36764 Regels ter implementatie van Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (*PbEU* 2022, L 333) (Cyberbeveiligingswet)

NOTA NAAR AANLEIDING VAN HET VERSLAG

Met belangstelling heb ik kennisgenomen van het verslag van de vaste commissie voor Digitale Zaken op het wetsvoorstel Cyberbeveiligingswet (hierna: Cbw). Dit wetsvoorstel strekt tot de uitvoering van de Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (hierna: NIS2-richtlijn).[1] Ik dank de commissie voor het binnen een korte periode uitbrengen van het verslag en dank de leden van de fracties voor de gestelde vragen, die ik in deze nota beantwoord. De vragen en opmerkingen uit het verslag zijn integraal opgenomen in cursieve tekst en de beantwoording daarvan in gewone typografie. Ik hoop de vragen genoegzaam te hebben beantwoord en hoop op een spoedige voortzetting van de behandeling van dit wetsvoorstel. Tot slot merk ik op dat ik tevens een nota van wijziging aanbied.

I. ALGEMEEN DEEL

1. Inleiding

De leden van de GroenLinks-PvdA-fractie hebben kennisgenomen van de Cyberbeveiligingswet (Cbw). Over de wet en alle aanhangige stukken hebben deze leden vragen en opmerkingen.

De leden van de VVD-fractie hebben met belangstelling kennisgenomen van de Cyberbeveiligingswet. Deze leden delen het doel van het wetsvoorstel om een hoog gemeenschappelijk niveau van cyberbeveiliging in de EU te bereiken, teneinde de werking van de interne markt te verbeteren. Zij stellen nog enkele vragen.

De leden van de NSC-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel ter implementatie van de Europese NIS2-richtlijn via de Cyberbeveiligingswet. Deze leden onderschrijven het belang van versterkte digitale weerbaarheid, vooral voor vitale processen en essentiële diensten. Zij merken op dat digitalisering diep doordringt in alle sectoren van de samenleving en daarmee de afhankelijkheid van goed functionerende en veilige digitale systemen vergroot. Daarom achten deze leden het van groot belang dat het wetgevend kader helder en werkbaar is. Tegelijkertijd constateren zij dat het wetsvoorstel op een aantal punten nadere toelichting of verduidelijking behoeft. Zij hebben in dat kader de volgende vragen en opmerkingen De leden van de voornoemde fractie wijzen op de recente datadiefstal bij laboratorium Clinical Diagnostics in Rijswijk. Dit onderstreept opnieuw de kwetsbaarheid van onze digitale infrastructuur. Deze gevoelige informatie omvat onder andere persoonsgegevens die gedeeld zijn met het laboratorium, wat voor de betrokkenen niet alleen een ernstige inbreuk op de privacy betekent, maar ook verhoogde risico's op phishing en identiteitsfraude met zich meebrengt. Dit incident werpt een urgent licht op de noodzaak van strengere en effectievere wetgeving op het gebied van cyberbeveiliging. De Cyberbeveiligingswet roept in dit kader belangrijke vragen op over de reikwijdte, handhaving en effectiviteit ervan, zeker wanneer gevoelige medische gegevens op zo'n grote schaal kunnen lekken. De leden van deze fractie vragen in hoeverre de huidige Cyberbeveiligingswet voldoende bescherming biedt tegen datalekken binnen organisaties die gevoelige medische gegevens verwerken. Vallen die altijd binnen deze wet?

Specifiek in verband met de risico's met betrekking tot de verwerking van persoonsgegevens, zoals het verlies van of de ongeoorloofde toegang tot die gegevens, geldt krachtens de Algemene verordening gegevensbescherming (hierna: Avg) reeds de verplichting voor elke verwerkingsverantwoordelijke om passende technische en organisatorische beveiligingsmaatregelen te treffen. In geval zich toch een datalek voordoet bevat de Avg ook de verplichting voor de verwerkingsverantwoordelijke om hiervan melding te doen. Op de naleving van deze verplichtingen wordt toezicht gehouden door de Autoriteit persoonsgegevens (hierna: AP).

[1] *PbEU* 2022, L 333.

Met de Cbw komt daarnaast ten aanzien van de entiteiten waarop die wet van toepassing zal zijn, met het oog op het waarborgen van de continuïteit van hun essentiële of belangrijke dienstverlening, onder meer te gelden dat zij verplicht zijn om passende en evenredige technische, operationele en organisatorische maatregelen te nemen. Die maatregelen moeten zij nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor hun dienstverlening of werkzaamheden gebruiken, te beheersen. Ook moeten zij die maatregelen nemen om incidenten, waarbij bijvoorbeeld de beschikbaarheid of vertrouwelijkheid van de genoemde systemen of van de daarin verwerkte gegevens in gevaar komt, te voorkomen en om de gevolgen daarvan te beperken. Ook geldt voor hen krachtens de Cbw de verplichting om significante incidenten, indien die zich toch voordoen, te melden bij hun bevoegde autoriteit en hun *Computer security incident response team* (hierna: CSIRT), zodat op basis daarvan onder meer door het CSIRT bijstand kan worden verleend bij het treffen van maatregelen om de continuïteit van hun dienstverlening te herstellen. Bij dergelijke incidenten kan het ook gaan om incidenten waarbij persoonsgegevens in het geding zijn, maar daarvan hoeft niet noodzakelijkerwijs sprake te zijn. De Cbw regelt ook dat op de naleving van deze verplichtingen toezicht wordt gehouden.

De hiervoor genoemde verplichtingen uit de Cbw zijn onder meer van toepassing op de in bijlage 1 van de Cbw genoemde soorten entiteiten in de sector gezondheidszorg, waaronder zorgaanbieders, EU-referentielaboratoria en entiteiten die farmaceutische basisproducten en farmaceutische bereidingen vervaardigen. Daarmee zal derhalve het verkleinen van het risico op datalekken binnen dergelijke entiteiten worden bevorderd.

De leden van de D66-fractie hebben met interesse kennisgenomen van de Cyberbeveiligingswet. Deze leden onderschrijven het belang van een hoog niveau van digitale weerbaarheid en de implementatie van de NIS2-richtlijn. Zij constateren wel dat hier sprake is van een grote stelselherziening met een omvangrijke uitbreiding van reikwijdte en verplichtingen. Daar hebben deze leden enkele vragen over.

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

De leden van de SP-fractie hebben de Cyberbeveiligingswet gelezen en hebben hier nog enkele vragen over. Kan de regering allereerst meer ingaan op het advies van de Raad van State voor zover het gaat over de taakverdeling tussen de vakministers en de zelfstandige bestuursorganen (zbo's)?

In haar advies op dit wetsvoorstel heeft de Afdeling advisering van de Raad van State aandacht voor de bevoegdheden van en taakuitoefening door de vakministers op grond van de Cbw en de bevoegdheden van en taakuitoefening door zelfstandige bestuursorganen op grond van andere wetgeving ten aanzien van dezelfde entiteiten. Hierover heeft de Afdeling geadviseerd om in kaart te brengen welke zelfstandige bestuursorganen belast zijn met toezichts- en handhavingstaken gericht op veiligheid, en om aan te geven hoe voorkomen wordt dat de uitoefening van deze taken in de praktijk tot problemen leidt, doordat dit overlapt met taken die zijn toebedeeld via de Cbw. De regering reflecteert hierop als volgt.

In artikel 15, eerste tot en met vijfde lid, Cbw zijn de vakministers aangewezen als de bevoegde autoriteit voor de entiteiten die onder het toepassingsbereik van de Cbw vallen. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw.[2] De vakministers wijzen bij besluit de ambtenaren aan die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[3] Daarbij zal het gaan om de aanwijzing van ambtenaren van onder meer de rijksinspecties Inspectie Leefomgeving en Transport (hierna: ILT), Rijksinspectie Digitale Infrastructuur (hierna: RDI), Inspectie van het Onderwijs, Inspectie Gezondheidszorg en Jeugd (hierna: IGJ) en Nederlandse Voedsel- en Warenautoriteit (hierna: NVWA). Voor wat betreft het zelfstandig

[2] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 15, zesde lid, onderdeel b, Cbw.

[3] Artikel 5:11 Awb spreekt in deze context over "toezichthouder".

bestuursorgaan Autoriteit Nucleaire Veiligheid en Stralingsbescherming (hierna: ANVS) geldt dat de Minister van Infrastructuur en Waterstaat het voornemen heeft om de toezichts- en handhavingstaken uit de Cbw aan de ANVS te mandateren. In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister).

Een entiteit kan onder meerdere wettelijke kaders vallen, zoals de Cbw en andere wetgeving, en daardoor te maken hebben met verplichtingen voortvloeiend uit verschillende wettelijke kaders en toezichthoudende ambtenaren van meerdere instanties. De regering kiest ervoor om het toezicht in het kader van de Cbw naast het toezicht van zelfstandige bestuursorganen op grond van hun wettelijk kader te laten bestaan en acht het niet mogelijk om *a priori* met een exclusieve taakafbakening te werken waarin overlap in dat toezicht niet bestaat. Dit maakt het van belang, zoals ook is aangegeven in het nader rapport, dat afstemming plaatsvindt tussen (de ambtenaren van) de hiervoor bedoelde verschillende instanties en dat samenwerkingsafspraken worden gemaakt om de doeltreffendheid en doelmatigheid van toezicht te waarborgen. Zoals ook in het nader rapport is aangegeven denkt de regering hierbij onder meer aan afspraken over samenloop van toezicht op eenzelfde entiteit, het voorkomen van onevenredige toezichtslasten en uitwisseling van gegevens. De regering acht het van belang dat in de samenwerkingsafspraken voor ogen wordt gehouden dat verschillende wetten in het veiligheidsdomein verschillende aspecten van veiligheid regelen, geredeneerd vanuit wettelijk verschillende gedefinieerde belangen. De ambtenaren van de hiervoor bedoelde verschillende instanties zullen derhalve elk op basis van hun eigen wettelijke grondslag hun taken uitvoeren en overlap in bevoegdheden doet geen afbreuk aan hun bevoegdheden en verantwoordelijkheden en die van het voor het toezicht verantwoordelijke bestuursorgaan.

En kan de regering iets zeggen over de Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)? Eerder is er bewust voor gekozen om al het toezicht bij de ANVS te leggen, maar nu krijgt de minister van Infrastructuur en Waterstaat (I&W) ook een deel van dat toezicht.

De Cbw introduceert nieuwe verplichtingen op het gebied van cyberbeveiliging voor essentiële entiteiten en belangrijke entiteiten die gebruik maken van netwerk- en informatiesystemen. De nucleaire sector komt onder de Wet weerbaarheid kritieke entiteiten (hierna: Wwke) en daarmee ook onder de Cbw te vallen, en komt daarmee ook onder het toezicht van de Minister van Infrastructuur en Waterstaat te vallen. In de Kernenergiewet zijn echter toezichts- en handhavingsbevoegdheden uitdrukkelijk toegekend aan de ANVS. Omdat de ANVS op grond van de Kernenergiewet al toezicht houdt op informatie- en cyberbeveiliging, heeft de Minister van Infrastructuur en Waterstaat het voornemen om de toezichts- en handhavingstaken uit de Cbw aan de ANVS te mandateren.[4]

De ANVS is per 1 augustus 2017 een zelfstandig bestuursorgaan geworden. Daarnaast verkreeg zij nog meer zelfstandigheid dan standaard is geregeld in de Kaderwet zelfstandige bestuursorganen doordat in afwijking van artikel 21, eerste lid, van die wet de Minister van Infrastructuur en Waterstaat geen beleidsregels kan vaststellen met betrekking tot de taakuitoefening door de ANVS.

Het Ministerie van Infrastructuur en Waterstaat en de ANVS zijn in overleg over de wijze waarop de ANVS het mandaat voor de nieuwe taken op een goede wijze kan gaan uitvoeren. De toezichts- en handhavingstaken zullen worden uitgeoefend door ambtenaren van de ANVS die ook het toezicht op de Kernenergiewet uitoefenen.

Met het voorgaande is gewaarborgd dat de Minister van Infrastructuur en Waterstaat de bestuurlijke verantwoordelijkheid en formele bevoegdheden als bevoegde autoriteit behoudt, terwijl de uitvoering van het toezicht en de handhaving in de nucleaire sector bij de ANVS belegd wordt.

Kan de regering aangeven of er nog andere zbo's zijn waar zo'n situatie kan voorkomen?

In artikel 15, eerste tot en met vijfde lid, Cbw zijn de vakministers aangewezen als de bevoegde autoriteit voor de entiteiten die onder het toepassingsbereik van de Cbw vallen. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de

[4] Dit voornemen geldt overigens ook voor de Wwke.

bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw.[5] De vakministers wijzen bij besluit de ambtenaren aan die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[6] Daarbij zal het gaan om de aanwijzing van ambtenaren van onder meer de rijksinspecties ILT, RDI, Inspectie van het Onderwijs, IGJ en NVWA. Voor wat betreft het zelfstandig bestuursorgaan ANVS geldt dat de Minister van Infrastructuur en Waterstaat het voornemen heeft om de toezichts- en handhavingstaken uit de Cbw aan de ANVS te mandateren. In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister).

Voor de ambtenaren van de rijksinspecties en de zelfstandige bestuursorganen geldt dat overlap kan bestaan in het toezicht in het kader van de Cbw en andere wetgeving. Bij de sectoren waar dat van toepassing is, vindt afstemming tussen (de ambtenaren van) die instanties plaats en worden samenwerkingsafspraken gemaakt. Doel is om zoveel mogelijk te voorkomen dat ambtenaren van verschillende instanties overlappende toezichtsactiviteiten uitvoeren bij dezelfde entiteiten, wat een hogere administratieve last geeft. In het specifieke voorbeeld van de ANVS, zal de ANVS moeten samenwerken met in elk geval de RDI om te komen tot effectief toezicht vanuit de Cbw.

De leden van de SP-fractie vragen tevens waarom de Autoriteit Persoonsgegevens (AP) tot op heden nog geen middelen heeft ontvangen om haar taak (samen met andere toezichthouders toezicht houden op de Cyberbeveiligingswet) uit te voeren. Daarbij houdt de AP toezicht op alle organisaties en sectoren en kan zij de samenwerking tussen de verschillende toezichthouders bevorderen. De AP geeft aan structureel circa twee miljoen euro nodig te hebben. Is de regering bereid de AP alsnog van deze middelen te voorzien?

De regering merkt allereerst op dat de AP geen toezicht zal houden op de naleving van de verplichtingen uit de Cbw. Met het toezicht op de naleving van die verplichtingen zijn namelijk de bevoegde autoriteiten, aangewezen in artikel 15 Cbw, belast. Deze bevoegde autoriteiten werken op grond van artikel 58, eerste lid, Cbw samen met de AP (die immers wel toezichthoudende autoriteit met betrekking tot de naleving van de Avg is) bij de behandeling van incidenten bij essentiële entiteiten en belangrijke entiteiten, die leiden tot inbreuken in verband met persoonsgegevens. In het kader van die samenwerking worden alle daarvoor noodzakelijke gegevens uitgewisseld. Daarnaast regelt artikel 58, tweede lid, Cbw dat wanneer de bevoegde autoriteit, bedoeld in de Cbw, bij toezicht of handhaving er kennis van krijgt dat een overtreding van de zorgplicht of de meldplicht uit de Cbw door een essentiële entiteit of belangrijke entiteit een inbreuk in verband met persoonsgegevens kan inhouden, die op grond van artikel 33 Avg moet worden gemeld, de bevoegde autoriteit de AP daarvan onverwijld in kennis stelt. Het behandelen van dergelijke meldingen van inbreuken in verband met persoonsgegevens behoort ook tot de reeds bestaande taken van de AP. De AP krijgt met de Cbw geen nieuwe wettelijke taken onder de Cbw en de regering ziet daarom geen noodzaak om de AP van extra middelen te voorzien vanwege de komst van de Cbw.

Daarnaast heeft de toenmalige Staatssecretaris Rechtsbescherming in zijn reactie op een evaluatie van de AP aangegeven dat hij samen met de AP stappen wil zetten om te komen tot een meer objectieve basis die ondersteunend is bij de besluitvorming over een passende hoogte van het budget van de AP. Daarbij heeft hij afgesproken dat de AP in de nabije toekomst, in samenspraak met het Ministerie van Justitie en Veiligheid, een meetinstrument en indicatoren ontwikkelt om inzicht te krijgen in het doelmatig en doeltreffend functioneren van de AP en om op een transparante wijze te verantwoorden dat middelen doelmatig en doeltreffend worden besteed. Belangrijk onderdeel van het creëren van een objectieve basis zal een vergelijking met Avg-toezichthouders in andere lidstaten van de Europese Unie zijn. Dit alles vergt de komende tijd aandacht en zal afhangen van politieke keuzes die gemaakt zullen worden.

---

[5] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 15, zesde lid, onderdeel b, Cbw.

[6] Artikel 5:11 Awb spreekt in deze context over “toezichthouder”.

De leden van de ChristenUnie-fractie hebben met interesse kennisgenomen van onderhavig wetsvoorstel. Deze leden merken op dat de Afdeling advisering van de Raad van State adviseert om nader in te gaan op de wijze waarop invulling wordt gegeven aan de coördinerende taak van de minister van Justitie en Veiligheid (J&V). Uit het nader rapport blijkt niet of de memorie van toelichting is aangevuld op dit punt. Ook wordt niet ingegaan op welke zbo's belast zijn met toezichts- en handhavingstaken, ondanks het advies van de Raad van State hierover. Kan de regering alsnog uitgebreider op beide zaken ingaan?

Naar aanleiding van deze inbreng van de leden van de ChristenUnie-fractie constateert de regering dat het nader rapport op het advies van de Afdeling advisering van de Raad van State weliswaar nader ingaat op de wijze waarop invulling wordt gegeven aan de coördinerende taak van de Minister van Justitie en Veiligheid, maar dat die uitleg per abuis niet (ook) is opgenomen in de memorie van toelichting op het wetsvoorstel.

In artikel 15, eerste tot en met vijfde lid, Cbw zijn de vakministers aangewezen als de bevoegde autoriteit voor de entiteiten die onder het toepassingsbereik van de Cbw vallen. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw.[7] De vakministers wijzen bij besluit de ambtenaren aan die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[8] Voor wat betreft het zelfstandig bestuursorgaan ANVS geldt dat de Minister van Infrastructuur en Waterstaat het voornemen heeft om de toezichts- en handhavingstaken uit de Cbw aan de ANVS te mandateren. In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister).

2. De NIS2-richtlijn

2.1. Kern van de richtlijn

De leden van de CDA-fractie vragen wat de reden is voor de keuze om uit te gaan van minimumharmonisatie, terwijl een van de problemen van de NIS1-richtlijn was dat er teveel verschillen tussen lidstaten ontstonden. In dat kader vragen deze leden of de regering een compleet overzicht wil delen van alle onderdelen van het wetsvoorstel die verder gaan dan de minimumeisen van de richtlijn.

De regering heeft geen aanleiding gezien om te kiezen voor zwaardere eisen dan de minimumeisen van de NIS2-richtlijn. In dit wetsvoorstel zijn er dan ook geen onderdelen aan te wijzen die verder gaan dan de minimumeisen van de NIS2-richtlijn. Doordat diverse lidstaten van de Europese Unie, waaronder Nederland, de minimumeisen implementeren in nationale wetgeving is sprake van de harmonisatie van een bepaald niveau (een minimum) aan eisen. Voor een aantal soorten entiteiten heeft de Europese Commissie met Uitvoeringsverordening (EU) 2024/2690 in een nog uitgebreidere harmonisatie van de minimumvereisten voorzien.[9]

De leden van de GroenLinks-PvdA-fractie hebben vragen over tekortkomingen van de NIS1-richtlijn. Volgens de regering bestaan er te veel verschillen tussen de implementatie in lidstaten. Kan de regering enkele

---

[7] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 15, zesde lid, onderdeel b, Cbw.

[8] Artikel 5:11 Awb spreekt in deze context over "toezichthouder".

[9] Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (*PbEU* L 2024/2690).

problematische tegenstrijdigheden tussen lidstaten noemen, die de komst van de NIS2-richtlijn rechtvaardigen? Kan de regering ook toelichten in welke mate Nederland de NIS1-richtlijn heeft geïmplementeerd?

De NIS1-richtlijn[10] laat veel discretionaire ruimte over aan de lidstaten van de Europese Unie bij de uitvoering van de richtlijn. Door die ruimte zijn er tussen lidstaten aanzienlijke verschillen ten aanzien van de implementatie van de richtlijn in de lidstaten. Zo zijn er tussen lidstaten aanzienlijke verschillen op het gebied van de afbakening van het toepassingsgebied van de NIS1-richtlijn. Dat verschil betekent concreet dat een aanbieder in de ene lidstaat wel onder de werking van de NIS1-richtlijn valt, terwijl een nagenoeg identieke aanbieder (dezelfde sector, met een soortgelijke dienstverlening, werkzaam in een soortgelijke context) uit een andere lidstaat niet onder de werking van de NIS1-richtlijn valt. Ook bestaan er aanzienlijke verschillen ten aanzien van de uitvoering van de verplichtingen op nationaal niveau, zoals het soort cyberbeveiligingseisen en de mate van gedetailleerdheid, en het toezicht op de naleving van de verplichtingen die uit de richtlijn volgen. Deze verschillen kunnen nadelige effecten hebben op de werking van de interne markt en kunnen sommige lidstaten meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Europese Unie. Met de NIS2-richtlijn is op de hiervoor genoemde onderwerpen een eenduidig beleid gekomen, wat zorgt voor minimumharmonisatie en bijdraagt aan het bereiken van een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie, hetgeen dan ook naar het oordeel van de regering de rechtvaardiging is voor de komst van de NIS2-richtlijn.[11] Het Europese instrument van een minimumharmonisatierichtlijn brengt overigens wel met zich mee dat er bij de implementatie verschillen tussen lidstaten kunnen gaan ontstaan, maar dit zal wel altijd binnen de kaders van de richtlijn zijn.

