openbare veiligheid en de concurrentiepositie van bedrijven. Dit lijkt deze leden goed en belangrijk.
De leden van de CDA-fractie lezen verder dat de Wet openbaarheid van bestuur wel van toepassing is op de uitoefening van alle overige toezichthoudende taken met betrekking tot cyberbeveiligingscertificaten met zekerheidsniveau 'hoog' (artikelen 58, zevende lid, onderdelen b, c, d, e, f, g en i van de cyberbeveiligingsverordening) op alle toezichthoudende taken inzake cyberbeveiligingscertificaten met zekerheidsniveaus 'basis' en 'substantieel'. Brengt dit nog risico's met zich mee?
De keuze met betrekking tot de beperking van het uitzonderen van de toepassing van de Wet openbaarheid bestuur (Wob) tot cyberbeveiligingscertificaten met zekerheidsniveau niveau 'hoog' is gebaseerd op de grote risico's die ICT-producten, -processen of -diensten die gecertificeerd zijn voor dit zekerheidsniveau met zich kunnen brengen. Gegevens die zijn verkregen in het kader van het goedkeuringsproces en het uitoefenen van toezichthoudende taken kunnen kwetsbare (veiligheids-)informatie bevatten en de openbaarmaking ervan zou aanzienlijke negatieve gevolgen kunnen hebben op het openbare leven.
De regering is van oordeel dat eventuele risico's bij openbaarmaking van informatie omtrent cyberbeveiligingscertificaten met zekerheidsniveaus 'basis' en 'substantieel' voldoende kunnen worden ondervangen met de uitzonderingsgronden uit de Wob. In het kader van transparantie is ervoor gekozen om dergelijke informatie niet van de toepassing van de Wob uit te zonderen. In het geval van een Wob-verzoek zal getoetst worden of de gevraagde informatie openbaar kan worden gemaakt of dat een weigeringsgrond van toepassing is, zoals bijvoorbeeld de weigeringsgrond inzake bedrijfsvertrouwelijke gegevens. Het is, in laatste instantie, aan de rechter om te bepalen of de weigeringsgronden juist zijn toegepast.
De regering erkent dat openbaarmaking van informatie omtrent cyberbeveiligingscertificaten met zekerheidsniveaus 'basis' en 'substantieel' ook risico's met zich meebrengt. Echter de maatschappelijke invloed van die risico's acht de regering beperkter. In het kader van transparantie is ervoor gekozen om dergelijke informatie niet van de toepassing van de Wob uit te zonderen. Daarnaast zal in het geval van een Wob-verzoek uiteraard getoetst worden of de gevraagde informatie openbaar kan worden gemaakt of dat een weigeringsgrond van toepassing is, zoals bijvoorbeeld de weigeringsgrond inzake bedrijfsvertrouwelijke gegevens. Het is, in laatste instantie, aan de rechter om te bepalen of de weigeringsgronden juist zijn toegepast.

De leden van de SP-fractie lezen dat in de Memorie van Toelichting wordt gesteld dat Nederland goede ervaringen heeft met modellen waarbij de markt wordt ingezet. Kan worden toegelicht welke modellen dit zijn?
Een voorbeeld is het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB), waarbij de conformiteitsbeoordeling wordt uitgevoerd door conformiteitsbeoordelingsinstanties, en waarbij de overheid, in de vorm van de NBV, een rol heeft. Deze positieve ervaringen hebben bijgedragen aan de nationale inrichting in dit wetsvoorstel om conformiteitsbeoordeling op het niveau 'hoog' door marktpartijen te laten uitvoeren met betrokkenheid van de nationale cyberbeveiligingscertificeringsautoriteit.