Nederland heeft in 2018 de NIS1-richtlijn volledig geïmplementeerd in de Wet beveiliging netwerk- en informatiesystemen (hierna: Wbni).

De leden van de GroenLinks-PvdA-fractie merken op dat Nederland de NIS2-richtlijn te laat implementeert in nationale wetgeving. Deze leden vragen de regering om duidelijk te maken of dit gevolgen heeft voor de cyberveiligheid van entiteiten, aangezien Nederland in de tussentijd geen gelijkgestemde wetgeving heeft met andere landen. Kan de regering de trage implementatie en de gevolgen daarvan nader toelichten? Op welke termijn verwacht de regering deze wet wel volledig te hebben ingevoerd?

De NIS2-richtlijn vormt een belangrijke basis voor het cybersecuritystelsel in Nederland en de weerbaarheid van de vitale infrastructuur en is daarom van grote waarde voor het verhogen van de weerbaarheid van Nederland. Of de vertraagde implementatie van de NIS2-richtlijn gevolgen heeft voor de cyberveiligheid van entiteiten die onder het toepassingsbereik van de Cbw zullen vallen en om welke specifieke gevolgen het daarbij gaat, valt niet in zijn algemeenheid te zeggen. Dat zal immers afhankelijk zijn van de aard en omstandigheden per geval, waarbij tevens meespeelt welke cybermaatregelen entiteiten op dit moment al hebben genomen voor hun essentiële of belangrijke dienstverlening. In dit verband merkt de regering op dat de rijksoverheid al gedurende enige tijd de organisaties die onder de Cbw komen te vallen oproept om de komst van de Cbw niet af te wachten, maar om zich al voor te bereiden op de komst van de Cbw. Hierbij is toegelicht dat de risico's die organisaties lopen zich nu al voordoen.[12] Daarnaast hebben verschillende organisaties in verband met de rechtstreekse werking van enkele bepalingen uit de NIS2-richtlijn per 17 oktober 2024 bepaalde rechten, zoals het recht op bijstand en advies van een CSIRT bij cyberincidenten. Hierover is uw Kamer bij brief van 16 oktober 2024 geïnformeerd.[13]

---

[10] 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).

[11] Zie ook het fiche van de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC) over de herziening van de NIS1-richtlijn: *Kamerstukken II* 2020/21, 22112, nr. 3053.

[12] Laatstelijk bij nieuwsbericht van 1 juli 2025: https://www.nctv.nl/actueel/nieuws/2025/06/30/concepten-cyberbeveiligingsbesluit-en-besluit-weerbaarheid-kritieke-entiteiten-gestuurd-naar-tweede-kamer. Zie voorts op deze website toelichting over hoe organisaties zich kunnen voorbereiden: https://www.nctv.nl/onderwerpen/c/cer--en-nis2-richtlijnen/hoe-kan-uw-organisatie-zich-voorbereiden-op-de-cer--en-nis2-richtlijnen.

[13] *Kamerstukken II* 2024/25, 22112, nr. 3968.

De Nederlandse inspanningen zijn er altijd op gericht geweest de omzetting van de NIS2-richtlijn naar nationale wetgeving tijdig en spoedig af te ronden. Het tot stand brengen van de vereiste wetgeving heeft helaas meer tijd gekost, waardoor het niet is gelukt om de implementatie tijdig af te ronden. Dit komt doordat de omzetting naar nationale wetgeving een omvangrijk en complex traject is, waarbij grote zorgvuldigheid is vereist. De Cbw, waarin in Nederland de NIS2-richtlijn wordt geïmplementeerd, zal immers aanzienlijke impact hebben op vele Nederlandse organisaties, zowel in de publieke sector als in de private sector. Er zijn ten opzichte van bestaande wetgeving (meer in het bijzonder de Wbni, waarin de NIS1-richtlijn is geïmplementeerd) meer en nieuwe sectoren en significant meer organisaties die moeten voldoen aan de nieuwe wetgeving. Vanwege de impact op organisaties is uit een oogpunt van zorgvuldige voorbereiding er ook voor gekozen om het wetsvoorstel open te stellen voor internetconsultatie, hoewel dit bij implementatiewetsvoorstellen niet verplicht is. De internetconsultatie heeft waardevolle reacties opgeleverd en heeft onder meer geleid tot aanpassingen van het wetsvoorstel en aanvullingen in de bijbehorende toelichting.

De regering hoopt dat de Cbw in het tweede kwartaal van 2026 in werking treedt.

2.2. Belangrijkste onderdelen van de richtlijn

De leden van de D66-fractie vragen de regering uiteen te zetten welke onderdelen van de huidige nationale wetgeving tekortschoten en waarom de gekozen verzwaringen noodzakelijk zijn, mede in het licht van het advies van het Adviescollege Toetsing Regeldruk (ATR) waarin gesteld wordt dat er geen aanleiding is om te kiezen voor zwaardere eisen dan de minimumeisen van de richtlijn.

De regering heeft geen aanleiding gezien om te kiezen voor zwaardere eisen dan de minimumeisen van de NIS2-richtlijn. Het wetsvoorstel voorziet dan ook niet in regels die verder gaan dan de minimumeisen van de NIS2-richtlijn.

Met betrekking tot de vraag van de leden van de D66-fractie welke onderdelen van de huidige nationale wetgeving tekort schieten, licht de regering het volgende toe. Er is niet zozeer sprake van tekortkomingen in de huidige nationale wetgeving, maar sprake van de implementatie van een richtlijn met veel nieuwe onderwerpen (onderwerpen die nog niet zijn geregeld in nationale wet- en regelgeving), van toepassing op een groot aantal sectoren.

2.3. Verhouding tot de CER-richtlijn en de Wwke

De leden van de GroenLinks-PvdA-fractie erkennen het belang van coherentie tussen de Wet weerbaarheid kritieke entiteiten (Wwke) en de Cyberbeveiligingswet. Echter vragen deze leden of de koppeling tussen de twee wetten strikt noodzakelijk is geweest, of andere lidstaten dezelfde keuze maken, en of dit heeft geleid tot vertraging.

De NIS2-richtlijn (welke wordt geïmplementeerd in de Cbw) en de CER-richtlijn (welke wordt geïmplementeerd in de Wwke) kennen op onderdelen een grote samenhang. Zo bevatten beide richtlijnen een (vergelijkbare) zorgplicht en een meldplicht bij grote incidenten. In het kader van uniform, duidelijk en begrijpelijk beleid en wet- en regelgeving acht de regering het van belang dat deze twee richtlijnen in gezamenlijkheid worden uitgewerkt. Dit wordt ook vanuit de Europese Commissie in hoge mate ondersteund. Zo worden er onder meer gezamenlijke Europese expertbijeenkomsten georganiseerd. In deze bijeenkomsten hebben het merendeel van de lidstaten van de Europese Unie aangegeven een gezamenlijk meldpunt voor NIS2- en CER-meldingen te realiseren en beleid te hebben voor een versterkte coördinatie tussen de NIS2- en CER-autoriteiten.

Op diverse momenten is bezien of het gelijk laten lopen van deze trajecten tot implementatie van de NIS2-richtlijn en de CER-richtlijn nog waardevol was. De conclusie was telkens dat het synchroon laten lopen van beide implementatietrajecten van belang en zinvol is.

De koppeling tussen de twee implementatietrajecten heeft niet geleid tot extra vertraging. Dit kan worden verklaard door de grote overlap op dezelfde thema’s.

De leden van de VVD-fractie begrijpen dat de NIS2-richtlijn regelt dat entiteiten die uit hoofde van de CER-richtlijn worden aangewezen als kritieke entiteit, ook onder het toepassingsbereik van de NIS2-richtlijn vallen en automatisch als essentiële entiteit in de zin van de NIS2-richtlijn kwalificeren. Andersom geldt dat echter niet: een essentiële entiteit kwalificeert niet automatisch als kritieke entiteit, omdat kritieke entiteiten eerst als zodanig moeten worden aangewezen. Kan de regering nader toelichten waarom hiervoor gekozen? Welke lidstaatopties zijn er mogelijk onder het bereik van de NIS2 en de CER-richtlijn bij het aanwijzen of kwalificeren van een essentiële entiteit of kritieke entiteit? Kan de regering nader schematisch uitleggen welke ruimte lidstaten hebben bij de beoordeling hiervan?

In artikel 6, tweede lid, CER-richtlijn zijn de criteria opgenomen op basis waarvan lidstaten van de Europese Unie moeten beoordelen of een entiteit kwalificeert als kritieke entiteit, waaronder het criterium dat een incident bij die entiteit aanzienlijke verstorende effecten zou hebben. Bij het bepalen of een verstorend effect aanzienlijk is, moeten lidstaten rekening houden met de criteria die zijn opgenomen in artikel 7, eerste lid, CER-richtlijn. Eén van die criteria betreft het aantal gebruikers dat afhankelijk is van de door de entiteit verleende essentiële dienst. Een ander criterium betreft de ernst en duur van de gevolgen die incidenten kunnen hebben voor economische en maatschappelijke activiteiten, het milieu, de openbare veiligheid en beveiliging, of de volksgezondheid. Welke entiteiten voldoen aan de hiervoor bedoelde criteria is afhankelijk van allerlei factoren binnen een lidstaat en kunnen dan ook per lidstaat verschillen. Daarom is in de CER-richtlijn ervoor gekozen om, weliswaar aan de hand van geharmoniseerde criteria, de beoordeling welke specifieke entiteiten als kritiek dienen te worden aangemerkt over te laten aan de lidstaten.

De NIS2-richtlijn bevat slechts in beperkte mate de ruimte voor lidstaten om entiteiten onder het toepassingsbereik te brengen van de nationale wet waarin die richtlijn is geïmplementeerd. Die ruimte is te vinden in artikel 2, vijfde lid, onderdelen a en b, NIS2-richtlijn (lidstaten kunnen bepalen dat de NIS2-richtlijn van toepassing is op overheidsinstanties op lokaal niveau en op onderwijsinstellingen) en artikel 3, eerste lid, onderdeel g, NIS2-richtlijn (lidstaten kunnen besluiten dat aanbieders van essentiële diensten in de zin van de NIS1-richtlijn als essentiële entiteiten in de zin van de NIS2-richtlijn worden beschouwd). Voor het overgrote deel van de entiteiten is in de NIS2-richtlijn al bepaald dat zij essentiële entiteit of belangrijke entiteit zijn. De reden voor deze beperkte ruimte voor lidstaten in de NIS2-richtlijn kan worden gevonden in één van de uitkomsten van de evaluatie van de NIS1-richtlijn, namelijk dat lidstaten op grond van de NIS1-richtlijn verantwoordelijk zijn voor het identificeren van aanbieders van essentiële diensten, waardoor er in dat opzicht grote verschillen zijn ontstaan tussen lidstaten terwijl deze verschillen – anders dan bij de CER-richtlijn – niet te verklaren zijn vanuit de specifieke lidstatelijke context.

2.4. Verhouding tot de DORA

De leden van de GroenLinks-PvdA-fractie lezen dat de samenhang met de Digital Operational Resilience Act (DORA) ervoor zorgt dat financiële instellingen gemakkelijk in het NIS2-regime vallen. Vanuit dit oogpunt valt het hen echter op dat de minister van Financiën als bevoegde entiteit wordt aangewezen. Is een andere rolverdeling verkend, bijvoorbeeld door de minister van Justitie en Veiligheid als één centraal aanspreekpunt aan te wijzen? Graag vernemen deze leden wat de specifieke bevoegdheden van de minister van Financiën behelzen.

Voor een aantal financiële instellingen (kredietinstellingen, exploitanten van handelsplatformen en centrale tegenpartijen) geldt dat zij zijn vermeld in bijlage I van de NIS2-richtlijn, zij uit dien hoofde essentiële entiteit dan wel belangrijke entiteit als bedoeld in de NIS2-richtlijn zijn en dat daarom het bepaalde in de Cbw in principe op hen van toepassing is. Van belang is echter dat er voor een groot deel van de financiële sector met de zogeheten *Digital Operational Resilience Act*[14] (hierna: DORA) sprake is van een sectorspecifieke rechtshandeling en daarom vanwege de in die verordening reeds opgenomen bepalingen ten aanzien van genoemde financiële instellingen het bepaalde in de Cbw over de zorgplicht, de meldplicht, en het toezicht en de handhaving daarop niet van toepassing zijn. Andere bepalingen in de Cbw, waaronder die over de verplichting om informatie te verstrekken ten behoeve van het nationaal

[14] Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (*PbEU* 2022, L 333).

register (zie artikel 44 Cbw), het toezicht en handhaving daarop, en bijstand door een CSIRT, zijn wél van toepassing ten aanzien van genoemde financiële instellingen. In verband hiermee is daarom in de Cbw voor deze financiële instellingen de Minister van Financiën als bevoegde autoriteit aangewezen, die tot taak heeft om toezicht te houden op de naleving van bijvoorbeeld de hiervoor genoemde verplichting tot informatieverstrekking. Met die aanwijzing van de Minister van Financiën als bevoegde autoriteit is aangesloten bij de keuze die ook voor andere essentiële entiteiten en belangrijke entiteiten is gemaakt om de vakminister aan te wijzen als de bevoegde autoriteit voor de (sub)sectoren die onder zijn beleidsverantwoordelijkheid vallen. De Minister van Financiën zal vanuit deze rol op grond van de Cbw waar noodzakelijk samenwerken en informatie uitwisselen met andere daarin genoemde instanties (CSIRT's, centraal contactpunt, andere bevoegde autoriteiten) en de toezichthoudende autoriteiten, bedoeld in de DORA. Daarnaast is in de DORA geregeld dat de daarin bedoelde toezichthoudende autoriteiten de mogelijkheid hebben om samen te werken en informatie uit te wisselen met de in de Cbw bedoelde instanties.

3. Nationale context

De leden van de GroenLinks-PvdA-fractie onderschrijven het belang van een brede maatschappelijke aanpak voor cyberveiligheid. Cyberveiligheid moet doorleefd worden in de hele structuur en cultuur van organisaties die het land draaiende houden. Deze leden vragen om een beknopte uiteenzetting van de doelstellingen uit artikel 7 van de NIS2-richtlijn en wat het antwoord op deze is zoals beschreven in de Nederlandse Cybersecuritystrategie (NLCS). Is het doel om beter zicht te hebben op cyberincidenten, -dreigingen en -risico's volledig afgedekt met de komst van de Cyberbeveiligingswet? Zij vragen de regering daarnaast om duidelijk te maken hoe abstract of concreet deze nationale strategie hoort te zijn volgens de NIS2-richtlijn, wetende dat de strategie nog per sector moet worden uitgewerkt.

Artikel 7, eerste lid, NIS2-richtlijn verplicht elke lidstaat van de Europese Unie tot het vaststellen van een nationale cyberbeveiligingsstrategie die voorziet in de strategische doelstellingen, de middelen die nodig zijn om die doelstellingen te behalen, en passende beleids- en regelgevingsmaatregelen, om een hoog niveau van cyberbeveiliging te bereiken en te handhaven. In deze bepaling is voorgeschreven waar de nationale cyberstrategie uit moet bestaan. Het gaat onder meer om de doelstellingen en prioriteiten, een governancekader voor die doelstellingen en prioriteiten en een plan om het algemene niveau van cyberbeveiligingsbewustzijn bij burgers te verbeteren.

Nederland heeft in 2022 de Nederlandse Cybersecuritystrategie 2022-2028 (hierna: NLCS) gepubliceerd. Dit is een strategisch beleidsdocument waarin de doelstellingen op het gebied van cyberbeveiliging zijn opgenomen. Het doel van de NLCS is niet alleen om beter zicht te hebben op cyberincidenten, -dreigingen en -risico's, maar ook dat een ieder zich blijft inzetten voor het verhogen van de weerbaarheid tegen cyberdreigingen. De NLCS is een levend document, waarbij ruimte is voor herijking. Er is echter, anders dan in de vraagstelling wordt verondersteld, geen sprake van het verder uitwerken per sector.

De NLCS bestaat uit een viertal pijlers. In het kader van de beantwoording van de door de leden van de GroenLinks-PvdA-fractie is een bespreking van met name pijler II en pijler IV van belang. Pijler ll gaat over veilige en innovatieve digitale producten en diensten. Deze pijler omvat onder meer het doel dat de overheid de ontwikkeling van veilige digitale producten via inkoop stimuleert. Aan dit doel zijn meerdere acties verbonden, waaronder het opstellen van Algemene Beveiligingseisen voor de Rijksoverheid (ABRO) waar bedrijven die gevoelige en/of gerubriceerde overheidsopdrachten vervullen aan moeten voldoen. Pijler IV ziet op de cybersecurity-arbeidsmarkt, het onderwijs en de digitale weerbaarheid van burgers. Deze pijler omvat meerdere doelen, waaronder het doel dat burgers goed beschermd zijn tegen digitale risico's en het doel dat burgers snel en adequaat reageren op cyberincidenten.

Bij de NLCS hoort een actieplan: Actieplan Nederlandse Cybersecuritystrategie 2022-2028.[15] Hierin zijn acties op gedetailleerd niveau uitgewerkt, inclusief concreet handelingsperspectief en tijdspaden.

Naast de NLCS en bijbehorend actieplan is er ook een Landelijk Crisisplan Digitaal. Dit plan is opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en biedt de kaders voor

[15] Te downloaden via https://www.nctv.nl/documenten/2022/10/10/actieplan-nederlandse-cybersecuritystrategie-2022-2028.

effectieve samenwerking tussen overheidsorganisaties, vitale aanbieders en niet-vitale sectoren bij een digitale crisis.

Met al het voorgaande (NLCS, met bijbehorende pijlers en actieplan, en het Landelijk Crisisplan Digitaal) voldoet Nederland aan de in artikel 7, eerste lid, NIS2-richtlijn opgenomen verplichting voor lidstaten tot het hebben van een nationale cyberbeveiligingsstrategie en de vereisten die aan die strategie worden gesteld.

Over de NLCS wordt jaarlijks een voortgangsrapportage uitgebracht. De eerstvolgende voortgangsrapportage is voorzien voor november 2025. In 2026 zal een tussentijdse evaluatie van de NLCS en het bijbehorende actieplan aan uw Kamer worden aangeboden.

4. Gemaakte implementatiekeuzes op hoofdlijnen

De leden van de GroenLinks-PvdA-fractie kunnen zich vinden in het besluit om de NIS2-richtlijn om te zetten in één centrale wet. Deze leden vragen de regering of zij een analyse heeft gemaakt om te bezien of er alsnog aanpassingen in sectorale wetgeving of samenhangend beleid noodzakelijk zijn voor een effectieve werking van de Cyberbeveiligingswet. Zo ja, waarom is er gekozen om niet gelijktijdig aan de Cyberbeveiligingswet ook samenhangende wetgeving aan te passen? Zo nee, met welke zekerheid kan de regering dan zeggen dat er geen tegenstrijdigheden of onduidelijkheden bestaan tussen de Cyberbeveiligingswet en andere wetgeving?

De regering heeft bezien of er aanpassingen nodig zijn in andere wetgeving, voor een effectieve werking van de Cbw en ter voorkoming van tegenstrijdigheden of onduidelijkheden. Naar aanleiding van deze inventarisatie zijn in het wetsvoorstel enkele wijzigingen opgenomen van andere wetgeving, waaronder de Telecommunicatiewet en de Wet bevordering digitale weerbaarheid bedrijven (hierna: Wbdwb). Zie de artikelen 99 tot en met 103 Cbw. Het wetsvoorstel regelt dus wél gelijktijdig de aanpassing van samenhangende wetgeving.

Overigens is na de indiening van het wetsvoorstel gebleken dat er nog enkele andere wetten zijn die ook moeten worden gewijzigd, waaronder de Wet bekostiging financieel toezicht 2019. Die wijzigingen worden geregeld middels een nota van wijziging op het wetsvoorstel.

De leden van de GroenLinks-PvdA-fractie vragen wat de voor- en nadelen zijn van het aanwijzen van vakministers als verantwoordelijk binnen hun sectoren. Over het algemeen achten zij het wenselijk dat coördinerende taken helder en centraal belegd zijn. Is er, gezien de centrale en coördinerende rol van de minister van Justitie en Veiligheid, niet veel voor te zeggen om deze minister als eindverantwoordelijk aan te wijzen voor alle sectoren? Deze leden vragen of dit de samenwerking en informatie-uitwisseling tussen sectoren kan verbeteren. Bovendien merken zij op dat de coördinerende staatssecretaris voor Digitalisering en Koninkrijksrelaties geen rol heeft in deze wet. Heeft de regering overwogen om de minister van Binnenlandse Zaken, gedelegeerd aan de relevante staatssecretaris, als coördinerend aan te wijzen?

De regering heeft bij de implementatie van de NIS2-richtlijn niet overwogen om de Minister van Binnenlandse Zaken en Koninkrijksrelaties als coördinerend bewindspersoon aan te wijzen voor de Cbw. De regering heeft ervoor gekozen om aan te sluiten bij de huidige verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid. Die verdeling houdt in dat elke vakminister verantwoordelijk is voor de digitale weerbaarheid en de continuïteit van de sectoren binnen zijn portefeuille en dat de Minister van Justitie en Veiligheid coördinerend bewindspersoon is op cybersecurity en nationale veiligheid. Voor wat betreft de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties geldt dat hij op grond van de huidige taakomschrijving is belast met de coördinerende verantwoordelijkheid voor digitalisering en met de digitale rijksdienst en digitale veiligheid van de overheid.[16] De verantwoordelijkheid voor de digitale veiligheid van de overheid sluit aan bij de rol die de Minister van Binnenlandse Zaken en Koninkrijksrelaties heeft voor organisaties binnen de sector overheid.

De ratio achter de hiervoor omschreven verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid is dat netwerk- en informatiesystemen verweven zijn met alle processen binnen de

[16] *Stcrt*. 2025, 23904.

samenleving en een sector- of entiteitspecifieke toepassing hebben. Dit vraagt om sectorspecifieke kennis en een holistische blik op de samenhang van de risico's ten aanzien van netwerk- en informatiesystemen met andere risico's binnen de sector. Dit heeft een positief effect op de slagkracht en effectiviteit.

Een mogelijk nadeel van deze gekozen verantwoordelijkheidsverdeling is dat er niet één centraal sectoroverstijgend aanspreekpunt is en er mogelijk sprake kan zijn van sectorspecifiek beleid, wat kan leiden tot differentiatie tussen sectoren. Deze nadelen worden echter ondervangen doordat de Minister van Justitie en Veiligheid coördinerend bewindspersoon is op cybersecurity en nationale veiligheid. Voor de Cbw betekent dit dat wanneer in de Cbw is voorgeschreven dat de vakminister nadere regels of besluiten voor zijn sector na overleg met of in overeenstemming met de Minister van Justitie en Veiligheid moet vaststellen, de Minister van Justitie en Veiligheid zal toetsen en adviseren op onder meer sectoroverstijgende effecten, de druk op het cybersecuritystelsel en de bredere impact op de nationale veiligheid. Door in de Cbw te regelen dat in veel gevallen afstemming moet plaatsvinden tussen de Minister van Justitie en Veiligheid en de vakminister, wordt de samenwerking en informatie-uitwisseling tussen de sectoren verbeterd.

De leden van de CDA-fractie constateren dat de reikwijdte van de richtlijn is uitgebreid ten opzichte van de NIS1-richtlijn. Deze leden vragen of de regering nader wil ingaan op de gemaakte keuzes in Europees verband. Zij vragen of is overwogen de reikwijdte nog verder uit te breiden en om welke sectoren het dan ging. Ook vragen de leden van de CDA-fractie wat de inzet van de regering was op dit punt, en in hoeverre deze inzet is overgenomen.

Voor de beantwoording van deze vraag verwijst de regering naar het fiche van de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC) over de herziening van de NIS1-richtlijn.[17] Hierin komt aan de orde dat het nieuwe voorstel van de Europese Commissie over de herziening van de NIS1-richtlijn via centrale aanwijzing regelt welke entiteiten binnen de reikwijdte van de richtlijn vallen. Hiermee wordt aan de lidstaten van de Europese Unie de mogelijkheid ontnomen om zelf te bepalen welke entiteiten essentieel of belangrijk zijn. Het kabinet geeft in het fiche aan dat centrale aanwijzing in het geval van essentiële entiteiten op gespannen voet staat met de uitsluitende verantwoordelijkheid van lidstaten met betrekking tot de bescherming van de nationale veiligheid. Tegelijkertijd onderkent het kabinet het belang van een gelijk speelveld voor aanbieders binnen de eengemaakte markt. Het kabinet heeft in de onderhandelingen over de herziening van de NIS1-richtlijn de aandacht gevraagd voor de verdragsrechtelijke afspraken betreffende de uitsluitende verantwoordelijkheid van lidstaten op het gebied van nationale veiligheid. Het kabinet was niet principieel tegen een uitbreiding van de reikwijdte met nieuwe sectoren, maar heeft het standpunt ingenomen dat regulering van extra diensten en aanbieders pas dient plaats te vinden na een grondige risicoanalyse, waarin wordt vastgesteld dat het opleggen van verplichtingen noodzakelijk is. Deze verplichtingen dienen ook proportioneel te zijn aan het risico. Vanuit die risicotoets kan de regering zich vinden in de sectoren die onder de NIS2-richtlijn zijn gebracht.

5. Gevolgen

5.1. Essentiële entiteiten en belangrijke entiteiten

5.1.1. Essentiële entiteiten en belangrijke entiteiten

De leden van de GroenLinks-PvdA-fractie lezen over het onderscheid tussen essentiële en belangrijke entiteiten. Kan de regering beeldend maken wat het onderscheid tussen beide categorieën is, door enkele voorbeelden te noemen van zowel essentiële als belangrijke entiteiten? Kan de regering daarbij onderbouwen op basis van welke kwalificaties deze entiteiten in een van de twee categorieën is geplaatst? Deze leden vragen de regering ook om voorbeelden te noemen van entiteiten die in meerdere sectoren actief zijn en te maken krijgen met verschillende sectorale verplichtingen en aanspreekpunten. Bovendien zien zij het risico dat entiteiten die in meerdere sectoren werken, in geval van crisis alsnog de weg niet kunnen vinden naar de juiste instantie. De leden vragen aan de regering om nader toe te lichten hoe entiteiten in meerdere sectoren worden geacht hun zorgplicht en meldplicht uit te voeren.

[17] *Kamerstukken II* 2020/21, 22112, nr. 3053.

Welke entiteiten kwalificeren als essentiële entiteit en welke als belangrijke entiteit volgt dwingend uit de NIS2-richtlijn, zie artikel 3, eerste en tweede lid, NIS2-richtlijn. Deze bepalingen zijn geïmplementeerd in de artikelen 8, 9, 10 en 12 Cbw. Ter ondersteuning van entiteiten heeft de rijksoverheid een zelfevaluatietool gemaakt waarmee zij kunnen bepalen of zij als essentiële entiteit dan wel als belangrijke entiteit onder de Cbw vallen.[18]

In veel gevallen is het voor het antwoord op de vraag of een entiteit kwalificeert als essentiële entiteit of als belangrijke entiteit, relevant in welke bijlage van de Cbw (bijlage 1 of bijlage 2) de soort entiteit in de bijbehorende (sub)sector is opgenomen. Ook is in veel gevallen de omvang van de entiteit van belang voor het bepalen of een entiteit kwalificeert als een essentiële entiteit of een belangrijke entiteit. Deze twee aspecten (sector en omvang) betreffen echter geen algemene kwalificaties waarmee ten aanzien van alle entiteiten kan worden bepaald of zij kwalificeren als essentiële entiteit dan wel belangrijke entiteit. Zo geldt bijvoorbeeld ten aanzien van sommige entiteiten, die zijn genoemd in één van de bijlagen, dat zij hoe dan ook essentiële entiteit zijn, los van de sector en omvang.

De volgende entiteiten zijn essentiële entiteiten:
- gekwalificeerde verleners van vertrouwensdiensten;
- aanbieders van registers voor topleveldomeinnamen;
- DNS-dienstverleners;
- aanbieders van openbare elektronische communicatienetwerken, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG[19];
- aanbieders van openbare elektronische communicatiediensten, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij Aanbeveling 2003/361/EG;
- andere entiteiten, genoemd in bijlage 1 van de Cbw, die de in artikel 2, eerste lid, van de bijlage bij Aanbeveling 2003/361/EG bedoelde drempel voor middelgrote ondernemingen overschrijden;
- de ministeries, met inbegrip van de daartoe behorende dienstonderdelen doch met uitzondering van de inlichtingen- en veiligheidsdiensten, en zelfstandige bestuursorganen van de centrale overheid, voor zover deze zelfstandige bestuursorganen kwalificeren als overheidsinstantie zoals gedefinieerd in artikel 1 Cbw;
- provincies, gemeenten en waterschappen;
- openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties als bedoeld in artikel 8, eerste, tweede, onderscheidenlijk derde lid, Wet gemeenschappelijke regelingen, voor zover deze openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties kwalificeren als overheidsinstantie zoals gedefinieerd in artikel 1 Cbw;
- kritieke entiteiten als bedoeld in artikel 6, eerste lid, Wwke; en
- de entiteiten die op grond van de artikelen 9, 10 of 11 Cbw bij regeling of besluit worden aangewezen als essentiële entiteit.

Enkele voorbeelden van essentiële entiteiten: transmissienetbeheerder TenneT, Royal Schiphol Group N.V. (Amsterdam Airport Schiphol), ziekenhuizen, VodafoneZiggo en de N.V. Nederlandse Spoorwegen.

De volgende entiteiten zijn belangrijke entiteiten:
- entiteiten, genoemd in bijlage 1 van de Cbw, niet zijnde een essentiële entiteit, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG;
- entiteiten, genoemd in bijlage 2 van de Cbw, niet zijnde een essentiële entiteit, die in aanmerking komen als middelgrote onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG of de in het eerste lid van laatstgenoemd artikel vastgestelde drempels voor middelgrote ondernemingen overschrijden;
- aanbieders van openbare elektronische communicatienetwerken, genoemd in bijlage 1 van de Cbw, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit;

[18] Deze tool is te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS-2-NL/.

[19] Aanbeveling 2003/361/EG van de Commissie van 6 mei 2003 betreffende de definitie van kleine, middelgrote en micro-ondernemingen (*PbEU* 2003, L 124).

- aanbieders van openbare elektronische communicatiediensten, genoemd in bijlage 1 van de Cbw, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit;
- verleners van vertrouwensdiensten, genoemd in bijlage 1 van de Cbw, die in aanmerking komen als kleine of micro-onderneming uit hoofde van artikel 2 van de bijlage bij de Aanbeveling 2003/361/EG, niet zijnde een essentiële entiteit; en
- de instellingen voor hoger onderwijs die op grond van artikel 13 Cbw bij regeling of besluit van de Minister van Onze Minister van Onderwijs, Cultuur en Wetenschap worden aangewezen als belangrijke entiteit.

Enkele voorbeelden van belangrijke entiteiten: PostNL en fabrikanten van medische hulpmiddelen.

Het kan voorkomen dat entiteiten in meerdere sectoren actief zijn. Hierdoor kunnen zij mogelijk te maken krijgen met verschillende bevoegde autoriteiten of CSIRT's. Met de aanwijzing van de bevoegde autoriteit in artikel 15, eerste tot en met vijfde lid, Cbw en de aanwijzing van het CSIRT in artikel 2, eerste en tweede lid, Cyberbeveiligingsbesluit (hierna: Cbb) is voor deze entiteiten voldoende duidelijk welke instantie zij moeten benaderen voor bijvoorbeeld het doen van een melding van een significant incident of een verzoek om bijstand bij dreigingen of incidenten.

Indien een entiteit onder meerdere sectoren valt, kan de situatie zich voordoen dat deze entiteit vanuit de ene sector waartoe het behoort van rechtswege essentieel is en vanuit de andere sector van rechtswege belangrijk. Enkele voorbeelden hiervan: de petrochemische industrie (essentieel in verband met olie en gas, belangrijk in verband met de chemische industrie) en drankproducenten die gebotteld water produceren (essentieel in verband met drinkwater, belangrijk in verband met de voedselproductie). In zulke gevallen wordt de gehele entiteit als essentieel beschouwd.

Voor elke essentiële entiteit en belangrijke entiteit geldt op grond van artikel 21 Cbw de verplichting om passende en evenredige technische, operationele en organisatorische maatregelen te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen, die zij voor haar werkzaamheden of voor het verlenen van haar diensten gebruiken, te beheersen. Dit betekent dat iedere entiteit ten minste de maatregelen dient te nemen die zijn opgesomd in artikel 21, derde lid, Cbw. Deze maatregelen zijn nader uitgewerkt in het Cbb. Daarnaast is het voor de vakministers mogelijk om bij ministeriële regelingen nadere regels te stellen over die maatregelen, bijvoorbeeld voor entiteiten die actief zijn in een bepaalde sector. Indien een entiteit onder meerdere sectoren – en daarmee mogelijk onder meerdere ministeriële regelingen – valt, dient zij al deze nadere regels in acht te nemen om op deze wijze aan de zorgplicht te voldoen.

In het kader van de meldplicht geldt dat elke essentiële entiteit en belangrijke entiteit – ongeacht de sector – op grond van artikel 25, eerste lid, Cbw bij het CSIRT en de bevoegde autoriteit melding moet maken van significante incidenten. Voor het doen van die meldingen kan gebruik worden gemaakt van één meldportaal en kan een entiteit die in meerdere sectoren actief is en uit hoofde daarvan behoort tot verschillende soorten entiteiten waarop de Cbw van toepassing, dat in dat portaal aangeven. Om te bepalen of een incident significant is, zijn in artikel 25, tweede lid, Cbw drie parameters opgenomen, namelijk de (mogelijke) ernstige operationele verstoring van de diensten van de entiteit, (mogelijke) financiële verliezen voor de entiteit en (mogelijke) materiële of immateriële schade voor andere entiteiten. Bij regelingen of besluiten van de vakministers zullen de criteria (ook wel drempelwaarden genoemd) worden vastgesteld op basis waarvan kan worden bepaald of sprake is van een significant incident als bedoeld in artikel 25, tweede lid, Cbw. Daarbij kan bijvoorbeeld tussen sectoren onderscheid worden gemaakt. Indien een entiteit onder meerdere sectoren valt, en voor die sectoren verschillende drempelwaarden worden vastgesteld, dient zij al deze drempelwaarden in acht te nemen teneinde aan de meldplicht te voldoen.

Enkele voorbeelden van entiteiten die in meerdere sectoren actief zijn: *charge point operators* (CPO's, de bedrijven achter de laadpalen) en fabrikanten van medische hulpmiddelen die ook elektronische consumentengoederen vervaardigen en daardoor zowel onder de sector gezondheidszorg als de sector vervaardiging vallen, zoals Philips.

De leden van de GroenLinks-PvdA-fractie voorzien mogelijke grijze gebieden als het aankomt op entiteiten die niet per wet als essentieel of belangrijk kunnen worden bestempeld. Hiervoor wordt de nationale vitaalbeoordeling gebruikt als methodiek. Het is voor deze leden echter niet duidelijk hoe deze beoordeling en de aanwijzing in de praktijk zal werken. Zij vragen de regering dan ook om beter duidelijk maken hoe dit aanwijzingsproces werkt, zodat het helder is hoe de beoordeling op basis van criteria wordt uitgevoerd, wie daarvoor verantwoordelijk is en wat er verwacht wordt van de desbetreffende entiteit. Zij vragen de regering om duidelijk te maken hoe de rollen verdeeld zijn tussen de vakminister en de minister van Justitie en Veiligheid.

De vakministers wijzen op grond van artikel 9, eerste lid, Cbw een in bijlage 1 of bijlage 2 van de Cbw genoemde entiteit aan als essentiële entiteit als zij voldoet aan één of meer van de criteria die in die bepaling staan genoemd. De invulling van dit aanwijzingsproces wordt op dit moment nader uitgewerkt. Van entiteiten wordt verwacht dat zij op verzoek informatie aanleveren die noodzakelijk is voor het uitvoeren van de beoordeling of voldaan wordt aan een criterium uit artikel 9, eerste lid, Cbw.

Om vast te stellen of een entiteit voldoet aan één of meer criteria uit artikel 9, eerste lid, Cbw zal gebruik worden gemaakt van de nationale vitaalbeoordeling. Het doel van de vitaalbeoordeling is om inzichtelijk te maken welke processen en diensten zo essentieel zijn voor de Nederlandse samenleving, dat uitval, verstoring of manipulatie daarvan kan leiden tot ernstige maatschappelijke ontwrichting, ernstige economische schade of – in het uiterste geval – een bedreiging van de nationale veiligheid. Deze geïdentificeerde processen worden vitale processen genoemd en gezamenlijk vormen deze vitale processen de vitale infrastructuur van Nederland.

Er is gekozen om de toetsing aan de criteria uit artikel 9, eerste lid, Cbw te doen aan de hand van de nationale vitaalbeoordeling, omdat de aanmerking als vitale aanbieder plaatsvindt op basis van vergelijkbare criteria als die voor het aanwijzen van essentiële entiteiten. Deze systematiek wordt ook toegepast voor het aanwijzen van kritieke entiteiten als bedoeld in de Wwke.

Het uitvoeren van de vitaalbeoordeling en de aanwijzing van entiteiten is in de eerste plaats de verantwoordelijkheid van de vakminister, in overleg met de Minister van Justitie en Veiligheid als coördinerend bewindspersoon voor de bescherming van de vitale infrastructuur en cybersecurity.

Artikel 9, eerste lid, Cbw schrijft voor dat de hiervoor bedoelde aanwijzing kan plaatsvinden bij regeling of bij besluit. De aanwijzing betreft hoe dan ook een besluit in de zin van artikel 1:3 Algemene wet bestuursrecht (hierna: Awb), ook als de aanwijzing geschiedt bij ministeriële regeling. Dit betekent dat de vakminister bij de aanwijzing moet voldoen aan de in de Awb gestelde eisen aan besluitvorming door bestuursorganen en dat tegen de aanwijzing bestuursrechtelijke rechtsbescherming open staat.

De leden van de VVD-fractie constateren dat het uitvoeren van de vitaalbeoordeling en de aanwijzing van entiteiten in de eerste plaats een verantwoordelijkheid is van de vakminister, in overleg met de minister van Justitie en Veiligheid (J&V) als coördinerend bewindspersoon voor de bescherming van de vitale infrastructuur en cybersecurity. Kan de regering nader toelichten hoe dit afstemmen efficiënt in de praktijk zal werken? Wat is de procedure bij mogelijke beleidsconflicten tussen de vakminister en de minister van J&V in zijn rol als coördinerend bewindspersoon? Deze leden vragen een uitgebreide toelichting op de coördinerende rol van de minister van J&V en hoe die in de praktijk zal worden vormgegeven.

Voor het vaststellen of een entiteit, die niet van rechtswege essentiële entiteit of belangrijke entiteit is, voldoet aan een criterium uit artikel 9, eerste lid, Cbw, en in verband daarmee zal worden aangewezen als essentiële entiteit, zal gebruik worden gemaakt van de nationale vitaalbeoordeling. Het uitvoeren van die beoordeling en het op grond daarvan aanwijzen van een entiteit als essentiële entiteit is inderdaad primair de verantwoordelijkheid van de betrokken vakminister. Daarmee wordt aangesloten bij de huidige verantwoordelijkheidsverdeling op het terrein van cybersecurity, alsook de huidige rolverdeling als het gaat om het uitvoeren van vitaalbeoordelingen, waarbij elke vakminister verantwoordelijk is voor onder meer de digitale weerbaarheid binnen zijn portefeuille. Bovenbedoelde beoordeling vraagt om sectorspecifieke kennis met betrekking tot onder meer risico's ten aanzien van de netwerk- en

informatiesystemen van entiteiten die binnen die sector actief zijn. De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op cybersecurity en de bescherming van de vitale infrastructuur.

In de praktijk betekent het voorgaande dat de vakminister de uitkomsten van een beoordeling van entiteiten aan de hand van criteria als bedoeld in artikel 9, eerste lid, Cbw binnen zijn sector ter toetsing zal voorleggen aan de Minister van Justitie en Veiligheid. De Minister van Justitie en Veiligheid zal toetsen en adviseren op onder meer sectoroverstijgende effecten, de druk op het cybersecuritystelsel en de bredere impact op de nationale veiligheid. In de praktijk zal de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) namens de Minister van Justitie en Veiligheid hieraan invulling geven en onder meer beoordelen wat de gevolgen en risico's zijn voor de nationale veiligheid en of het voorstel van de vakminister passend is binnen het bredere cybersecuritystelsel.

Een eventueel verschil van inzicht over het al dan niet op grond van artikel 9, eerste lid, Cbw aanwijzen van een entiteit als essentiële entiteit kan worden opgelost via de gangbare afstemmings- en overlegstructuren, maar de vakminister neemt uiteindelijk eigenstandig de eindbeslissing. De vakminister mag deze beslissing pas nemen nadat er overleg heeft plaatsgevonden met de Minister van Justitie en Veiligheid, wat inhoudt dat de vakminister verplicht is te overleggen met de Minister van Justitie en Veiligheid.

5.1.2. Overheidsinstanties

De leden van de GroenLinks-PvdA-fractie staan achter de keuze om de NIS2-richtlijn toe te passen op medeoverheden. Echter, deze leden hebben twijfels over de capaciteit van gemeenten, provincies en waterschappen om zich voldoende voor te bereiden op de Cyberbeveiligingswet. Welke duidelijkheid verschaft de regering aan medeoverheden over de nodige voorbereiding? Zij wijzen op nieuwe verplichtingen, (voorbereidings)budget, aanvullende capaciteit en dergelijke waar medeoverheden zich op moeten kunnen voorbereiden. De leden vragen aan de regering om aan te tonen dat zij medeoverheden hier adequaat over hebben geïnformeerd en welke middelen de regering beschikbaar heeft gesteld voor het steunen van overheidsorganisaties.

Reeds voorafgaand aan de onderhandelingen over de NIS2-richtlijn heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties met de verschillende bestuurslagen vanaf het voorjaar van 2019 ambtelijk overleg gevoerd om wetgeving voor te bereiden ter zake van de informatieveiligheid van de overheid.[20] Deze wetgeving moest een eerste stap zijn om een veelheid aan interbestuurlijke informatiebeveiligingseisen en toezicht daarop bij de medeoverheden te vereenvoudigen. Deze vereenvoudiging heeft als doel om de lastendruk bij medeoverheden, met name gemeenten, te verlagen. Het ENSIA-initiatief[21] is een goede illustratie van het verlagen van de lastendruk en wordt al een aantal jaar door gemeenten gebruikt voor hun geharmoniseerde verantwoording over informatiebeveiliging. Het verder brengen van deze harmonisering is bovendien als ambitie opgenomen in de Werkagenda Waardengedreven Digitalisering.[22]

De NIS2-richtlijn geeft de mogelijkheid om de eerste stap van deze ambitie versneld te realiseren. Hierover zijn de verschillende bestuurslagen formeel per brief geïnformeerd op 20 november 2023.[23] Bij het opstellen van lagere regelgeving onder de Cbw is, met het oog op het beperken van de lastendruk, voor medeoverheden het voornemen om maximaal gebruik te maken van bestaande verplichtingen. Voor de nadere invulling van de zorgplicht voor de overheid wordt gebruikgemaakt van de herziene Baseline

---

[20] Wetgeving werd al genoemd als mogelijk instrument in de *Eindrapportage Taskforce Bestuur & Informatieveiligheid Dienstverlening*, februari 2015.