3. Regeldruk
De leden van de VVD-fractie lezen met verbazing dat de extra regeldruk voor bedrijven "iets anders ligt" dan voor burgers. Deze leden behoeven meer toelichting van de regering wanneer het gaat om de extra kosten en uren die hiermee gemoeid zijn voor (kleine) ondernemers. Vanzelfsprekend zijn deze leden zich bewust van de noodzaak om strengere eisen te stellen aan de producten/diensten en processen van vitale aanbieders. Deze leden vragen in hoeverre het wenselijk is dat ondernemers in het midden- en kleinbedrijf te maken krijgen met dezelfde regeldruk als grote vitale aanbieders in het geval van eventuele verplichting. Hoe beoordeelt de regering de proportionaliteit van het voorliggende wetsvoorstel in het licht van de verplichtingen die hiervoor worden aangegaan door kleine ondernemers ten opzichte van de grootte en functie van deze bedrijven? Is de regering bereid om meer inzicht te geven in de eventuele extra regeldruk voor bedrijven en specifiek kleine ondernemers?
De regering benadrukt dat het hier vooralsnog gaat om vrijwillige certificering. In hoeverre het midden- en kleinbedrijf hier gebruik van zal maken voor de ICT-producten, -diensten en -processen die zij aanbieden, is een bedrijfsmatige afweging. Zo geldt dat ook voor de keuze voor certificaten met zekerheidsniveau hoog, substantieel of basis. De regering is zich terdege bewust van het belang om ook het klein en middenbedrijf te stimuleren, en zet zich hier op Europees niveau voor in. Wat betreft een eventuele verplichte certificering geldt dat ook hier indien nodig onderscheid gemaakt zou kunnen worden. De regering zal het belang van regeldruk voor het midden- en kleinbedrijf meewegen wanneer in de EU een eventuele verplichting aan de orde is.

De regering acht het wetsvoorstel proportioneel. Het wetsvoorstel betreft een implementatie van een verordening die rechtstreeks van toepassing is en kent geen tot nauwelijks beoordelingsruimte.

De leden van de CDA-fractie lezen in de memorie van toelichting dat momenteel nog niet duidelijk is hoeveel Europese cyberbeveiligingscertificeringsregelingen er zullen komen, op welke ICT-producten, -processen, of -diensten deze cyberbeveiligingscertificeringsregelingen betrekking zullen hebben, hoe deze regelingen eruit zullen zien en hoeveel er gebruik van zal worden gemaakt. Deze leden merken op dat het ontbreken van deze informatie het lastig maakt om de volledige (regeldruk)effecten van dit wetsvoorstel te overzien. Wanneer denkt de regering dat hierover meer bekend is?
Het is inderdaad complex om op dit moment de volledige (regeldruk) effecten van het wetsvoorstel in te schatten. Het wetsvoorstel geeft namelijk uitvoering aan een Europees certificeringskader dat op een later moment zal nader worden ingevuld door Europese cyberbeveiligingscertificeringsregelingen. De keuze voor een Europese cyberbeveiligingscertificeringsregeling wordt op Europees niveau gemaakt en de regelingen worden op Europees niveau vastgesteld en bepaald, en zijn vooralsnog vrijwillig.
Op het moment wordt gewerkt aan de eerste certificeringsregelingen, zoals de Europese cyberbeveiligingscertificeringsregeling voor ICT-beveiligingsproducten (EUCC). Naar verwachting wordt deze regeling in de tweede helft van dit jaar vastgesteld. Vervolgens zal in de loop van volgend jaar de cyberbeveiligingscertificeringsregeling inzake clouddiensten vastgelegd worden. Wanneer een Europese cyberbeveiligingscertificeringsregeling is vastgesteld, kan inzicht gegeven worden in de daaruit voortvloeiende regeldruk en kosten.