[21] Dit staat voor *Eenduidige Normatiek Single Information Audit*. ENSIA is een initiatief van gemeenten, het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Sociale Zaken en Werkgelegenheid. ENSIA streeft naar een zo effectief en efficiënt mogelijk ingericht verantwoordingsstelsel voor informatiebeveiliging en informatiekwaliteit. Meer informatie is terug te vinden op www.ensia.nl.

[22] *Kamerstukken II* 2022/23, 26643, nr. 940, bijlage 1062267, paragraaf 2.4.

[23] *NIS2 bij de overheid,* https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/nis2-richtlijn/nis2-bij-de-overheid-kamerbrief/.

Informatiebeveiliging Overheid (BIO), waaraan alle overheidslagen zich eerder hebben gecommitteerd.[24] De totstandkoming van de BIO heeft bovendien plaatsgevonden onder coördinatie van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in samenwerking met alle bestuurslagen. Dit zijn om die reden geen nieuwe verplichtingen.

Bij het proces van totstandkoming van de Cbw en onderliggende regelgeving is er bovendien regelmatig contact met alle overheidslagen, met als doel om wensen en knelpunten vanuit medeoverheden al in een vroeg stadium van het wetgevingsproces te betrekken. Dat gebeurt onder meer via reguliere overleggen met de koepelvertegenwoordigers van de medeoverheden, vanuit het proces van de Uitvoerbaarheidstoets Decentrale Overheden (UDO) en de werkgroepen BIO. Bovendien is op verschillende momenten formeel gecommuniceerd over de voortgang van het wetgevingstraject: via de Minister van Justitie en Veiligheid over de algehele voortgang en via de Verzamelbrieven Digitalisering van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties over de toepassing voor de overheid. Daarnaast verzorgt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties op verschillende manieren informatie aan overheidsorganisaties over de komst van de Cbw: via webinars, kennissessies en de website www.digitaleoverheid.nl, waar bovendien handige tools en ondersteuning worden gedeeld.

Er wordt reeds aan verschillende overheidsorganen ondersteuning geboden, welke inzet wordt voortgezet. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties financiert daartoe het Centrum voor Informatiebeveiliging en Privacy (CIP). Het CIP organiseert en faciliteert kennisdeling in vele vormen, zoals themabijeenkomsten, webinars, podcasts, workshops en games. Het CIP biedt bovendien een reeks van producten aan die iedereen kan downloaden en vrij kan gebruiken.[25] Bovendien wordt op korte termijn, met subsidie vanuit het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, gestart met regioaanjagers bij gemeenten om hen te helpen met het implementeren van maatregelen voor hun informatiebeveiliging.

Ten slotte wordt het volgende opgemerkt. Overheidsorganen zijn heel verschillend. De ene organisatie zal vanwege zijn aard meer en/of andere maatregelen hebben getroffen dan de ander. De overheid kent reeds het uitgangspunt van risicogestuurd beveiligen: afhankelijk van het te beschermen belang en de dreiging wordt een afweging gemaakt welke maatregelen noodzakelijk zijn. Deze aanpak voorkomt te hoog ingeschatte kosten waar deze eigenlijk niet nodig zijn, maar ook te lage kosteninschattingen die niet toereikend blijken.

De leden van de GroenLinks-PvdA-fractie merken op dat criterium A wijst op het algemene belang dat een overheidsdienst moet dienen. Echter zijn veel overheidsdiensten in de jaren geliberaliseerd, denk aan de Nederlandse Spoorwegen (NS), die zowel een essentiële overheidsdienst vervullen als opereren onder marktomstandigheden. Voldoen dergelijke entiteiten aan criterium A? Acht de regering het wenselijk om dit soort organisaties wel of niet als overheidsinstanties aan te merken?

De leden van de GroenLinks-PvdA-fractie merken op dat criterium C alleen toeziet op organisaties met een meerderheidsaandeel van de overheid. Deze leden vragen aan de regering om te onderbouwen waarom dit criterium niet van toepassing is op organisaties die voor een aanzienlijk deel, maar minder dan 50%, gefinancierd worden door de overheid. Is er bij deze organisaties niet evengoed sprake van een bijzonder algemeen belang?

Voor de definitie van het begrip overheidsinstantie, welke is opgenomen in artikel 1 Cbw, geldt dat dit de implementatie betreft van de definitie van dat begrip in artikel 6, onderdeel 35, NIS2-richtlijn. De regering heeft daarbij, indachtig het kabinetsbeleid dat er geen nationale koppen komen op Europese regelgeving, geen ruimte gezien om af te wijken van die definitie uit de NIS2-richtlijn door de daarin opgenomen criteria te veranderen.

Of van geprivatiseerde overheidsdiensten kan worden gezegd dat ze zijn opgericht om te voorzien in behoeften van algemeen belang en geen industrieel of commercieel karakter hebben, zal van geval tot geval moeten worden bezien. Los hiervan is een entiteit slechts een overheidsinstantie in de zin van de

[24] *Stcrt.* 2019, 26526.

[25] Dat kan via www.cip-overheid.nl.

Cbw indien aan alle vier de criteria uit de definitie van overheidsinstantie (opgenomen in artikel 1 Cbw) is voldaan. Specifiek voor de N.V. Nederlandse Spoorwegen geldt dat die behoort tot de sector vervoer, subsector spoor, en daarmee al onder het toepassingsbereik van de Cbw valt.

Over het derde criterium (in artikel 1 Cbw aangeduid met de letter c) wordt overigens opgemerkt dat daaraan niet alleen is voldaan als de entiteit grotendeels wordt gefinancierd door de overheid, maar ook indien de entiteit is onderworpen aan beheerstoezicht door de overheid of indien meer dan de helft van de leden van een bestuurs-, leidinggevend of toezichthoudend orgaan van de entiteit door de overheid wordt benoemd.

De leden van de GroenLinks-PvdA-fractie merken op dat het ministerie van Defensie niet onder het bereik van de NIS2-richtlijn valt. Hoewel de uitzonderlijke positie van dit departement begrijpelijk is, vragen deze leden om een nadere onderbouwing waarom deze buiten de reikwijdte valt van dit criterium en hoe onder welk cyberveiligheidsregime het departement wél valt.

De NIS2-richtlijn is niet van toepassing op overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het voorkomen, onderzoeken, opsporen en vervolgen van strafbare feiten. Voor Nederland betekent dit dat onder meer het Ministerie van Defensie buiten het toepassingsbereik van de NIS2-richtlijn valt en daarmee ook de Cbw, waarin de NIS2-richtlijn wordt geïmplementeerd. Deze voornoemde activiteiten vallen namelijk binnen de uitsluitende verantwoordelijkheid van de lidstaten van de Europese Unie. In artikel 4 Verdrag betreffende de Europese Unie (VEU) is hierover vastgelegd dat de bescherming van de nationale veiligheid, de verdediging van de territoriale integriteit van de staat en de handhaving van de openbare orde, essentiële staatsfuncties zijn die vanuit de Europese Unie dienen te worden geëerbiedigd. Hierin wordt onderstreept dat “met name de nationale veiligheid” de uitsluitende verantwoordelijkheid blijft van elke lidstaat.

Defensie draagt zorg voor de cyberveiligheid van haar netwerken op vergelijkbare wijze als opgenomen in de Cbw. Voor het Ministerie van Defensie gelden immers onafhankelijk van de toepassing van de Cbw reeds verschillende internationale normen, zoals eisen vanuit de NAVO en de Europese Unie, en nationale normen, zoals de Baseline Informatiebeveiliging Overheid (BIO), het Besluit voorschrift informatiebeveiliging rijksdienst 2007 (VIR) en het Besluit voorschrift informatiebeveiliging rijksdienst bijzondere informatie 2025 (VIR-BI). Bovendien geeft de herziene Defensie Cyberstrategie, die op 3 oktober jl. naar uw Kamer is verstuurd onder meer richting aan de taak van eigen cyberveiligheid en de bijdrage van Defensie aan de cyberweerbaarheid van Nederland en bondgenoten.[26]

5.1.3. Onderwijsinstellingen

De leden van de GroenLinks-PvdA-fractie lezen dat de minister van Onderwijs, Cultuur en Wetenschap (OCW) de bevoegdheid krijgt om onderwijsinstellingen aan te wijzen als essentiële of belangrijke entiteit. Deze leden vragen de regering om helder te formuleren wanneer de minister van OCW deze bevoegdheid inzet. Welke instellingen zullen per direct aangewezen worden als zodanig? Welke andere voorwaarden zijn er verbonden aan deze aanwijzing? Bovendien lezen zij dat er “intensief overleg [is] gevoerd met alle betrokken stakeholders.” Graag vernemen de leden welke instellingen dit betreft en of deze unaniem instemden met het voorstel. Zijn er in deze gesprekken concessies gedaan vanuit de regering?

In de Cbw is, in lijn met de NIS2-richtlijn, de mogelijkheid opgenomen voor de Minister van Onderwijs, Cultuur en Wetenschap om instellingen in het hoger onderwijs als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw aan te wijzen en daarmee onder de reikwijdte van de Cbw te brengen. Gezien het belang van een brede en duurzame beheersing van cyberrisico’s, ook voor het onderwijs, heeft de regering besloten om de bekostigde instellingen in het hoger beroepsonderwijs en wetenschappelijk onderwijs (hierna: hbo- en wo-instellingen) als essentiële entiteit of belangrijke entiteit aan te wijzen en daarmee onder het toepassingsbereik van de Cbw te brengen. Hierover is uw Kamer met de brief van 24 april 2025 geïnformeerd.[27] De bevoegdheid van de Minister van Onderwijs, Cultuur en Wetenschap om de

[26] *Kamerstukken II* 2024/25, 26643, nr. 1422.

[27] *Kamerstukken II* 2024/25, 31288, nr. 1189.

hbo- en wo-instellingen aan te wijzen, zal worden ingezet met ingang van het moment dat de Cbw in werking treedt.

In antwoord op de vraag van de leden van de GroenLinks-PvdA-fractie of de instellingen unaniem instemden met het voorstel is het antwoord dat dit niet het geval is geweest. Het besluit om deze instellingen in bovenbedoelde zin aan te wijzen betreft geen voorstel aan de instellingen, maar een besluit op basis van een integrale afweging van de regering waarvoor de sectoren via de koepelorganisaties intensief zijn geraadpleegd. De koepelorganisaties hebben daarbij aangegeven zorgen te hebben over de negatieve gevolgen die de keuze om genoemde instellingen onder het toepassingsbereik van de Cbw te brengen volgens hen gaat hebben, gezien de tijd, inzet en middelen die dit vraagt van instellingen om zich voor te bereiden op de nieuwe verplichtingen die de aanwijzing met zich meebrengt. Om die reden heeft de regering besloten om in het wetsvoorstel te regelen dat de zorgplicht, opgenomen in artikel 21 Cbw, en de in artikel 24 Cbw opgenomen verplichtingen over governance, vanaf 36 maanden na de aanwijzing van toepassing zijn op deze instellingen. Dit is geregeld in artikel 97 Cbw. Deze regeling betekent ook dat gedurende de periode van 36 maanden vanaf de aanwijzing, er ten aanzien van deze verplichtingen geen sprake is van extern toezicht in het kader van de Cbw. De hiervoor genoemde regeling geeft de instellingen de tijd om zich zorgvuldig voor te bereiden op en toe te werken naar het voldoen aan de zorgplicht uit de Cbw.

Voor de andere verplichtingen uit de Cbw, waaronder de meldplicht van significante incidenten en de registratieplicht, geldt dat die wel direct van toepassing zijn zodra de instellingen onder het toepassingsbereik van de Cbw zijn gebracht en dat op de naleving daarvan dan ook meteen extern toezicht zal plaatsvinden. Ook voor het in de Cbw geregelde recht op bijstand door een CSIRT bij dreigingen en incidenten geldt dat dit ten aanzien van de instellingen direct na aanwijzing van toepassing zal zijn.

Over bovenbedoeld besluit en het hierover gevoerde overleg met alle betrokken stakeholders is uw Kamer geïnformeerd via de eerdergenoemde brief van 24 april 2025.[28]

De regering heeft nog geen besluit genomen of de hbo- en wo-instellingen als belangrijke entiteit of als essentiële entiteit zullen worden aangewezen. Dit is onderdeel van de nadere uitwerking van het besluit om de instellingen onder de toepasselijkheid van de Cbw te brengen. De regering zal uw Kamer naar verwachting begin 2026 van de inhoud van dit besluit op de hoogte brengen.

De leden van de GroenLinks-PvdA-fractie merken op dat ziekenhuizen en zorginstellingen niet onder het toepassingsbereik van de NIS2-richtlijn vallen. Dit zijn echter cruciale organisaties die het algemene belang dienen. Biedt de NIS2-richtlijn de ruimte om ziekenhuizen en zorginstellingen standaard als essentiële of belangrijke entiteit aan te wijzen en zo ja, heeft de regering deze mogelijkheid overwogen?

Anders dan de leden van de GroenLinks-PvdA-fractie veronderstellen is de Cbw wel van toepassing op ziekenhuizen en zorginstellingen voor zover zij kwalificeren als zorgaanbieder als bedoeld in de Wet kwaliteit, klachten en geschillen in de zorg en zij voldoen aan een bepaalde omvang (de zogeheten *size cap*). De regering verwijst hierbij naar de artikelen 8, eerste lid, onderdeel f, en 12, eerste lid, onderdeel a, Cbw jo. bijlage 1 van de Cbw, waarin de hiervoor bedoelde zorgaanbieders zijn opgenomen als soort entiteit onder de sector gezondheidszorg.

De leden van de D66-fractie zijn geschokt door recente cyberaanvallen op onderwijsinstellingen. Deze leden achten het zeer noodzakelijk om de cyberveiligheid van onderwijsinstellingen te versterken. Zij vragen de regering wel om nader te motiveren waarom onderwijsinstellingen worden aangewezen onder de Cyberbeveiligingswet, terwijl dit in de richtlijn optioneel is en andere lidstaten deze keuze niet maken en welke andere opties de regering heeft overwogen om cyberveiligheid van onderwijsinstellingen te versterken.

Met de leden van de D66-fractie deelt de regering dat de toenemende digitale dreiging die ook het onderwijs raakt onverminderd zorgelijk blijft. Dit maakt de noodzaak voor een gezamenlijke, brede en duurzame aanpak om zo de cyberweerbaarheid, ook van onderwijsinstellingen, te versterken des te

[28] *Kamerstukken II* 2024/25, 31288, nr. 1189.

dringender. De regering heeft daarom besloten om de hbo- en wo-instellingen onder het toepassingsbereik van de Cbw te brengen door hen aan te wijzen als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw. Hiermee komt er onder meer een wettelijke plicht voor deze onderwijsinstellingen om op basis van een risicobeoordeling passende en evenredige maatregelen te treffen om risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen (zorgplicht), een meldplicht van significante incidenten, een registratieplicht en onafhankelijk extern toezicht op de naleving van de genoemde wettelijke verplichtingen. Door de aanwijzing hebben zij niet alleen te maken met verplichtingen, maar krijgen zij ook recht op bijstand door een CSIRT bij dreigingen en incidenten. De regering is er van overtuigd dat hiermee de cyberweerbaarheid van onderwijsinstellingen in afdoende mate wordt verhoogd.

Een andere optie die de regering heeft overwogen, is de voortzetting van het staande beleid waarbij met bestuurlijke afspraken wordt gewerkt aan de versterking van de cyberweerbaarheid. Het besluit is genomen om de hbo- en wo-instellingen als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw aan te wijzen en niet om het staande beleid voort te zetten. Dit besluit is genomen op basis van een integrale afweging van de regering, waarvoor de sectoren intensief zijn geraadpleegd en een analyse is gemaakt van de impact en het te beschermen belang van brede en duurzame beheersing van cyberrisico's. Over dit besluit en het hierover gevoerde overleg met alle betrokken stakeholders is uw Kamer geïnformeerd per brief van 24 april 2025.[29]

Anders dan waar de leden van de D66-fractie van uitgaan, maken ook andere lidstaten eenzelfde keuze en wijzen ook zij hbo- en wo-instellingen aan als belangrijke entiteit of essentiële entiteit onder de nationale wet waarin de NIS2-richtlijn is geïmplementeerd.

De leden van de D66-fractie vragen of de regering onderkent dat er al een sectorbreed systeem van bestuurlijke afspraken, audits en samenwerking via SURF bestaat, waarmee de cyberweerbaarheid van onderwijsinstellingen de afgelopen jaren is versterkt. Acht de regering het voldoende proportioneel en doeltreffend om een nieuw systeem op te tuigen in plaats van het huidige systeem te verbeteren? Deze leden vragen tevens hoe wordt voorkomen dat bestaande governance en toezichtstructuren, zoals de externe audits, de rol van de Raden van Toezicht en het toezicht conform de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW) moeten worden vervangen door nieuwe en nog niet bewezen inspectiestructuren, waardoor dubbele toezichtlagen ontstaan. Hoe verhouden nieuwe verplichtingen zich tot de bestaande verantwoordelijkheden van bestuurders en Raden van Toezicht?

Langs de bestuurlijke afspraken uit 2021 werken de onderwijsinstellingen in het vervolgonderwijs aan de verhoging van de digitale weerbaarheid.[30] Hierin zijn concrete maatregelen vastgelegd voor de versterking van de cyberweerbaarheid van deze instellingen.[31] De inhoudelijke normen in de Cbw sluiten hier voor een groot deel bij aan. De instellingen zien met intern toezicht en onafhankelijke audits toe op de voortgang en over de versterking van de cyberweerbaarheid vindt periodiek overleg plaats met het Ministerie van Onderwijs, Cultuur en Wetenschap. De regering hecht eraan te benadrukken dat met het aanwijzen van de hbo- en wo-instellingen als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw de bestaande interne governance- en toezichtstructuren van de instellingen niet hoeven te worden vervangen. De Cbw wijzigt namelijk niet de relatie tussen het instellingsbestuur en de raad van toezicht, zoals deze zijn vastgelegd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek, en laat de rol van de interne toezichthouder onverlet.

Met de aanwijzing van de hbo- en wo-instellingen als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw, komt er extern onafhankelijk toezicht op de naleving van de verplichtingen uit de Cbw door deze instellingen, inclusief bijbehorend handhavingsinstrumentarium. Dit is aanvullend op het huidige toezicht van de Inspectie van het Onderwijs.[32] De Cbw kan, naast de maatregelen die instellingen moeten nemen in het kader van de meldplicht en registratieplicht, nieuwe maatregelen van de instellingen vragen

[29] *Kamerstukken II* 2024/25, 31288, nr. 1189.

[30] *Kamerstukken II* 2021/22, 31288, nr. 922.

[31] Deze maatregelen zijn uiteengezet in de brief van 14 juli 2022 aan de Tweede Kamer (*Kamerstukken II* 2021/22, 35925 VIII, nr. 190). Over de voortgang is de Tweede Kamer geïnformeerd per brief van 24 april 2025 (*Kamerstukken II* 2024/25, 31288, nr. 1189).

als het gaat om de invulling van de zorgplicht en de monitoring en evaluatie op de genomen maatregelen. In hoeverre dit het geval is, zal afhangen van de risicobeoordeling van de individuele instelling en de mate waarin al maatregelen genomen zijn. In het kader van de nadere uitwerking van het besluit tot aanwijzing zal met betrekking tot het toezicht op de naleving van de verplichtingen in de Cbw worden bekeken op welke manier zo veel als mogelijk rekening kan worden gehouden met zowel de werkwijze van de sector zelf, als de externe audits die zij laten uitvoeren. Dit zal uiteraard samen met de Inspectie van het Onderwijs (de instantie waarvan naar verwachting de ambtenaren worden belast met dat toezicht) worden gedaan.

Om de instellingen voldoende tijd te geven om zich voor te bereiden op de toepasselijkheid van de Cbw is in het wetsvoorstel geregeld dat de zorgplicht, opgenomen in artikel 21 Cbw, en de in artikel 24 Cbw opgenomen verplichtingen over governance, vanaf 36 maanden na de aanwijzing van toepassing zijn op de aangewezen hbo- en wo-instellingen. Dit is geregeld in artikel 97 Cbw. Deze regeling betekent ook dat gedurende de periode van 36 maanden vanaf de aanwijzing, er ten aanzien van deze verplichtingen geen sprake is van extern toezicht in het kader van de Cbw. De hiervoor genoemde regeling geeft de instellingen de tijd om zich zorgvuldig voor te bereiden op en toe te werken naar het voldoen aan de zorgplicht en de verplichtingen over governance uit de Cbw. Vanuit het oogpunt van uitvoerbaarheid hecht de regering zeer aan het inbouwen van voldoende tijd voor de voorbereiding door de hbo- en wo-instellingen op de zorgplicht en verplichtingen over governance uit de Cbw. Voor de goede orde wordt hierbij benadrukt dat de andere verplichtingen uit de Cbw, zoals de meldplicht en de registratieplicht, wel direct vanaf het moment van de aanwijzing van toepassing zijn op de aangewezen instelling en dat op de naleving van deze verplichtingen vanaf datzelfde moment extern toezicht wordt gehouden. Ook geldt dat aangewezen instellingen vanaf het moment van de aanwijzing recht hebben op bijstand door een CSIRT bij dreigingen en incidenten.