De leden van de ChristenUnie-fractie vragen wat de nog te verwachten Europese cyberbeveiligingscertificeringsregelingen voor invloed zullen hebben op de regeldruk en kosten voor bedrijven die ICT-producten, -diensten en –processen laten certificeren. Is er een mogelijkheid voor toezicht op of evaluatie van de regeldruk en kosten die de nog te verwachten Europese cyberbeveiligingscertificeringsregelingen mogelijk met zich meebrengen? Is hier bijvoorbeeld een rol voor de nationale cyberbeveiligingscertificeringsautoriteit weggelegd?
Iedere Europese cyberbeveiligingscertificeringsregeling zal verschillende gevolgen hebben voor regeldruk en kosten. De Europese cyberbeveiligingscertificeringsregelingen bevatten immers bepalingen die verplichtingen opleggen en welke effect kunnen hebben op kosten. Van belang is ook dat het vooralsnog gaat om vrijwillige certificering.
Bij de totstandkoming van een nieuwe Europese cyberbeveiligingscertificeringsregeling wordt nadrukkelijk aandacht besteed aan onder andere de regeldruk en kosten.

a) Aanbieders
De leden van de CDA-fractie lezen in de memorie van toelichting dat er een opwaartse ontwikkeling zichtbaar is van het aantal certificeringen dat in Nederland wordt uitgevoerd. Kan de regering dit kwantificeren?
Het aantal certificeringen voor het Nederlandse Schema voor Certificatie op het gebied van IT-Beveiliging (NSCIB) is al een aantal jaren aan het groeien. In 2020 is het aantal nieuwe certificaten gegroeid van 30 in voorgaande jaren naar 54 certificaten. In de eerste prognose voor 2021 lijkt dit te stabiliseren maar betrokken marktpartijen houden rekening met verdere groei, ook onder de Europese certificeringsregeling voor ICT-beveiligingsproducten (EUCC) die het Nederlandse schema gaat vervangen.
Voor andere toekomstige Europese cyberbeveiligingscertificeringsregelingen is een dergelijke kwantificering niet mogelijk omdat er geen huidige praktijk bestaat.

De leden van de CDA-fractie constateren dat de kosten per certificering sterk kunnen verschillen en zijn afhankelijk van de eisen die een cyberbeveiligingscertificeringsregeling bevat per zekerheidsniveau, de complexiteit van een product, dienst of het proces dat wordt gecertificeerd, de aard van het product, dienst of proces dat moet worden gecertificeerd en de geldigheidsduur van een certificaat. Deze leden vragen of de ontwikkeling van deze kosten zal worden gemonitord.
Het is inderdaad niet mogelijk om op dit moment in generieke zin over de kostenontwikkeling van een Europees cyberbeveiligingscertificaat te spreken en die te monitoren. Uiteraard wordt bij de ontwikkeling van Europese cyberbeveiligingscertificeringsregelingen het aspect van kosteneffectiviteit steeds opnieuw vanaf de start van de ontwikkeling meegenomen. Immers de omvang en zwaarte van de certificeringseisen zijn uiteindelijk de bepalende aspecten voor de kosten van een certificering.

b) Conformiteitsbeoordelingsinstanties

De leden van de CDA-fractie lezen in de memorie van toelichting dat de totale extra last voor een conformiteitsbeoordelingsinstantie wordt dan bij certificeringen op zekerheidsniveau 'hoog' op 270 euro worden geschat. Het is een keuze van de conformiteitsbeoordelingsinstantie om deze kosten aan de aanbieder door te berekenen. Is de verwachting dat veel conformiteitsbeoordelingsinstanties dit zullen doen?
Conformiteitbeoordeling is een hoog arbeidsintensieve activiteit met beperkte marges. Het is daarom te verwachten dat conformiteitsbeoordelingsinstanties in principe alle kosten doorberekenen aan hun klanten. Het is echter aan de conformiteitsbeoordelingsinstanties om de prijs van hun diensten te bepalen.

4. Advies en consultatie

a) Internetconsultatie

De leden van de D66-fractie horen graag een nadere toelichting waarom er niet voor gekozen wordt om de omgang met updates of hacks vast te leggen in het wetsvoorstel, zoals voorgesteld wordt door zowel de Afdeling advisering van de Raad van State als verschillende inbrengen geleverd bij de internetconsultatie. Waarom zou het wenselijker zijn om dit middels en ministeriële regeling vast te leggen?
Zoals eerder aangegeven in antwoord op een vraag van de leden van de GroenLinks-fractie biedt de cyberbeveiligingsverordening een kader om Europese cyberbeveiligingscertificeringsregelingen te ontwikkelen voor ICT-producten, ICT-diensten en ICT-processen. De regels omtrent het beschikbaar stellen en uitvoeren van updates en de wijze waarop voorheen onopgemerkte kwetsbaarheden in de cyberbeveiliging, zoals bijvoorbeeld een hack, moeten worden aangepakt zijn inderdaad niet in de cyberbeveiligingsverordening zelf opgenomen maar zullen een onderdeel van iedere Europese cyberbeveiligingscertificeringsregeling zijn (artikel 51, aanhef en onder j, respectievelijk artikel 54, eerste lid, aanhef en onder m, van de cyberbeveiligingsverordening). Omdat deze regels geen deel uitmaken van de cyberbeveiligingsverordening, zijn die niet in het wetsvoorstel opgenomen.
Aan de Europese cyberbeveiligingscertificeringsregelingen kan uitvoering worden gegeven middels een ministeriele regeling. Artikel 7 van het wetsvoorstel voorziet in een delegatiegrondslag voor regels ter uitvoering van deze uitvoeringshandelingen indien en voor zover dat nodig is voor een goede uitvoering van de cyberbeveiligingsverordening of een Europese cyberbeveiligingscertificeringsregeling.

De leden van de CDA-fractie merken op dat twee organisaties in hun advies hebben gesteld dat de beslistermijnen van de goedkeuringsprocedure tot onnodige vertraging zullen leiden, met een mogelijk negatieve marktwerking in Nederland tot gevolg. De Algemene wet bestuursrecht (Awb) stelt dat een besluit binnen een redelijke termijn van maximaal acht weken genomen dient te worden. Het uitganspunt van de regering is dat de besluitvormingsprocessen binnen de autoriteit niet tot onnodige vertraging zullen gaan leiden en waar mogelijk gewerkt zal worden met standaardprocedures. Worden de doorlooptijden gemonitord?
Agentschap Telecom gaat de doorlooptijden inderdaad monitoren.

b) Advies van het Adviescollege Toetsing Regeldruk

De leden van de CDA-fractie merken op dat het Adviescollege Toetsing Regeldruk (ATR) adviseert om aan de hand van scenario's een indicatie van de totale regeldrukgevolgen in kaart te brengen van verplichte certificering van ICT-producten, -diensten en -processen. Dit is nu niet mogelijk, omdat veel relevante informatie nog niet bekend is. Is de regering voornemens in een later stadium alsnog het advies van het ATR op te volgen?
Wanneer middels Europese wetgeving wordt overgegaan tot verplichte certificering, zal de regering, overeenkomstig de gebruikelijke procedures, de regeldruk in kaart brengen en voorleggen aan het ATR.

c) Uitvoering- en handhaafbaarheidstoets van Agentschap Telecom

De leden van de CDA-fractie merken op dat het AT adviseert om in het wetsvoorstel een grondslag op te nemen voor verplichte certificering op nationaal niveau, op grond waarvan het agentschap adequaat kan ingrijpen op 'zich in de praktijk snel en onverwacht manifesterende cyberrisico's'. De regering neemt dit advies niet over, omdat het voorstander is van certificering op Europees niveau. Hoe denkt de regering op andere wijze aan de zorgen van het AT tegemoet te kunnen komen, daar het AT zelf schrijft dat 'de bestaande bevoegdheden van het agentschap ontoereikend zijn om bij bepaalde risico's te kunnen ingrijpen'?
AT adviseert om een grondslag op te nemen waarin certificering op nationaal niveau kan worden verplicht. Dit voorstel heeft de regering niet overgenomen. Ten aanzien hiervan dient opgemerkt te worden dat de regering inzet op verplichte certificering op Europees niveau. Hiermee ontstaat meer