Daarnaast constateren de leden van de D66-fractie dat de invoering van de Cyberbeveiligingswet voor onderwijsinstellingen aanzienlijke administratieve verplichtingen en extra kosten met zich meebrengt, terwijl de meerwaarde in termen van veiligheid ten opzichte van de huidige systematiek vooralsnog onduidelijk is. Hoe wordt geborgd dat deze lasten in verhouding staan tot de verwachte veiligheidswinst? Welke middelen stelt de regering beschikbaar om de extra uitvoerings- en financieringslasten voor instellingen en SURF op te vangen, mede gezien de structurele bezuinigingen op de onderwijsbegroting en het feit dat instellingen momenteel zelfs bijdragen aan de kosten van SURF en de Inspectie van het Onderwijs? Ook vragen deze leden hoe de regering de claim van onderwijsinstellingen beoordeelt dat de termijnen die nu gesteld zijn voor onderwijsinstellingen "volstrekt onhaalbaar" zijn.

Met de bestuurlijke afspraken uit 2021[33] ter versterking van de cyberweerbaarheid hebben de instellingen de afgelopen jaren een stevige basis opgebouwd en stappen gezet met onder meer een goede inrichting van risicomanagement. De verplichtingen uit de Cbw sluiten hier voor een groot deel op aan. Voor de uitvoering van deze bestuurlijke afspraken heeft de regering aanvullende middelen beschikbaar gesteld.

De komende periode wordt het besluit om de bekostigde hbo- en wo-instellingen als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw aan te wijzen, nader uitgewerkt. Bij de nadere uitwerking zijn onder meer de Inspectie van het Onderwijs (de instantie waarvan naar verwachting de ambtenaren door de Minister van Onderwijs, Cultuur en Wetenschap worden belast met het toezicht op de naleving van de verplichtingen uit de Cbw door aangewezen hbo- en wo-instellingen), het beoogde CSIRT (SURFcert), Universiteiten van Nederland, Vereniging Hogescholen, SURF en het Ministerie van Justitie en Veiligheid betrokken. Hierbij wordt ook nader gekeken naar welke financiële implicaties er zijn verbonden aan de uitvoering van de Cbw.[34]

---

[32] Indien door de Inspectie van het Onderwijs na gedegen onderzoek is vastgesteld dat er sprake is van wanbeheer (als bedoeld in artikel 9.9a, 10.3e en 11.7a Wet op het hoger onderwijs en wetenschappelijk onderzoek) kan de Minister van Onderwijs, Cultuur en Wetenschap overgaan tot het geven van een aanwijzing aan de raad van toezicht. Dit kan bijvoorbeeld wanneer de instelling bij een cyberincident noodzakelijke maatregelen nalaat waardoor als gevolg daarvan de continuïteit of kwaliteit van het onderwijs en onderzoek in het gedrang komt.

[33] *Kamerstukken II* 2021/22, 31288, nr. 922.

[34] Voor het toezicht op de naleving van de verplichtingen uit de Cbw door entiteiten uit de sector onderwijs en voor het CSIRT voor entiteiten in de sector onderwijs is een bedrag van € 4.800.000,- gereserveerd.

De regering neemt de zorgen die de onderwijsinstellingen hebben geuit met betrekking tot het feit dat het onder het toepassingsbereik van de Cbw brengen van deze instellingen nieuwe verplichtingen met zich meebrengt, waarop deze instellingen nog niet volledig zijn ingericht, serieus. Het is essentieel dat de instellingen voldoende tijd krijgen om zich voor te bereiden op de toepasselijkheid van de Cbw. Om die reden is in het wetsvoorstel geregeld dat de zorgplicht, opgenomen in artikel 21 Cbw, en de in artikel 24 Cbw opgenomen verplichtingen over governance, vanaf 36 maanden na de aanwijzing van toepassing zijn op de aangewezen hbo- en wo-instellingen. Dit is geregeld in artikel 97 Cbw. Deze regeling betekent ook dat gedurende de periode van 36 maanden vanaf de aanwijzing, er ten aanzien van deze verplichtingen geen sprake is van extern toezicht in het kader van de Cbw. Met deze regeling geeft de regering de instellingen nadrukkelijk de tijd om zich zorgvuldig voor te kunnen bereiden en toe te werken naar het voldoen aan de eisen die in het kader van de zorgplicht uit de Cbw aan de instellingen worden gesteld. Andere verplichtingen uit de Cbw, zoals de meldplicht van significante incidenten, zullen direct vanaf het moment van de aanwijzing van toepassing zijn op de instellingen. Op de naleving hiervan zal vanaf datzelfde moment extern toezicht plaatsvinden. Ook voor het in de Cbw geregelde recht op bijstand door een CSIRT bij dreigingen en incidenten geldt dat dit na de aanwijzing van de instellingen toepasselijk zal zijn.

Daarbij vragen de leden van de D66-fractie expliciet om te reflecteren op de indruk die in overleg met het ministerie van OCW is ontstaan dat het hoger onderwijs niet onder deze wet zou vallen en dat er door het ministerie van OCW niet is ingezet op voorbereiding voor implementatie van deze wet.

In het wetsvoorstel is, in lijn met de NIS2-richtlijn, de mogelijkheid opgenomen voor de Minister van Onderwijs, Cultuur en Wetenschap om hbo- en wo-instellingen onder de reikwijdte van de Cbw te brengen. Het Ministerie van Onderwijs, Cultuur en Wetenschap heeft de diverse stakeholders (Vereniging Hogescholen, Universiteiten van Nederland, MBO-raad, SURF en het Ministerie van Justitie en Veiligheid) veelvuldig geraadpleegd over de impact van het onder de Cbw brengen van de hbo- en wo-instellingen en hoe dit zich verhoudt tot het staande beleid om via bestuurlijke afspraken te werken aan de versterking van de cyberweerbaarheid. Daarbij zijn beide opties serieus overwogen. Het besluit om de hbo- en wo-instellingen aan te wijzen betreft uiteindelijk een besluit op basis van een integrale afweging van de regering. De regering maakt uit deze vraag van de leden van de D66-fractie op dat in het veld klaarblijkelijk de indruk is ontstaan dat het hoger onderwijs in geen geval onder de Cbw zou gaan vallen. De regering herkent zich hier niet in.

De leden van de CDA-fractie constateren dat de keuze is gemaakt om hoger onderwijsinstellingen onder het toepassingsbereik van de richtlijn te brengen. Deze leden lezen dat dit met name ziet op kritieke onderzoeksactiviteiten. Zij vragen of de regering deelt dat het per instelling en soort onderwijs (hoger beroepsonderwijs en universiteiten) verschilt in hoeverre sprake is van kritieke onderzoeksactiviteiten. De leden vragen daarom of er mogelijkheden zijn om het begrip 'onderwijsinstellingen' nader te specificeren zodat het toepassingsbereik echt gericht wordt op instellingen die kritieke onderzoeksactiviteiten verrichten. Deze leden vragen verder of de regering nader wil ingaan op de vraag wat wel en niet onder kritieke onderzoeksactiviteiten wordt verstaan. Zij vragen of inmiddels al duidelijk is of de minister van OCW gebruik zal maken van deze nieuwe bevoegdheid en wat hiervan de financiële implicaties zijn.

Overwegende de impact van de Cbw, maar ook het belang van een brede en duurzame beheersing van cyberrisico's gezien de toenemende digitale dreiging, heeft de regering besloten om de bekostigde instellingen in het hoger beroepsonderwijs en wetenschappelijk onderwijs onder de reikwijdte van de Cbw te brengen.[35] Hierbij is geen onderscheid gemaakt tussen instellingen met kritieke onderzoeksactiviteiten. De regering is het met de leden van de CDA-fractie eens dat de mate van kritieke onderzoeksactiviteiten verschilt per instelling. Gezien de samenwerking en de sterke onderlinge afhankelijkheid in het hoger beroepsonderwijs en het wetenschappelijk onderwijs acht de regering het onwenselijk om de Cbw op een deel van de instellingen toepasbaar te laten zijn. Het in dat verband nader specificeren van onderwijsinstellingen door het maken van onderscheid in mate of aard van kritieke onderzoeksactiviteiten die worden verricht, is daarnaast ook vanuit het oogpunt van uitvoerbaarheid onwenselijk. In dit verband is het ook van belang dat elke instelling op basis van een risicoafweging passende en evenredige

[35] *Kamerstukken II* 2024/25, 31288, nr. 1189.

maatregelen dient te nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen te beheersen.

De komende periode wordt het besluit om de bekostigde hbo- en wo-instellingen als belangrijke entiteit of essentiële entiteit als bedoeld in de Cbw aan te wijzen, nader uitgewerkt. Hierbij wordt ook gekeken naar welke financiële implicaties er zijn verbonden aan de uitvoering van de Cbw.

5.2. Zorgplicht

5.2.1. Inleiding

De leden van de GroenLinks-PvdA-fractie hebben begrip voor de keuze om uit te gaan van een interne risicobeoordeling. Echter, deze leden vinden de aanname dat entiteiten goed inzicht hebben in hun eigen dienstverlening en systemen te kort door de bocht. Zij vrezen dat niet alle entiteiten beschikken over de nodige IT-kennis, of dit hebben uitbesteed aan derden. Daarom vragen de leden aan de regering of er in bijzondere gevallen ook onafhankelijke risicobeoordelingen kunnen worden uitgevoerd. Heeft de regering een plan om entiteiten met onvoldoende interne IT-kennis te ontzien en de risicobeoordeling bij een onafhankelijke instantie te beleggen? Is het borgen en versterken van de IT-kennis binnen organisaties ook een doel van de NIS2-richtlijn?

Vanuit de rijksoverheid zijn verschillende tools en kennisproducten opgesteld die met name entiteiten die momenteel onvoldoende IT-kennis hebben, kunnen helpen bij het voldoen aan de vereisten uit de zorgplicht van de Cbw. Zo is op de website van het Digital Trust Center (hierna: DTC) een stappenplan te vinden die entiteiten helpt om in vier stappen hun risico's in kaart te brengen.[36] Daarnaast is in paragraaf 5.2.3 van de memorie van toelichting op het wetsvoorstel verwezen naar bestaande normenkaders, die gewoonlijk zijn gebaseerd op een internationale, Europese, nationale of sectorale norm (zoals de ISO/IEC 27000-serie) met een procesbeschrijving en eisen voor het beveiligen van netwerk- en informatiesystemen, waaronder ook een procesbeschrijving voor het verrichten van een risicoanalyse. Er zijn verschillende onafhankelijke marktpartijen die op basis van deze normenkaders entiteiten kunnen ondersteunen bij het opstellen van een risicoanalyse en het treffen van andere beveiligingsmaatregen met het oog op het voldoen aan de wettelijke vereisten. Entiteiten hebben daarmee de mogelijkheid om de risicoanalyse uit te besteden aan een derde. In dit kader wijst de regering er echter wel op dat een normenkader entiteiten houvast geeft bij het beheersen van risico's, maar dat het voldoen aan een eigen normenkader op zichzelf niet betekent dat entiteiten daarmee aan de zorgplicht van artikel 21 Cbw voldoen.

Het borgen en versterken van de IT-kennis binnen organisaties is geen op zichzelf staand doel van de NIS2-richtlijn. Wel is het zo dat wanneer entiteiten voldoen aan de verplichtingen uit de NIS2-richtlijn (in Nederland geïmplementeerd in de Cbw), dat daaruit logischerwijs zal volgen dat de cybersecuritykennis geborgd en versterkt wordt.

5.2.2. Beveiliging van netwerk- en informatiesystemen

De leden van de GroenLinks-PvdA-fractie volgen de technologieneutrale definitie van 'netwerk- en informatiesystemen.' Deze leden zetten echter een vraagteken bij de definitie van 'digitale weerbaarheid.' Is het volgens de regering te kwantificeren wanneer een entiteit voldoende digitaal weerbaar is? Zij leden vragen een heldere definitie van dit begrip.

In de NLCS is nader uitgelegd wat wordt verstaan onder digitale weerbaarheid. Daarin is toegelicht dat het bij digitale weerbaarheid gaat om het vermogen om risico's tot een aanvaardbaar niveau te brengen door middel van een verzameling van maatregelen om cyberincidenten te voorkomen en wanneer cyberincidenten zich hebben voorgedaan deze te ontdekken, schade te beperken en herstel eenvoudiger te maken. Dit betekent dat een entiteit voldoende digitaal weerbaar is als zij door middel van gedane risicoanalyses maatregelen neemt om de risico's te mitigeren en incidenten te voorkomen en gevolgen te beperken, waarmee zij voldoet aan de zorgplicht, bedoeld in artikel 21 Cbw.

[36] Zie https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse.

5.2.3. De maatregelen

De leden van de GroenLinks-PvdA-fractie moedigen het gebruik van de best beschikbare standaarden en technieken aan. Deze leden vragen de regering wel om te verhelderen hoe de effectiviteit van maatregelen wordt gemeten: is dit mede op basis van analyses van casussen waarin bepaalde maatregelen effectief een aanval of storing hebben voorkomen? Bovendien vragen zij hoe de kans op incidenten en de mogelijke maatschappelijke en economische gevolgen daarvan worden vastgesteld. Is hier een standaardmethodiek voor die voor alle sectoren van toepassing is?

Voor elke essentiële entiteit en belangrijke entiteit geldt dat zij in het kader van de wettelijke zorgplicht in elk geval de maatregelen, genoemd in artikel 21, derde lid, Cbw en nader uitgewerkt in het Cbb, moeten treffen. De concrete invulling van deze maatregelen door de entiteit zal, in relatie tot de risico's waarmee de entiteit met betrekking tot de beveiliging van de netwerk- en informatiesystemen te maken kan krijgen, op passende en evenredige wijze moeten plaatsvinden.

Bij de beoordeling door de entiteit welke specifieke maatregelen effectief en daarmee passend zijn, kan het gebruik van nationale, Europese of internationale standaarden of normenkaders behulpzaam zijn. Voorbeelden hiervan zijn onder meer ISO 27001, NEN7510 voor de sector gezondheidszorg, IEC en de Baseline Informatiebeveiliging Overheid versie 2.0 (BIO2) voor de overheid. Op de website van bijvoorbeeld de *International Organization for Standardization* (ISO) is terug te vinden hoe dergelijke normenkaders tot stand komen, namelijk door ontwikkeling door technische commissies, bestaande uit deskundigen uit bijvoorbeeld industriële, technische en zakelijke marktsegmenten die hebben gevraagd om de norm. De commissies kunnen hierbij geassisteerd worden door vertegenwoordigers van onder meer overheidsinstanties, brancheorganisaties en consumentenverenigingen. Nadat de inhoud van de nieuw ontwikkelde norm tot stand gekomen is, wordt het concept voor commentaar voorgelegd aan alle deelnemende landen, waarna definitieve goedkeuring volgt.[37]

Voor het inschatten van de risico's voor de beveiliging van de netwerk- en informatiesystemen en de kans op en ernst van incidenten, met inbegrip van maatschappelijke en economische gevolgen, bestaan er voor entiteiten standaardmethodieken die daarbij behulpzaam kunnen zijn. Een voorbeeld hiervan is ISO 31000. Naast deze standaardmethodieken kan er bijvoorbeeld ook gebruik gemaakt worden van handreikingen vanuit de rijksoverheid die op de websites van onder andere het Nationaal Cyber Security Centrum (hierna: NCSC) en het DTC zijn geplaatst. Op de website van het DTC is een stappenplan te vinden die entiteiten helpt om in vier stappen hun risico's in kaart te brengen.[38]

Ten slotte dienen essentiële entiteiten en belangrijke entiteiten rekening te houden met de stand van de techniek. Dit houdt onder andere in dat entiteiten rekening moeten houden met alle technische kennis en middelen die beschikbaar zijn, bijvoorbeeld nieuwe soorten beveiligingsmaatregelen.

De leden van de GroenLinks-PvdA-fractie vragen hoe de evenredigheid van maatregelen wordt vastgesteld. Gezien de risicobeoordeling bij entiteiten zelf wordt belegd, bestaat de kans dat evenredigheid subjectief wordt geïnterpreteerd. Welke waarborgen bouwt de regering in om ervoor te zorgen dat evenredigheid zo objectief als mogelijk wordt vastgesteld?

De vraag op welke wijze invulling moet worden gegeven aan de maatregelen in het kader van de zorgplicht (artikel 21 Cbw) is afhankelijk van de risicoanalyse die entiteiten moeten verrichten. Hieruit vloeit voort welke invulling van de maatregelen passend en evenredig is voor de betreffende entiteit. De uitkomsten van de risicoanalyse en daarmee de invulling van de genomen maatregelen én de evenredigheid ervan, zullen daarom per entiteit verschillen vanwege de specifieke en unieke kenmerken van iedere entiteit.

Het is vervolgens aan de toezichthouder om te beoordelen of de entiteit passende en evenredige maatregelen heeft genomen. Dit toezicht is risicogestuurd. Dit houdt in dat de toezichthouder per entiteit

[37] Zie voor een nadere uitleg https://isoregister.nl/informatie-over-de-iso-normen/.

[38] Zie https://www.digitaltrustcenter.nl/stappenplan-risicoanalyse.

zal beoordelen of de specifieke invulling van de maatregelen voldoet aan de zorgplicht. Hiermee wordt gewaarborgd dat de evenredigheid zo objectief als mogelijk wordt vastgesteld. De instanties waarvan de ambtenaren door de vakministers worden belast met het toezicht op de naleving van de verplichtingen uit de Cbw werken daarnaast op grond van artikel 55 Cbw zoveel mogelijk samen bij het (onderling gecoördineerd) toezicht houden op entiteiten.

De leden van de GroenLinks-PvdA-fractie zien de groeiende afhankelijkheid van een selecte groep niet-Europese techleveranciers als één van de belangrijkste dreigingen voor onze cyberveiligheid en weerbaarheid. Wordt onder de NIS2-richtlijn expliciet aandacht gevraagd voor het terugdringen van deze afhankelijkheden en het bevorderen van de strategische autonomie? Kortom, geldt het diversificeren van de eigen IT-systemen en het afbouwen van afhankelijkheden als een legitieme cyberveiligheidsmaatregel? Deze leden vragen de regering om toe te lichten hoe de NIS2-richtlijn de strategische autonomie bevordert.

In artikel 21, derde lid, Cbw zijn, ter implementatie van artikel 21, tweede lid, NIS2-richtlijn, de maatregelen opgesomd die essentiële entiteiten en belangrijke entiteiten in het kader van de wettelijke zorgplicht ten minste moeten nemen. Die maatregelen moeten op grond hiervan onder meer de beveiliging van de toeleveringsketen omvatten (zie artikel 21, derde lid, onderdeel d, Cbw). De NIS2-richtlijn erkent in overweging 90 met betrekking tot artikel 21, tweede lid, NIS2-richtlijn dat afhankelijkheden en andere niet-technische risicofactoren, zoals ongepaste beïnvloeding door derde landen, technologische lock-ins of verborgen kwetsbaarheden, een risico kunnen vormen voor de beveiliging en de weerbaarheid van netwerk- en informatiesystemen. In dat kader voorziet artikel 22 NIS2-richtlijn in gecoördineerde beveiligingsrisicobeoordelingen van kritieke toeleveringsketens door de samenwerkingsgroep, bedoeld in artikel 14 NIS2-richtlijn, de Europese Commissie en Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging). De uitkomsten van deze beoordelingen moeten door essentiële entiteiten en belangrijke entiteiten worden betrokken bij hun eigen risicobeoordeling op grond van artikel 21, vierde lid, onderdeel c, NIS2-richtlijn.

De regering ziet het in kaart brengen van en het bepalen van de omgang met dergelijke afhankelijkheden wel als een belangrijk onderdeel van de maatregelen die essentiële entiteiten en belangrijke entiteiten met betrekking tot de beveiliging van de toeleveringsketen moeten nemen. Artikel 10, eerste lid, Cbb verplicht daarom, in het kader van de nadere regeling van de zorgplicht, essentiële entiteiten en belangrijke entiteiten om in hun beleid over de beveiliging van de toeleveringsketen hun omgang te bepalen met afhankelijkheden van producten en diensten van hun leveranciers en dienstverleners die invloed kunnen hebben op de beveiliging van hun netwerk- en informatiesystemen. Zij moeten dat beleid schriftelijk vastleggen en aantoonbaar toepassen.

Hoewel hiermee niet wordt voorgeschreven dat de eerder genoemde afhankelijkheid wordt beperkt, kan uit de in artikel 21 Cbw voorgeschreven risicoanalyse blijken dat een dergelijke afhankelijkheid een te hoog risico voor de beveiliging van de netwerk- en informatiesystemen met zich brengt dat gemitigeerd moet worden. Het diversificeren van de eigen IT-systemen en het afbouwen van afhankelijkheden kunnen in dat geval passende en evenredige maatregelen zijn om dat risico te mitigeren. Dit kan bijdragen aan de strategische autonomie van de entiteit.

De leden van de D66-fractie vragen de regering om te reageren op de zorgen vanuit NLdigital en het bedrijfsleven met betrekking tot het laat toegevoegde artikel 18 van het Cyberbeveilingsbesluit, met een grondslag enkel in de memorie van toelichting, waarin de zorgplicht wordt uitgebreid en te reageren op het door hen aangedragen alternatief. Deze leden vragen daarbij hoe deze Nederlandse uitbreiding zich verhoudt tot het streven naar een Europees gelijk speelveld en welke impact de regering verwacht op het Nederlandse vestigingsklimaat voor internationale techbedrijven.

De bevoegdheid in artikel 18 Cbb betreft een uitwerking van de algemene zorgplicht van artikel 21 Cbw. De grondslag voor (onder meer) deze nadere uitwerking van de zorgplicht is opgenomen in artikel 21, vijfde lid, Cbw. Omdat het gaat om een uitwerking van genoemde wettelijke verplichting, is het niveau van een amvb passend. Voor de in artikel 18 Cbb vervatte bevoegdheid is reden gezien vanwege de mogelijke situatie dat het gebruik van producten en diensten van een specifieke leverancier door een essentiële entiteit of belangrijke entiteit risico's met zich brengt voor de beveiliging van haar netwerk- en

informatiesystemen die de nationale veiligheid raken. Met het oog daarop kan het noodzakelijk zijn om ter bescherming van de nationale veiligheid vanuit de rijksoverheid de verplichting op te leggen om die producten of diensten uit de kritieke onderdelen van genoemde systemen te weren.

Het in de vraagstelling bedoelde aangedragen alternatief betreft de regeling die in Duitsland is getroffen. De Duitse regeling bevat verschillende elementen die ook deel uitmaken van artikel 18 Cbb (bijvoorbeeld het weren van producten of diensten alleen in kritieke onderdelen en een overgangsfase in verband met de continuïteit van de dienstverlening), maar bevat tegelijk ook elementen die extra uitvoeringslasten opleveren. Voor de in artikel 18 Cbb opgenomen bevoegdheid geldt dat het een maatregel betreft die ter uitwerking van de zorgplicht in de NIS2-richtlijn in nationale wetgeving kan worden geregeld. Mede omdat de inzet van deze bevoegdheid alleen kan plaatsvinden als dat noodzakelijk is ter voorkoming van anders onbeheersbare risico's voor de beveiliging van de netwerk- en informatiesystemen die nadrukkelijk de nationale veiligheid raken, wordt niet verwacht dat dit een negatieve impact zal hebben op het Nederlandse vestigingsklimaat voor bedrijven.

5.3. Governance

5.3.1. Inleiding

De leden van de GroenLinks-PvdA-fractie vinden het essentieel dat bestuursleden van entiteiten doordrongen zijn van het belang van cyberveiligheid. Deze leden constateren echter dat er in veel instanties te weinig interne kennis en kunde is op het gebied van IT, wat bestuurlijk overleg over cyberveiligheid bemoeilijkt. Zij wijzen op het nut van een 'cyberjaarverslag,' een gestandaardiseerd jaarlijks inzicht in de stand van de IT en het voldoen aan digitale wetgeving. De leden vragen de regering om de aangenomen motie van het lid Kathmann (Kamerstuk 26643, nr.1342), die oproept om het invoeren van een cyberjaarverslag te verkennen, te betrekken bij de implementatie van de Cyberbeveiligingswet. Zij menen dat het cyberjaarverslag bijdraagt aan een beter en bruikbaar inzicht in de IT voor bestuurders van organisaties.

De regering deelt de opvatting van de leden van de GroenLinks-PvdA-fractie dat het van groot belang is dat bestuurders over voldoende inzicht beschikken in de staat van de IT-beheersing en de mate waarin organisaties voldoen aan wet- en regelgeving daaromtrent. Een gestandaardiseerd jaarverslag kan hierin een belangrijke ondersteunende rol vervullen, doordat het bestuurders in staat stelt beter geïnformeerd het gesprek over IT-beheersing te voeren en gerichte keuzes te maken.

Als reactie op de genoemde motie van het lid Kathmann zijn het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Economische Zaken gestart met de voorbereiding van een verkenning naar de mogelijkheden van een IT-jaarverslag op basis van de Internationale Digitale Rapportage Standaard (IDRS). Bij de opzet van deze verkenning wordt aangesloten bij bestaande trajecten en ervaringen. De verkenning heeft als doel het verbeteren van de IT-beheersing en het verminderen van de administratieve lasten. In de verkenning wordt expliciet meegenomen hoe een IT-jaarverslag kan aansluiten bij relevante wetgeving, waaronder de implementatie van de Cbw. Uw Kamer zal via de Verzamelbrief Digitalisering periodiek worden geïnformeerd over de voortgang van de uitvoering van de motie van het lid Kathmann.

5.3.2. Training

De leden van de GroenLinks-PvdA-fractie prijzen de inzet op het trainen van bestuurders. Deze leden vragen de regering of zij een verkenning heeft uitgevoerd of er voldoende cursusaanbieders en -materiaal beschikbaar is om te voldoen aan deze bepaling. Aan welke organisatie of toezichthouder moeten bestuurders aantonen dat zij deze trainingen hebben gevolgd en hun certificaten vernieuwen?

De regering heeft een dergelijke verkenning niet uitgevoerd, aangezien bekend is dat er voldoende (externe) cursusaanbieders zijn in de cyberbeveiligingssector die dergelijke trainingen kunnen aanbieden. Tegelijk houdt de regering ook ruimte voor entiteiten om zelf intern een geschikte opleiding te verzorgen. De leden van het bestuur moeten aan de bevoegde autoriteit van de sector waar de entiteit onder valt kunnen aantonen dat zij de verplichtingen uit artikel 24 Cbw naleven.

5.3.3. Normadressaat

5.3.3.1 Bestuur van essentiële entiteiten en belangrijke entiteiten, niet zijnde overheidsinstanties

De leden van de GroenLinks-PvdA-fractie begrijpen de keuze om beveiligingsmaatregelen alleen met goedkeuring van het dagelijks bestuur te laten vaststellen en om alle bestuursleden te laten voldoen aan de opleidingsverplichting. De kennis over IT en cyberveiligheid dient breed gedragen te worden. Het risico bestaat echter dat de brede opleidingsverplichting de kennis kan verwateren. Biedt de NIS2-richtlijn de kans voor besturen om één bestuurslid als eindverantwoordelijke op het gebied van IT en cyberveiligheid aan te wijzen, zodat deze beschikt over diepere specialistische kennis, in plaats van dat alle bestuursleden enkel over algemene kennis beschikken? Deze leden zijn benieuwd of de regering deze benadering heeft overwogen.

De regering heeft bezien of artikel 20, tweede lid, NIS2-richtlijn ook volledig kan worden geïmplementeerd als in nationale wetgeving wordt opgenomen dat de opleidingsverplichting enkel voor één lid van het bestuur geldt. De regering heeft geconstateerd dat dat niet kan, omdat artikel 20, tweede lid, NIS2-richtlijn de lidstaten van de Europese Unie niet de ruimte biedt om ervoor te kiezen dat de bedoelde opleidingsverplichting enkel geldt voor één lid van het bestuur. Deze bepaling gaat uit van “de leden van de bestuursorganen” en daarmee wordt dus het voltallige bestuur bedoeld. Los van dat het niet mogelijk is om te regelen dat de opleidingsverplichting alleen van toepassing is op één lid van het bestuur, is het ook niet wenselijk om dat te regelen als dat wél mogelijk was geweest. Bestuursleden spelen immers een cruciale rol in het neerzetten van een sterke cyberweerbaarheidscultuur en moeten vanuit hun voorbeeldfunctie cyberbewustheid uitdragen. Uiteraard kan er wel voor gekozen worden om voor het bestuur een opleiding aan te bieden die voldoet aan de eisen van de Cbw en daarnaast een bestuurslid, wiens aandachtsgebied binnen de bedrijfsvoering cybersecurity is, een verdieping hierop te laten volgen.

5.3.3.2 Bestuur van overheidsinstanties

De leden van de GroenLinks-PvdA-fractie missen in de rolverdeling binnen overheidsorganisaties duidelijkheid over de rol van de volksvertegenwoordiging. Gemeenten, provincies en het Rijk hebben immers verantwoording af te leggen aan de controlerende macht. Deze leden vragen de regering daarom om toe te lichten op welke wijze de volksvertegenwoordiging dient te worden geïnformeerd (al dan niet vertrouwelijk) over de maatregelen die volgen uit de NIS2-richtlijn. Zij benadrukken het belang van transparantie en medezeggenschap over politieke keuzes inzake digitalisering en cyberveiligheid. Op welke manier kunnen raadsleden, Statenleden en Kamerleden de genomen maatregelen controleren en (bij)sturen?

Het klopt dat de besturen van de overheidsinstanties die onder het toepassingsbereik van de Cbw vallen, verantwoording moeten afleggen aan volksvertegenwoordigende organen. Dit is voor cyberveiligheid in het algemeen en de uitvoering van de Cbw in het bijzonder niet anders dan voor andere beleidsterreinen. Het is aan de volksvertegenwoordigende organen zelf om te bepalen op welke manier en met welke frequentie zij willen worden geïnformeerd. Raadsleden, Statenleden en Kamerleden kunnen daarover afspraken maken met de besturen. Ook kunnen zij gebruikmaken van bestaande instrumenten waarmee zij de besturen om inlichtingen kunnen vragen en ter verantwoording kunnen roepen. De besturen zijn op hun beurt, net als op andere beleidsterreinen, gehouden om de volksvertegenwoordigende organen zo nodig actief te informeren over cyberveiligheid.

5.4. Meldplicht

De leden van de GroenLinks-PvdA-fractie vragen de regering om een overzicht van alle (beoogde) sectorale Computer Security Incident Response Teams (CSIRT’s) die volgen uit de NIS2-richtlijn.

Op dit moment is het voornemen om de volgende organisaties als CSIRT aan te wijzen: Z-CERT voor entiteiten uit de sector gezondheidszorg en de subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, het CERT Watermanagement (onderdeel van het openbaar lichaam Het Waterschapshuis) voor de waterschappen, de Informatiebeveiligingsdienst (IBD, onderdeel van VNG Realisatie B.V.) voor gemeenten, SURFcert voor hoger onderwijsinstellingen die zijn

aangewezen als essentiële entiteit of belangrijke entiteit en het NCSC voor wat betreft alle andere essentiële entiteiten en belangrijke entiteiten.

De leden van de GroenLinks-PvdA-fractie zijn van mening dat melden van incidenten, groot en klein, zo veel als mogelijk gestimuleerd moeten worden. Deze leden vragen daarom of de meldplicht bij significante incidenten niet als nadeel heeft dat kleine incidenten, die alsnog grote gevolgen blijken te hebben, niet (op tijd) worden gemeld. Heeft de regering overwogen om de meldplicht te verbreden of de drempelwaarden te verlagen? Zij ontvangen graag meer informatie over deze afweging en hoe mogelijke alternatieve invullingen van de meldplicht zijn ontvangen door de betrokken sectoren. De leden ontvangen daarnaast graag, wanneer dat beschikbaar is, informatie over de vastgestelde drempelwaarden per sector. Hoe komen deze drempelwaarden tot stand en wat voor overleg gaat hieraan vooraf met belanghebbenden? Deze leden achten het van belang dat deze waarden en de afweging hiervan openbaar en controleerbaar zijn.

Essentiële entiteiten en belangrijke entiteiten moeten op grond van artikel 25, eerste lid, Cbw alle significante incidenten melden. In artikel 25, tweede lid, Cbw is bepaald dat een incident een significant incident is als het een ernstige operationele verstoring van de diensten of financiële verliezen voor de betrokken entiteit veroorzaakt of kan veroorzaken, of andere entiteiten heeft getroffen of kan treffen door aanzienlijke materiële of immateriële schade te veroorzaken.

Bij de implementatie van de NIS2-richtlijn in nationale wetgeving is de regering, indachtig het kabinetsbeleid dat er geen nationale koppen komen op Europese regelgeving, binnen de kaders van de door de NIS2-richtlijn voorgeschreven meldplicht gebleven. Van een nationale kop is sprake als Nederland bij de omzetting van Europese regelgeving verder gaat dan strikt genomen op grond van de Europese regelgeving noodzakelijk is.

De criteria op basis waarvan wordt bepaald of sprake is van een significant incident worden bij regeling of besluit van de vakminister vastgesteld (zie artikel 25, derde lid, Cbw jo. artikel 24, eerste lid, Cbb). Deze criteria worden ook wel drempelwaarden genoemd. Voor zover het gaat om de vaststelling van die drempelwaarden bij ministeriële regeling, geldt dat de concepten hiervan met bijbehorende toelichting zullen worden geconsulteerd.

De leden van de GroenLinks-PvdA-fractie vinden het onduidelijk waarom de regering enkel streeft naar het invoeren van een dubbele meldplicht aan het CSIRT die slechts één handeling van de betrokken entiteit vergt. Waarom is dit een streven en geen doel? Graag een toelichting over welke drempels er in de weg staan om dit technisch zo in te richten dat één handeling afdoende is.

Op dit moment is er een meldportaal ontwikkeld waarmee met één handeling kan worden voldaan aan de dubbele meldplicht. Het meldportaal wordt beheerd en onderhouden door het NCSC en alle entiteiten uit alle sectoren moeten hierin hun meldingen doen. Dit meldportaal zal bij de inwerkingtreding van de Cbw beschikbaar zijn.

De leden van de CDA-fractie constateren dat voor essentiële entiteiten en belangrijke entiteiten een dubbele meldplicht geldt. Deze leden vragen of de regering kan garanderen dat voor deze entiteiten een centraal loket wordt ingericht, direct vanaf het moment dat de wet in werking treedt, zodat entiteiten niet met onnodige lasten worden opgezadeld.

Op dit moment is er een meldportaal ontwikkeld waarmee met één handeling kan worden voldaan aan de dubbele meldplicht. Het meldportaal wordt beheerd en onderhouden door het NCSC en alle entiteiten uit alle sectoren moeten hierin hun meldingen doen. Dit meldportaal zal bij de inwerkingtreding van de Cbw beschikbaar zijn.

De leden van de CDA-fractie vragen ook of de regering nader wil ingaan op de gevolgen in de praktijk van de nieuwe meldplicht. Deze leden vragen of de regering kan inschatten hoeveel extra meldingen zullen worden gedaan als gevolg van de nieuwe meldplicht. Ook vragen zij of de CSIRT's en toezichthoudende instanties in staat zijn een toename van meldingen te behandelen, en welke keuzes daarin worden gemaakt.

Uit een eerdere grove schatting komt naar voren dat er circa 1.000 incidenten per jaar onder de meldplicht van de Cbw zouden kunnen vallen. Hierbij wordt wel nadrukkelijk aangetekend dat een betrouwbare schatting van dit aantal op basis van de bestaande uitvoeringspraktijk niet mogelijk is. Dit heeft onder andere te maken met nieuwe sectoren waarmee nog geen ervaring is vanuit de CSIRT's, de snelle ontwikkeling van het (cyber)dreigingslandschap, de ontwikkeling van de weerbaarheid (bijvoorbeeld dankzij de zorgplicht uit de Cbw) en het nog ontbreken van de drempelwaarden voor incidenten die onder de meldplicht zullen vallen.

Het NCSC bereidt zich – als één van de CSIRT's onder de Cbw – hier op voor door onder meer in te zetten op automatisering en schaalbaarheid van de dienstverlening. Indien het NCSC tegelijkertijd veel meldingen ontvangt vindt er een nadere prioritering plaats, waartoe artikel 16, vierde lid, Cbw ruimte biedt. Andere CSIRT's worden momenteel verder uitgerust om hun taken onder de Cbw te kunnen uitvoeren. Zodra bij hen veel meldingen (via het centrale meldloket) tegelijkertijd plaatsvinden zullen ook zij gaan prioriteren. Daarnaast kunnen CSIRT's elkaar – indien dit bij meldingen noodzakelijk blijkt – bijstaan, zoals voorgeschreven in artikel 51, eerste lid, Cbw. Ook de instanties waarvan de ambtenaren door de vakministers worden belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw zullen bij een groot aantal gelijktijdige meldingen gaan prioriteren.

5.5. CSIRT

5.5.1. Aanwijzing CSIRT's

De leden van de GroenLinks-PvdA-fractie vragen de regering om helder uit te leggen hoe de structuur van een CSIRT er in de praktijk uit zal zien. Deze leden vragen de regering om in duidelijke taal uit te leggen over welke capaciteit, structuur en kennis een CSIRT zal moeten beschikken.

Een CSIRT moet voldoen aan de eisen die zijn opgenomen in artikel 11, eerste lid, NIS2-richtlijn. Op grond van die bepaling moet een CSIRT onder meer een hoge mate van beschikbaarheid van haar communicatiekanalen garanderen door zwakke punten te voorkomen, uitgerust zijn met een adequaat systeem voor het beheren en routeren van verzoeken en de vertrouwelijkheid en betrouwbaarheid van haar activiteiten waarborgen.

Een CSIRT heeft de taken die zijn opgenomen in artikel 11, derde lid, NIS2-richtlijn. Op grond van die bepaling heeft een CSIRT onder meer de taak om cyberdreigingen, kwetsbaarheden en incidenten te monitoren en te analyseren en de taak om vroegtijdige waarschuwingen, meldingen en aankondigingen te verstrekken over cyberdreigingen, kwetsbaarheden en incidenten.

De NIS2-richtlijn bevat geen voorschriften over de structuur van een CSIRT.

Beleidsmatig is afgesproken dat alle CSIRT's voor het invullen van de hiervoor bedoelde eisen en het uitvoeren van de hiervoor bedoelde taken, het internationaal breed gebruikte *Security Incident Management Maturity Model (SIM 3) framework* hanteren op het niveau *intermediate* zoals omschreven door Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging). Dit is een gestandaardiseerd model om op een gestructureerde wijze de volwassenheid van een CSIRT te beoordelen en stimuleert daarbij ook tot continue verbeteringen.

Het is aan de vakminister om het CSIRT uit te rusten met voldoende capaciteit en middelen voor het uitvoeren van de taken. De omvang en aard van deze capaciteit en middelen is afhankelijk van de sector die de desbetreffende CSIRT moet bedienen.

5.5.2. Verwerking van gegevens door het CSIRT

De leden van de GroenLinks-PvdA-fractie erkennen het belang van een snelle en volledige informatie-uitwisseling door CSIRT's. Deze organisaties kunnen enkel hun werk uitvoeren door te beschikken over belangrijke en gevoelige data. Dat roept bij deze leden de vraag op of CSIRT's zelf ook niet moeten voldoen aan relevante cyberveiligheidseisen, zoals voorgeschreven aan entiteiten die onder de NIS2-richtlijn vallen. Als het CSIRT

platligt, heeft dat immers ook gevolgen voor de digitale weerbaarheid. Hoe wordt de cyberveiligheid van CSIRT's gewaarborgd en wie ziet daarop toe?

In artikel 11, eerste lid, NIS2-richtlijn is bepaald aan welke eisen een CSIRT moet voldoen. Een organisatie kan alleen worden aangewezen als CSIRT als zij voldoet aan al die eisen. Eén van de eisen is dat de organisatie de vertrouwelijkheid en betrouwbaarheid van haar activiteiten waarborgt. Hiermee wordt de cyberveiligheid van een CSIRT gewaarborgd.

Het is de verantwoordelijkheid van de vakminister om ervoor te zorgen dat een CSIRT adequaat is uitgerust. Voor het NCSC is dat de Minister van Justitie en Veiligheid in afstemming met de vakminister.

Overigens kan het zijn dat een aangewezen CSIRT zelf een essentiële entiteit als bedoeld in de Cbw is, en daarmee onder het toezicht in het kader van de Cbw valt. Ook hebben enkele inspecties, zoals de Inspectie Justitie en Veiligheid in relatie tot het NCSC, de mogelijkheid om zelfstandig onderzoek te doen naar de kwaliteit van de taakuitvoering door een CSIRT.

5.5.3. Rol NCSC

De leden van de GroenLinks-PvdA-fractie vragen de regering om te specificeren welk 'groot deel van de entiteiten die onder het toepassingsbereik van de Cyberbeveiligingswet vallen' vermoedelijk onder het Nationaal Cyber Security Centrum (NCSC) zal vallen als nationale CSIRT.

Op dit moment is het voornemen om de volgende organisaties als CSIRT aan te wijzen: Z-CERT voor entiteiten uit de sector gezondheidszorg en de subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek, het CERT Watermanagement (onderdeel van het openbaar lichaam Het Waterschapshuis) voor de waterschappen, de Informatiebeveiligingsdienst (IBD, onderdeel van VNG Realisatie B.V.) voor gemeenten, SURFcert voor hoger onderwijsinstellingen die zijn aangewezen als essentiële entiteit of belangrijke entiteit en het NCSC voor wat betreft alle andere essentiële entiteiten en belangrijke entiteiten. Dit betekent dat voor alle essentiële entiteiten en belangrijke entiteiten die niet onder de sector gezondheidszorg vallen of die geen waterschap, gemeente of hoger onderwijsinstelling zijn, het NCSC hun CSIRT zal zijn. Het gaat hierbij om circa 90% van de entiteiten die onder het toepassingsbereik van de Cbw vallen.

De leden van de D66-fractie vragen of de regering kan reageren op de behoefte vanuit G4 gemeenten waarbij burgemeesters rechtstreeks gegevens van het NCSC kunnen ontvangen, omdat zij die gegevens nodig achten om de lokale impact van cyberdreigingen en veiligheidsincidenten te kunnen duiden. Kan de regering toelichten of, en zo ja, welke mogelijkheden voor zulke gegevensdeling reeds bestaan in bestaande wet- en regelgeving? Of moet er in de Cyberbeveiligingswet een expliciete wettelijke grondslag worden opgenomen?

Voor de gemeenten is het voornemen om de Informatiebeveiligingsdienst (IBD, onderdeel van VNG Realisatie B.V.) aan te wijzen als hun CSIRT. Alle CSIRT's hebben op grond van artikel 16, tweede lid, onderdeel b, Cbw onder meer de taak om informatie te verspreiden aan de betrokken essentiële entiteit of belangrijke entiteit. Dit betekent dus dat gemeenten, en daarmee ook de G4-gemeenten, via de IBD informatie zullen ontvangen die relevant wordt geacht voor hun cyberveiligheid. Het NCSC fungeert als centraal informatieknooppunt en zorgt ervoor dat relevante cyberinformatie bij de IBD terecht komt.