uniformiteit inzake de cyberbeveiliging, wordt het gelijke speelveld in de digitale interne markt behouden en de concurrentiepositie van Nederlandse bedrijven versterkt. Van belang is dat Nederland en Europa een integrale aanpak hebben om de digitale veiligheid te vergroten en bepaalde cyberbeveiligingsrisico's te verminderen. Standaarden en certificering leveren daar een belangrijke bijdrage aan, maar daarnaast wordt er bijvoorbeeld ook op Europees niveau diverse wet- en regelgeving ontwikkeld die betrekking heeft op de cyberbeveiliging van ICT-producten, diensten en processen, zoals cybersecurityeisen voor IoT-apparaten onder de Radioapparatenrichtlijn.
In afwachting van de verplichte Europese cyberbeveiligingscertificeringsregelingen zal het kabinet de markt stimuleren om gebruik te maken van de nieuwe Europese cybercertificeringsregelingen.

De leden van de ChristenUnie-fractie lezen in de memorie van toelichting dat wanneer een cyberbeveiligingscertificaat niet voldoet aan de Europese voorschriften, de cyberbeveiligingscertificeringsautoriteit kan ingrijpen. Als een ICT-product, -dienst of –proces niet voldoet aan de cyberbeveiligingsverordening kan echter niet worden ingegrepen door de nationale cyberbeveiligingscertificeringsautoriteit. Betekent dit dat wanneer een ICT-product, -dienst of –proces zonder certificaat wordt gebruikt er geen toezicht is op correcte cyberbeveiliging van het product, de dienst of het proces? Deze leden vragen bij wie de verantwoordelijkheid ligt van correcte cyberbeveiligingscertificering van ICT-producten, -diensten of –processen en eventuele gevolgen van incorrecte certificering voor de cyberbeveiliging.
Certificering onder de cyberbeveiligingsverordening is vrijwillig wat kan betekenen dat ook ongecertificeerde ICT-producten, diensten en processen kunnen worden gebruikt door afnemers. In het kader van de Europese cyberbeveiligingscertificeringsregelingen wordt alleen toezicht gehouden op de naleving van de eisen die de cybercertificeringsregeling stelt en dus betreft dit alleen gecertificeerde producten en diensten.
De keuze voor het gebruik van gecertificeerde producten en diensten is aan de afnemers van een ICT-product, dienst of proces tenzij andere wet- en regelgeving een dergelijke keuze voorschrijft.
De cyberbeveiligingsverordening biedt een kader om Europese cyberbeveiligingscertificeringsregelingen te ontwikkelen voor ICT-producten, ICT-diensten en ICT-processen. De regels omtrent het toezicht en de gevolgen van niet-conformiteit zullen een onderdeel van iedere certificeringsregeling zijn. Het is derhalve op dit moment nog niet bekend welke gevolgen zullen intreden indien een ICT-product, -dienst of –proces niet meer aan een Europese cyberbeveiligingscertificeringsregeling voldoet.
De verantwoordelijkheid van correcte cyberbeveiligingscertificering ligt in eerste instantie bij het desbetreffende bedrijf die zijn ICT-product, diensten of proces certificeert of laat certificeren en bij de conformiteitsbeoordelingsinstanties die zijn geaccrediteerd om certificering op grond van Europese cyberbeveiligingscertificeringsregelingen te mogen uitvoeren. Eventuele gevolgen van incorrecte certificering zal daarom naast bij het desbetreffende bedrijf en bij conformiteitsbeoordelingsinstanties liggen.
De nationale cyberbeveiligingscertificeringsautoriteit houdt toezicht op de afgegeven certificaten.