De behoefte van de G4-gemeenten is echter om daarnaast informatie van alle organisaties binnen gemeentegrenzen rechtstreeks van het NCSC te kunnen ontvangen om de lokale impact op de openbare orde en veiligheid van cyberdreigingen binnen de gemeentegrenzen te kunnen duiden. Met de G4-gemeenten is gesproken over de wettelijke grondslag hiertoe in de Cbw na het ontvangen van hun consultatiereactie op het wetsvoorstel. De Cbw biedt hier geen grondslag voor.

Het verzoek van de G4-gemeenten gaat breder en vraagt nadere uitwerking. Deze nadere uitwerking is reeds onderdeel van het Bestuurlijk convenant digitale veiligheid gemeenten. Dit convenant is in 2022 is gesloten tussen de Staatssecretaris van Koninkrijksrelaties en Digitalisering, de Minister van Justitie en Veiligheid en de voorzitter van de Vereniging van Nederlandse Gemeenten (VNG). Ter uitwerking van dit

convenant is de afgelopen tijd nader onderzoek uitgevoerd, wat net als de behoefte geuit door de G4-gemeenten in hun consultatiereactie, ingaat op rollen, taken en verantwoordelijkheden in verschillende incidenttypes. Op dit moment wordt dit onderzoek afgerond en kijken de betrokken partijen naar mogelijke vervolgacties. Een uitwerking van de door de leden van de D66-fractie genoemde behoefte van de G4-gemeenten is hier onderdeel van. Dit onderzoek neemt niet weg dat de Cbw geen ruimte biedt voor het (door)delen van informatie die niet ziet op de eigen cyberveiligheid van de gemeenten.

Tot slot merkt de regering op dat een CSIRT, daarmee ook het NCSC, soms pas op de hoogte is van cyberdreigingen nadat zij hiervan een melding heeft gekregen. Dit kan oplopen tot 72 uur na een cyberincident. Dit betekent concreet dat het goed mogelijk is dat een gemeente zelf eerder op de hoogte is van de lokale impact van een cyberdreiging of veiligheidsincident.

5.5.4. Samenwerking tussen CSIRT's

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen hoe en waar de samenwerkingsprotocollen tussen CSIRT's worden gepubliceerd. Deze leden hechten belang aan het openbaar maken van deze protocollen.

De samenwerkingsprotocollen zullen in ieder geval op de website van het NCSC worden gepubliceerd, met uitzondering van de eventuele technische afspraken die zien op de veilige uitwisseling van informatie tussen de CSIRT's.

5.6. Handhaving

5.6.1. Handhaving van verplichtingen uit Cbw, uitvoeringshandelingen en gedelegeerde handelingen

De leden van de GroenLinks-PvdA-fractie zijn van mening dat het nog onduidelijk is wanneer er sprake is van 'effectief toezicht' zoals bedoeld in artikel 32 van de NIS2-richtlijn. Deze leden vragen de regering om dit te definiëren. Daarnaast vragen zij aan de regering om duidelijk te maken wanneer geldboeten aan een entiteit zouden worden opgelegd. Wat gebeurt er met de inkomsten uit boetes die worden opgelegd aan entiteiten? Volgens de leden van de moet de regering overwegen om deze boetes standaard terug te investeren in de cyberveiligheid van Nederland. Zij horen graag de reactie van de regering.

De verplichting voor de lidstaten van de Europese Unie om ervoor te zorgen dat hun bevoegde autoriteiten effectief toezicht houden op de naleving van de NIS2-richtlijn is opgenomen in artikel 31, eerste lid, NIS2-richtlijn. In artikel 31, tweede tot en met vierde lid, NIS2-richtlijn worden een aantal aspecten van effectief toezicht benoemd. Hierbij gaat het om het kunnen prioriteren van toezichtstaken, gebaseerd op een risicogebaseerde benadering, de samenwerking met toezichthoudende autoriteiten uit hoofde van de Avg bij de aanpak van incidenten die leiden tot inbreuken in verband met persoonsgegevens, evenals de beschikking over passende bevoegdheden en de operationele onafhankelijkheid in het kader van het toezicht op overheidsinstanties. De bevoegdheden om effectief toezicht te kunnen houden zijn in de Cbw uitgewerkt in de artikelen 68 tot en met 93. Effectief toezicht en handhaving zorgt onder meer ervoor dat organisaties conform hun wettelijke verplichtingen onder de Cbw hun cyberrisico's beheersen, incidenten voorkomen en gevolgen ervan beperken en significante incidenten melden. Dit in het bijzonder met het oog op het in stand houden van kritieke maatschappelijke of economisch belangrijke functies of activiteiten.

Het opleggen van bestuurlijke boetes is als volgt ingekaderd. Artikel 69 Cbw geeft het algemene afwegingskader voor de bevoegde autoriteit (de vakminister) voor het opleggen van sancties, waaronder een bestuurlijke boete. Deze vereisten vloeien voort uit de artikelen 32 en 33 NIS2-richtlijn. Daarnaast gelden de algemene regels voor het opleggen van bestuurlijke boetes zoals vastgelegd in de Awb. Ten slotte kan een boetebeleid en kunnen beleidsregels worden vastgesteld voor het opleggen van boetes waarin nader staat gespecificeerd in welke situaties tot een boete wordt overgegaan en welke hoogte deze boete gegeven die situatie heeft. In artikel 1:1, vierde lid, Awb is bepaald dat de vermogensrechtelijke gevolgen van een handeling van een bestuursorgaan de rechtspersoon treffen waartoe het bestuursorgaan behoort. Omdat de vakministers zijn aangewezen als bevoegde autoriteit, zullen de

bestuurlijke boetes toekomen aan de Staat. Deze inkomsten worden niet specifiek gereserveerd voor het herinvesteren in de cyberveiligheid van Nederland.

5.6.2. Bestuursrechtelijke handhaving

5.6.3. Differentiatie in het toezicht

De leden van de GroenLinks-PvdA-fractie hebben begrip voor het aanbrengen van differentiatie in toezicht op verschillende sectoren. Wel waken deze leden ervoor dat dit niet mag leiden tot een feitelijk betere of slechtere mate van toezicht, afhankelijk van sectoren. Zij vragen de regering hoe dit risico wordt voorkomen.

In artikel 15, eerste tot en met vijfde lid, Cbw zijn de vakministers aangewezen als de bevoegde autoriteit voor de entiteiten die onder het toepassingsbereik van de Cbw vallen. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw.[39] De vakministers wijzen bij besluit de ambtenaren aan die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[40] Daarbij zal het gaan om de aanwijzing van ambtenaren van onder meer de rijksinspecties ILT, RDI, Inspectie van het Onderwijs, IGJ en NVWA. In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister).

Sinds de komst van de Wbni in 2019 werken de toezichthoudende (ambtenaren van) instanties op cybersecurity van vitale processen samen in het Samenwerkend Toezicht Digitale Weerbaarheid (STDW). Met de aanstaande komst van de Cbw en Wwke heeft de RDI het initiatief genomen de samenwerking te intensiveren en is dit in de vorm van een directeurenoverleg (DTWD) opgericht. Het DTDW richt zich op de uitvoering van effectief toezicht op de (digitale) weerbaarheid.

In het STDW en DTDW werken de volgende instanties samen:
- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Autoriteit persoonsgegevens (AP)
- De Nederlandsche Bank (DNB)
- Inspectie Gezondheidszorg en Jeugd (IGJ)
- Inspectie Leefomgeving en Transport (ILT)
- Inspectie Justitie en Veiligheid (Inspectie JenV)
- Inspectie van het Onderwijs (IvhO)
- Nederlandse Voedsel- en Warenautoriteit (NVWA)
- Rijksinspectie Digitale Infrastructuur (RDI)
- Staatstoezicht op de Mijnen (SodM)

Zij werken aan een werkplan met ambities op verschillende gebieden.[41] Zo wordt er bijvoorbeeld gewerkt aan de harmonisatie van de wijze waarop risicogestuurd toezicht vorm kan krijgen, de wijze waarop op naleving wordt getoetst en de wijze van interventies, zodat op gelijkwaardige wijze wordt omgaan met entiteiten. Hierdoor ontstaat een consistente toezichtspraktijk en ontstaat er meer duidelijkheid over toezicht voor entiteiten die aan de Cbw (en/of Wwke) moeten voldoen, in het bijzonder als zij te maken hebben met toezichthoudende ambtenaren van meerdere instanties. De intensivering van de samenwerking staat daarbij overigens niet in de weg aan een sectorale aanpak van deze instanties.

[39] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 15, zesde lid, onderdeel b, Cbw.

[40] Artikel 5:11 Awb spreekt in deze context over “toezichthouder”.

[41] Zie ook dit nieuwsbericht hierover: https://www.rijksinspecties.nl/actueel/nieuws/2025/04/07/toezichthouders-werken-samen-aan-versterken-digitale-weerbaarheid.

De hiervoor genoemde instanties zijn overeengekomen om samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Hierin wordt onder meer vastgelegd wanneer zij informatie kunnen uitwisselen binnen de grondslag van wetgeving en hoe wordt omgegaan met overlap in het toezicht waarbij een entiteit te maken heeft met toezichthoudende ambtenaren van meerdere instanties. Op deze wijze wordt geborgd dat verschillen in sectorale context niet tot te grote verschillen in mate van toezicht leiden, dat gelijkwaardig toezicht op alle entiteiten wordt geborgd en dat onnodige toezichtslasten worden voorkomen.

5.6.4. Handhavingsinstrumentarium

De leden van de GroenLinks-PvdA-fractie vragen de regering om duidelijk te maken welke eisen er worden gesteld aan de onafhankelijke organisaties die beveiligingsscans en audits uitvoeren bij essentiële en belangrijke entiteiten. Deze leden wijzen erop dat de organisaties die deze onderzoeken doen betrouwbaar moeten zijn. Is het uitgesloten dat niet-Europese organisaties deze onderzoeken uitvoeren? Gezien de gevoeligheid van de onderzoeken achten deze leden dit wenselijk. Bovendien vragen zij of de methodiek voor audits en scans wordt gestandaardiseerd, en zo ja, volgens welke standaardmethodiek deze plaatsvinden.

De Cbw stelt als eis dat wanneer de bevoegde autoriteit een beveiligingsscan of beveiligingsaudit door een derde partij laat uitvoeren, dat deze partij een onafhankelijke en gekwalificeerde deskundige dient te zijn. De Cbw stelt geen expliciete eisen aan de betrouwbaarheid van de betreffende partij, of de eis dat dit uitsluitend Europese organisaties mogen zijn. De afwegingen en het maken van passende keuzes daarover liggen bij de bevoegde autoriteit die besluit tot het inzetten van de betreffende bevoegdheid tot het laten uitvoeren van een beveiligingsscan of beveiligingsaudit. Het object van onderzoek van beveiligingsscans en beveiligingsaudits wordt risicogebaseerd vastgesteld door de bevoegde autoriteit. Voor de uitvoering ervan zal worden aangesloten bij internationale standaarden en beste praktijken die passen bij het doel van de betreffende beveiligingsscan of beveiligingsaudit. Aangezien de doelen van een beveiligingsscan of beveiligingsaudit sterk uiteen kunnen lopen, van het beoordelen van managementsystemen tot beveiligingstesten op specifieke technologie, is het niet wenselijk om dit *a priori* te standaardiseren.

De leden van de CDA-fractie constateren dat de Raad van State heeft geadviseerd om in kaart te brengen welke zelfstandige bestuursorganen (zbo's) belast zijn met toezichts- en handhavingstaken gericht op veiligheid, en om in de toelichting aan te geven hoe wordt voorkomen dat de uitoefening van deze taken in de praktijk tot problemen leidt, doordat zij overlapt met taken die zijn toebedeeld via het wetsvoorstel. Deze leden vragen of de regering alsnog specifiek wil ingaan op dit punt en ook om dit overzicht te delen.

In artikel 15, eerste tot en met vijfde lid, Cbw zijn de vakministers aangewezen als de bevoegde autoriteit voor de entiteiten die onder het toepassingsbereik van de Cbw vallen. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw.[42] De vakministers wijzen bij besluit de ambtenaren aan die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[43] Daarbij zal het gaan om de aanwijzing van ambtenaren van onder meer de rijksinspecties ILT, RDI, Inspectie van het Onderwijs, IGJ en NVWA. Voor wat betreft het zelfstandig bestuursorgaan ANVS geldt dat de Minister van Infrastructuur en Waterstaat het voornemen heeft om de toezichts- en handhavingstaken uit de Cbw aan de ANVS te mandateren. In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister).

Voor de ambtenaren van de rijksinspecties en de zelfstandige bestuursorganen geldt dat overlap kan bestaan in het toezicht in het kader van de Cbw en andere wetgeving. Bij de sectoren waar dat van toepassing is, vindt afstemming tussen (de ambtenaren van) die instanties plaats en worden

[42] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 15, zesde lid, onderdeel b, Cbw.

[43] Artikel 5:11 Awb spreekt in deze context over "toezichthouder".

samenwerkingsafspraken gemaakt. Doel is om zoveel mogelijk te voorkomen dat er ambtenaren van verschillende instanties overlappende toezichtsactiviteiten uitvoeren bij dezelfde entiteiten, wat een hogere administratieve last geeft.

5.6.5. Bepalen einddatum, verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur

5.6.5.1 Implementatie van artikel 32, vijfde lid, NIS2-richtlijn

De leden van de GroenLinks-PvdA-fractie vragen om een nadere onderbouwing welke organisaties bedoeld worden met 'certificerings- of vergunningsinstanties.'

Met certificeringsinstanties wordt bedoeld: een instantie die een certificaat afgeeft. Hierbij kan onder meer worden gedacht aan certificeringsinstanties die geaccrediteerd zijn om ISO-certificeringen af te geven.

Een vergunningsinstantie is een instantie die een vergunning mag afgeven. Een vergunning is een beschikking van een bestuursorgaan die bepaalde activiteiten of handelingen toestaat, die zonder deze beschikking niet zijn toegestaan. Een voorbeeld van een instantie die (onder meer) vergunningen afgeeft, is de ILT.

5.6.5.2 Bepaling einddatum door toezichthoudende instantie

De leden van de GroenLinks-PvdA-fractie vinden het van belang dat het vaststellen van een einddatum, waarop maatregelen getroffen moeten zijn om overtredingen te voorkomen, op een transparante wijze gebeurt. Kan de regering toelichten hoe toezichthoudende instanties geacht worden deze einddatum vast te stellen, en aan welke instantie zij dit moeten motiveren? Wordt hiervoor een afwegingskader per sectorale toezichthouder opgesteld, al dan niet in samenspraak met betrokken entiteiten? Deze leden benadrukken dat sancties en ingrepen als doel moeten hebben om de cyberveiligheid feitelijk te verbeteren. Het is dus wenselijk dat entiteiten niet verrast worden door handhaving en vroegtijdig worden gewezen op realistische verbeterpunten.

De instanties waarvan de ambtenaren door de vakministers worden belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw hanteren een interventiebeleid. In dat interventiebeleid wordt bepaald hoe gegeven bepaalde omstandigheden in beginsel zal worden opgetreden. Het stellen van een einddatum is een instrument dat de bevoegde autoriteit op grond van artikel 76 Cbw kan inzetten tegen een essentiële entiteit. De bevoegde autoriteit kan na het vaststellen van een overtreding van de Cbw een einddatum bepalen waarop de essentiële entiteit de daarbij genoemde maatregelen moet hebben genomen om de overtreding te beëindigen of waarop de essentiële entiteit aan de daarbij nader omschreven eisen moet hebben voldaan ter beëindiging van de overtreding.[44]

Het bepalen van een einddatum is een besluit in de zin van artikel 1:3 Awb. Dat betekent dat de bevoegde autoriteit dit besluit op schrift aan de betreffende essentiële entiteit laat toekomen, dat het besluit onderbouwd dient te zijn en dat hiertegen bezwaar en beroep open staat. Zoals beschreven in paragraaf 5.6.5.2 van de memorie van toelichting op het wetsvoorstel is het stellen van een einddatum een relatief zwaar instrument en zal de bevoegde autoriteit daarbij moeten motiveren waarom de eerdere genomen maatregel of maatregelen ondoeltreffend zijn en waarom andere maatregelen naar redelijke verwachting ondoeltreffend zullen zijn, en daarom niet eerst worden opgelegd voordat de termijn wordt gesteld. Het inzetten van dit instrument zou gezien deze waarborgen niet tot onverwachte situaties behoren te leiden.

Het inzetten van sancties en ingrepen staat ten dienste van het bevorderen van de naleving van de wetgeving. Zoals eerder geantwoord werken de hiervoor bedoelde instanties aan een consistente toezichtspraktijk.

---

[44] Dit geldt ook voor een overtreding van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie.

5.6.5.3 Verzoek tot schorsing certificering of vergunning en verzoek tot schorsing leden van het bestuur

De leden van de GroenLinks-PvdA-fractie onderstrepen dat het schorsen van leden uit een bestuur een zeer zwaarwegend middel is. Deze leden vragen de regering om een scenario te schetsen waarin deze maatregelen doeltreffend en proportioneel zou zijn.

Een voorbeeld is een situatie waarin door handelen of nalaten van een lid van het bestuur, met overwegende invloed binnen de essentiële entiteit, de desbetreffende entiteit opzettelijk en voortdurend niet voldoet aan de wettelijke eisen van de Cbw, als gevolg waarvan belangrijke (maatschappelijke) belangen in het geding komen. Als in een dergelijk geval aangetoond kan worden dat de betreffende bestuurder de naleving van de Cbw actief belemmert, kan het gezien de omstandigheden van het geval voor de bevoegde autoriteit doeltreffend en proportioneel zijn om de burgerlijke rechter te verzoeken om deze bestuurder te schorsen. De bevoegde autoriteit kan pas daartoe overgaan nadat zij op grond van artikel 76, eerste lid, Cbw een einddatum heeft bepaald waarop de essentiële entiteit de daarbij genoemde maatregelen moet hebben genomen of waarop de essentiële entiteit aan de daarbij nader omschreven eisen moet hebben voldaan, zulks ter beëindiging van de overtreding van de Cbw, en nadat de essentiële entiteit op die datum daar niet aan heeft voldaan. Het is vervolgens aan de burgerlijke rechter om te oordelen over het verzoek van de bevoegde autoriteit tot schorsing van het bestuurslid.

5.6.6. Bestuurlijke boete

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen welke mogelijkheden entiteiten hebben om bezwaar te maken tegen een boetebesluit. Tevens vragen de leden hoe de hoogte van het boetemaximum is onderbouwd. Deze leden merken op dat de regering het boetemaximum bij overige overtredingen niet evenredig vindt. Kan de regering kort toelichten dat dit boetemaximum in geen geval evenredig is? Verder merken deze leden op dat entiteiten zwaar beboeten mogelijk als gevolg heeft dat, door de hoogte van de boete, de continuïteit bij een dienstverlenende entiteit in gevaar kan komen. Kan de regering toelichten hoe wordt voorkomen dat een hoge boete leidt tot haperingen in de dienstverlening?

Een boetebesluit is een besluit in de zin van artikel 1:3 Awb en staat daarmee open voor bezwaar en beroep. De betreffende entiteit heeft bovendien de mogelijkheid om haar zienswijze naar voren te brengen alvorens het boetebesluit wordt genomen. Artikel 69 Cbw omschrijft de relevante omstandigheden die moeten worden meegewogen voor het opleggen van een sanctie. Daarnaast dient de bevoegde autoriteit op grond van de Awb de bestuurlijke boete af te stemmen op de ernst van de overtreding en de mate waarin deze aan de overtreder kan worden verweten. Zij houdt daarbij zo nodig rekening met de omstandigheden waaronder de overtreding is gepleegd.

De NIS2-richtlijn omschrijft in artikel 34, vierde en vijfde lid, de maximale administratieve boeten die moeten kunnen worden opgelegd voor een overtreding van de zorgplicht, de meldplicht en de verplichting tot het informeren van ontvangers van diensten. Naast de zorgplicht, de meldplicht en de verplichting tot het informeren van ontvangers van diensten bevat de Cbw ook andere verplichtingen voor entiteiten. Een voorbeeld hiervan is de verplichting voor entiteiten om informatie te verstrekken ten behoeve van het nationale register van entiteiten (artikel 44 Cbw). Voor wat betreft een bestuurlijke boete voor de overtreding van die andere voor entiteiten geldende verplichtingen is gekozen voor een maximum van € 1.000.000,–. Dat betreft een voortzetting van de gekozen lijn in het kader van de implementatie van de NIS1-richtlijn in nationale wet- en regelgeving. Het hoge boetemaximum dat geldt voor een overtreding van de zorgplicht, de meldplicht en de verplichting tot het informeren van ontvangers van diensten (€ 10.000.000,– of 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar, of € 7.000.000,– of 1,4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar) ziet de regering als onevenredig in verhouding tot de aard van de overtredingen van overige verplichtingen.

Uit artikel 3:4 Awb vloeit voort dat de voor één of meer belanghebbenden nadelige gevolgen van een besluit, in dit geval een boetebesluit, niet onevenredig mogen zijn in verhouding tot de met het besluit te dienen doelen. De gevolgen voor de continuïteit van de dienstverlenende entiteit en de gevolgen die onderbreking van de dienstverlening van de entiteit voor andere belanghebbende kan hebben, kan

daarmee gegeven de omstandigheden van het geval relevant zijn bij het bepalen van de hoogte van een bestuurlijke boete.

5.6.7. Overtrederschap

De leden van de GroenLinks-PvdA-fractie merken op dat overtredingen van de Cyberbeveiligingswet kunnen leiden tot handhaving jegens individuen, zoals bestuursleden. Deze leden vragen de regering om te bevestigen of dit inderdaad het geval is, en zo ja, om te onderbouwen dat bestraffen op persoonlijke titel effectief leidt tot betere cyberveiligheid.

De bevoegde autoriteit kan bij een overtreding van een verplichting uit de Cbw handhavend optreden tegen de entiteit die de overtreding begaat, maar ook tegen degenen die worden aangemerkt als opdrachtgever van de door de entiteit begane overtreding en degenen die feitelijke leiding hebben gegeven aan de verboden gedraging. Dit kunnen zowel natuurlijke personen als rechtspersonen zijn. Voor een uitgebreide toelichting hierop wordt verwezen naar paragraaf 5.6.7 van de memorie van toelichting op het wetsvoorstel.

De vraag of handhavend optreden jegens een individu leidt tot betere cyberveiligheid, kan niet in zijn algemeenheid worden beantwoord. Dat zal immers per casus verschillen en hangt af van diverse aspecten, waaronder de aard van de omstandigheden en de verplichting die wordt overtreden.

5.6.8. Samenwerking toezichtoudende instanties

De leden van de GroenLinks-PvdA-fractie erkennen het belang van een goede samenwerking tussen toezichthouders. Deze leden vragen aan de regering op welke wijze de samenwerkafspraken tussen toezichthouders worden vastgesteld en waar en wanneer deze worden gepubliceerd.

In artikel 15, eerste tot en met vijfde lid, Cbw zijn de vakministers aangewezen als de bevoegde autoriteit voor de entiteiten die onder het toepassingsbereik van de Cbw vallen. Op grond van artikel 15, zesde lid, onderdeel a, Cbw heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Cbw.[45] De vakministers wijzen bij besluit de ambtenaren aan die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[46] Daarbij zal het gaan om de aanwijzing van ambtenaren van onder meer de rijksinspecties ILT, RDI, Inspectie van het Onderwijs, IGJ en NVWA. In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister).

De hiervoor bedoelde instanties werken intensief samen ten behoeve van een doeltreffende en doelmatige inrichting van het toezicht op de Cbw en de Wwke en zijn overeengekomen om de samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Dit protocol wordt op dit moment opgesteld. Het is de verwachting dat het protocol begin 2026 wordt gepubliceerd.

5.7. Registratie

De leden van de GroenLinks-PvdA-fractie hebben twijfels over de registratieplicht van de NIS2-richtlijn. Deze leden stellen dat het opbouwen van een lijst met relevante entiteiten ook leidt tot een nieuwe, gevoelige dataset. Onderschrijft de regering dat een dergelijk overzicht gevoelige informatie betreft? Zij vinden het niet duidelijk beschreven hoe de vertrouwelijke en veilige toegang tot het register door CSIRT's wordt geregeld. De regering spreekt van een "technische oplossing" die dit moet waarborgen. Welke techniek betreft dit en is deze waterdicht?

---

[45] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van de artikelen 21, vijfde lid, en 23, elfde lid, NIS2-richtlijn vastgestelde uitvoeringshandelingen en de op grond van artikel 24, tweede lid, NIS2-richtlijn vastgestelde gedelegeerde handelingen, voor zover in die uitvoeringshandelingen of gedelegeerde handelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 15, zesde lid, onderdeel b, Cbw.

[46] Artikel 5:11 Awb spreekt in deze context over "toezichthouder".

De regering onderschrijft het belang van een goede beveiliging van het nationale register, bedoeld in artikel 43 Cbw, ter bescherming van alle gegevens die daarin worden opgenomen.

Het beheer van het register ligt in de praktijk bij het NCSC. Het NCSC neemt de nodige maatregelen om ervoor te zorgen dat de in het register opgenomen informatie veilig, verantwoord en in overeenstemming met de Cbw en – voor zover het persoonsgegevens betreft – met de Avg wordt verwerkt.

Alle door entiteiten aangeleverde gegevens worden als vertrouwelijk behandeld en veilig opgeslagen. Dit betekent dat de gegevens niet leesbaar zijn voor onbevoegden, zowel tijdens de opslag als bij de verzending. Hiervoor maakt het NCSC gebruik van versleuteling, een techniek die informatie beschermt tegen toegang door derden.

Daarnaast maakt het NCSC regelmatig back-ups die veilig worden opgeslagen. Dit zorgt ervoor dat gegevens hersteld kunnen worden bij een technische storing, menselijke fout of cyberaanval. De systemen worden verder beveiligd met geavanceerde netwerkbescherming, zoals firewalls en systemen die verdachte activiteiten detecteren en blokkeren.

De bevoegde autoriteiten en de CSIRT's hebben toegang tot het register ten behoeve van de uitoefening van hun taken uit de Cbw, voor zover de toegang ziet op informatie over de entiteiten waarvoor zij zijn aangewezen als de bevoegde autoriteit respectievelijk het CSIRT. Alleen de medewerkers van deze instanties die de gegevens nodig hebben voor hun functie-uitoefening, krijgen derhalve toegang. Deze toegang is strikt gereguleerd en beperkt tot wat noodzakelijk is voor hun functie. Ditzelfde geldt voor medewerkers van het NCSC die het technisch onderhoud en beheer van het register verzorgen. Om te voorkomen dat toegang onnodig lang blijft bestaan, worden rechten regelmatig gecontroleerd en aangepast. Het NCSC houdt ook een logboek bij van wie toegang heeft gehad tot de gegevens en controleert deze logs om misbruik te voorkomen.

Om ervoor te zorgen dat gegevens altijd beschermd blijven, voert het NCSC regelmatig beveiligingstests uit. Dit omvat onder andere het simuleren van cyberaanvallen en het opsporen van kwetsbaarheden in de systemen. Dankzij deze tests kunnen beveiligingsproblemen vroegtijdig worden gesignaleerd en worden opgelost, zodat gegevens veilig blijven.

De leden van de GroenLinks-PvdA-fractie lezen dat cloudcomputingdiensten en socialenetwerkdiensten vallen onder de reikwijdte van de NIS2-richtlijn. Dit betreft echter veelal niet-Europese bedrijven die diensten verlenen aan Nederlandse en Europese instanties. Daarom vragen deze leden om helder te maken welke verplichtingen (kunnen) worden opgelegd aan bedrijven die essentiële ICT en communicatiemogelijkheden verlenen, maar niet onder Europese jurisdictie vallen. Zij vinden het gerechtvaardigd om niet-Europese bedrijven zoveel als mogelijk aan de NIS2-richtlijn te laten voldoen.

Indien aanbieders van cloudcomputingdiensten en aanbieders van platforms voor socialenetwerkdiensten diensten verlenen of activiteiten verrichten in Nederland of een andere lidstaat van de Europese Unie, zijn deze aanbieders op grond van de NIS2-richtlijn verplicht om een hoofdvestiging dan wel vertegenwoordiger te hebben in een lidstaat van de Europese Unie én vallen zij als gevolg daarvan onder de jurisdictie van die lidstaat. Hierdoor maakt het ten aanzien van deze aanbieders op zich niet uit of zij al dan niet Europese bedrijven zijn. Indien de hoofdvestiging of vertegenwoordiger van deze aanbieders zich in Nederland bevindt, dan vallen zij onder de Cbw. Bevindt de hoofdvestiging of vertegenwoordiger zich in een andere lidstaat van de Europese Unie, dan vallen deze aanbieders onder de nationale wetgeving van die lidstaat waarin de NIS2-richtlijn is geïmplementeerd. Dit betekent dat ook deze aanbieders moeten voldoen aan de verplichtingen uit de NIS2-richtijn, waaronder de zorgplicht en de meldplicht.

Voor het bepalen of een aanbieder een hoofdvestiging in Nederland heeft wordt allereerst in aanmerking genomen of de beslissingen met betrekking tot de maatregelen voor het beheersen van cyberbeveiligingsrisico's hoofdzakelijk in Nederland worden genomen. Indien deze beslissingen niet hoofdzakelijk in Nederland of een andere lidstaat van de Europese Unie worden genomen, of indien niet kan worden bepaald in welke lidstaat van de Europese Unie die beslissingen hoofdzakelijk worden genomen, wordt de hoofdvestiging geacht zich in Nederland te bevinden indien de

cyberbeveiligingsactiviteiten in Nederland worden uitgevoerd. Indien de cyberbeveiligingsactiviteiten niet in Nederland of een andere lidstaat van de Europese Unie worden uitgevoerd, of niet kan worden bepaald in welke lidstaat van de Europese Unie de cyberbeveiligingsactiviteiten worden uitgevoerd, wordt de hoofdvestiging geacht zich
te bevinden in Nederland indien de Nederlandse vestiging het grootste aantal werknemers in de Europese Unie heeft.

Indien een entiteit geen enkele vestiging in de Europese Unie heeft, maar wél diensten verleent of activiteiten verricht in Nederland of een andere lidstaat van de Europese Unie, dan is de entiteit verplicht om een vertegenwoordiger aan te wijzen die is gevestigd in een lidstaat van de Europese Unie waar deze entiteit die diensten verleent of activiteiten verricht. Als het daarbij gaat om de aanwijzing van een vertegenwoordiger die is gevestigd in Nederland, dan valt de entiteit onder de Cbw.

5.8. Toepassing in Caribisch deel van het Koninkrijk

De leden van de GroenLinks-PvdA-fractie zijn teleurgesteld over het niet meenemen van Caribisch Nederland onder het bereik van de Cyberbeveiligingswet. Deze leden vragen de regering om veel duidelijker te stellen waarom dit nu niet mogelijk is, en welke randvoorwaarden er nodig zijn om dit wel mogelijk te maken. Hierin achten zij het waardevol om hardop de ambitie uit te spreken dat Caribisch Nederland op termijn wordt opgenomen in de Cyberbeveiligingswet. De formulering van de regering is momenteel te vrijblijvend en leidt niet tot een verbetering van de cyberveiligheid in het Caribische deel van het Koninkrijk.

De NIS2-richtlijn is alleen van toepassing op Europees Nederland en niet op Caribisch Nederland. Conform het principe van *comply or explain* dient te worden bepaald of en hoe de Cbw van toepassing moet worden verklaard voor Caribisch Nederland. Het kabinet heeft ervoor gekozen Caribisch Nederland niet direct te betrekken bij de implementatie van de NIS2-richtlijn. Zoals in paragraaf 5.8 van de memorie van toelichting op het wetsvoorstel is aangegeven, is de toepassing van de Cbw in Caribisch Nederland op dit moment nog niet uitvoerbaar. Er wordt op dit moment nog uitvoering gegeven aan enkele randvoorwaarden voor het verhogen van de digitale weerbaarheid in Caribisch Nederland. Zo wordt gewerkt aan het in kaart brengen welke processen in Caribisch Nederland mogelijk maatschappelijk ontwrichtende effecten hebben en daarmee betere bescherming behoeven. Het volledig van toepassing verklaren van de Cbw op Caribisch Nederland wordt om die reden als te vroeg gezien.

Het versterken van de digitale weerbaarheid in Caribisch Nederland is met de toenemende digitalisering van Caribisch Nederland van toenemend belang. De regering onderschrijft dan ook de ambitie zoals aangegeven door de leden van de GroenLinks-PvdA-fractie van het versterken van de digitale weerbaarheid in het Caribisch deel van het Koninkrijk. Om deze reden wordt er op verschillende manieren in samenwerking met Caribisch Nederland gewerkt aan het fundament van hun cybersecuritystelsel, door hen aan te sluiten op het nationaal cybersecuritystelsel. Op korte termijn is dit gericht op relatiemanagement met relevante stakeholders en betrokken partijen, kennis- en informatiedeling en het in kaart brengen van de belangrijkste processen. Dat wordt onder meer gedaan door het betrekken van Bonaire, Sint Eustatius en Saba in het Cyberweerbaarheidsnetwerk, waar samenwerking wordt gefaciliteerd en gecoördineerd op verschillende terreinen van digitale veiligheid, zodat Caribisch Nederland in staat gesteld wordt om, met oog voor de lokale context, haar digitale weerbaarheid te versterken. Dat is tevens randvoorwaardelijk om op termijn de Cbw of een daarmee vergelijkbare wet in Caribisch Nederland te implementeren en een gelijkwaardig beschermingsniveau als in Europees Nederland te realiseren. Hierbij wordt bovendien samenwerking gezocht met de autonome landen in het Caribische deel van het Koninkrijk, gezien de reeds bestaande onderlinge samenwerking en digitale afhankelijkheden met Caribisch Nederland.

5.9. Rechtsbescherming en vereisten aan besluiten

De leden van de GroenLinks-PvdA-fractie erkennen het belang van openbaarheid over overtredingen. Echter ligt het risico van reputatieschade voor entiteiten op de loer, met nadelige effecten voor de integriteit en het vertrouwen in deze entiteiten. Deze leden benadrukken dat hiermee het ontwrichtende effect van cyberaanvallen

alsnog tot uiting kan komen. Daarom horen zij graag van de regering of er scenario's zijn waarin het niet openbaren van overtredingen de voorkeur heeft.

De regering is bewust van de risico's die de openbaarmaking van overtredingen met zich kunnen brengen, zoals reputatieschade voor entiteiten, het verlies van het vertrouwen in de betrokken entiteiten en de cyberbeveiliging van entiteiten als zodanig. De bevoegde autoriteit dient bij de besluitvorming over het al dan niet openbaar maken van een vastgestelde overtreding en de genomen maatregelen, de omstandigheden van het geval en de verwachte effecten van een openbaarmaking af te wegen met het beoogde doel van de openbaarmaking. Indien bijvoorbeeld de nadelige effecten voor de betrokken entiteit en/of de maatschappij niet in verhouding staan met het beoogde doel van de openbaarmaking, kan de bevoegde autoriteit besluiten een overtreding niet of geanonimiseerd openbaar te maken.

6. Verhouding tot het hoger recht

6.1. Inleiding

6.2. Gegevensverwerkingen

De leden van de GroenLinks-PvdA-fractie lezen dat CSIRT's geacht worden om gevoelige informatie onderling uit te wisselen. Deze leden vragen de regering om een toelichting over de technische maatregelen die getroffen zullen worden om de vertrouwelijkheid van deze communicatie te waarborgen.

Voor CSIRT's geldt op grond van artikel 52 Cbw dat zij voor de doeltreffende en doelmatige uitvoering van hun wettelijke taken met elkaar en met CSIRT's van andere lidstaten van de Europese Unie samenwerken en in het kader van die samenwerking alle daarvoor noodzakelijke gegevens, waaronder persoonsgegevens, uitwisselen. In artikel 11, eerste lid, onderdeel d, NIS2-richtlijn is geregeld dat de CSIRT's onder meer aan de eis moeten voldoen dat zij de vertrouwelijkheid en betrouwbaarheid van hun activiteiten waarborgen. Die eis betreft dus ook de uitwisseling van gegevens door een CSIRT met andere CSIRT's. Mede met het oog op het voorkomen van kwetsbaarheden voor aanvallen kan niet openbaar worden gemaakt welke technische maatregelen de CSIRT's precies nemen met betrekking tot het waarborgen van de vertrouwelijkheid van de informatie-uitwisseling met andere CSIRT's. Wel kan in meer algemene zin worden aangegeven dat de CSIRT's ter waarborging van de vertrouwelijkheid van de verwerkte gegevens onder meer maatregelen als encryptie en *role-based access control* (RBAC, een methode voor toegangsbeheer waarbij gebruikerstoegang tot bronnen wordt toegewezen op basis van de rol van de gebruiker binnen een organisatie) zullen nemen.

6.3. EVRM

6.3.1. Beperking moet legitiem doel dienen en noodzakelijk zijn

De leden van de GroenLinks-PvdA-fractie waarschuwen dat bevoegdheden die gaan over het verzamelen van gevoelige informatie aan stevige kaders gebonden moeten zijn. Dit voorkomt zogenaamde 'mission creep', waarin het doel waarvoor informatie wordt verzameld en verwerkt verwatert. Deze leden vragen de regering om uit te leggen dat hier geen sprake van kan zijn.

Voor de verwerking van persoonsgegevens door de in de Cbw genoemde instanties (bevoegde autoriteit, CSIRT, centrale contactpunt) geldt dat dit in de Cbw uitdrukkelijk is gekoppeld aan de uitvoering van de taken die aan hen in die wet zijn toegewezen. Bij het in het kader daarvan verwerken van persoonsgegevens moeten deze instanties voldoen aan de in de Avg daaraan gestelde eisen, waaronder het vereiste dat de verwerking van persoonsgegevens beperkt blijft tot wat noodzakelijk is voor de doeleinden waarvoor zij worden verwerkt. Op de naleving hiervan wordt toezicht gehouden door de AP en de functionaris gegevensbescherming. Voor de verstrekking van gegevens door genoemde instanties in het kader van de samenwerking met elkaar of met andere in de Cbw genoemde instanties is in de Cbw ook specifiek bepaald dat dat beperkt blijft tot wat noodzakelijk is voor de uitvoering van de taken van de instantie waaraan wordt verstrekt. De verwerking van persoonsgegevens door bijvoorbeeld een CSIRT of

bevoegde autoriteit is hiermee voorzien van voldoende stevige kaders om te voorkomen dat dit verder gaat dan noodzakelijk is voor de uitvoering van hun taken in de Cbw.

De leden van de VVD-fractie lezen dat ter bevordering van grensoverschrijdende samenwerking het nodig is dat iedere lidstaat een centraal contactpunt aanwijst dat verantwoordelijk is voor het leggen van verbindingen op het niveau van de EU, en meer in het bijzonder het informeren van andere lidstaten in geval van incidenten van grensoverschrijdende consequenties. In Nederland is de minister van Justitie en Veiligheid aangewezen als het centrale contactpunt. Hoe vindt dit contact nu in de praktijk plaats, door welke organisatie en wat is de huidige wettelijke grondslag daarvoor? Deze leden vragen hoe binnen het ministerie van Justitie en Veiligheid deze taak wordt belegd, waarom hiervoor is gekozen en hoe in de praktijk overlap wordt voorkomen met andere centrale contactpunten.

Op dit moment is de Minister van Justitie en Veiligheid belast met de taak van het centrale contactpunt als bedoeld in de NIS1-richtlijn. Dit is wettelijk vastgelegd in de artikelen 2, 3 en 19 Wbni. Die taak wordt in de praktijk namens die minister uitgevoerd door het NCSC. Het gaat hierbij in hoofdzaak om het zorgen voor grensoverschrijdende samenwerking van de Nederlandse autoriteiten met de betrokken autoriteiten van andere lidstaten van de Europese Unie, de samenwerkingsgroep, bedoeld in artikel 14 NIS2-richtlijn, en het CSIRT-netwerk door middel van het vervullen van een verbindingsfunctie. Meer in het bijzonder zorgt het NCSC als centrale contactpunt ervoor dat centrale contactpunten van andere lidstaten op de hoogte worden gesteld van incidenten, die binnen Nederland zijn gemeld bij het CSIRT, als die gevolgen hebben voor entiteiten in die andere lidstaat. Ook informeert het NCSC in Nederland het CSIRT of de bevoegde autoriteit als van het centrale contactpunt van een andere lidstaat informatie over een voor Nederland relevant grensoverschrijdend incident is ontvangen. Het NCSC staat voor het uitvoeren van deze taken in regelmatig contact met genoemde andere centrale contactpunten alsook de samenwerkingsgroep en het CSIRT-netwerk. In lijn hiermee is ervoor gekozen om de taak van het centrale contactpunt als bedoeld in de NIS2-richtlijn, die overeenkomt met die van het centrale contactpunt als bedoeld in de NIS1-richtlijn, te beleggen bij de Minister van Justitie en Veiligheid en in de praktijk door het NCSC te laten blijven uitvoeren.

Van overlap met andere centrale contactpunten is in Nederland geen sprake, omdat het NCSC die rol namens de Minister van Justitie en Veiligheid als enige vervult.

6.3.1.1 Dringende maatschappelijke behoefte

De leden van de GroenLinks-PvdA-fractie vragen of de afstemming tussen vakministers en de coördinerende minister van Justitie en Veiligheid niet zal leiden tot onnodig veel overdrachten van gevoelige data. Hierdoor ontstaan er meerdere datapunten die elk het risico op een lek kunnen vergroten. Heeft de regering passende maatregelen getroffen om in het schakelen tussen sectoren, vakministers en het centrale contactpunt geen extra risico te lopen op datalekken?

Voor de vakministers die in de Cbw zijn aangewezen als bevoegde autoriteit, de Minister van Justitie en Veiligheid die in de Cbw is aangewezen als het centrale contactpunt en de organisaties die in het Cbb of lagere regelgeving zijn aangewezen als CSIRT geldt dat artikel 51, eerste lid, Cbw bepaalt dat zij met elkaar samenwerken voor de doeltreffende en doelmatige uitvoering van hun in de Cbw vastgelegde taken. Ook is in die bepaling bepaald dat zij in het kader daarvan gegevens, waaronder persoonsgegevens, met elkaar uitwisselen. Daarbij geldt nadrukkelijk dat het bij verstrekking telkens moet gaan om gegevens die noodzakelijk zijn voor de uitvoering van de taken van de instantie waaraan wordt verstrekt en dat het hierbij dus niet zal gaan om onnodig veel overdrachten van informatie.

Alle hiervoor genoemde instanties (bevoegde autoriteiten, CSIRT's, het centrale contactpunt) zullen onder meer maatregelen moeten nemen om de vertrouwelijkheid van de uitwisseling van informatie met de andere instanties te waarborgen.

Ten aanzien van de hiervoor genoemde ministers geldt bovendien dat alle ministeries essentiële entiteit in de zin van de Cbw zijn en op grond van de zorgplicht (artikel 21 Cbw) passende en evenredige maatregelen moeten nemen. Zij moeten in het kader van de zorgplicht onder meer maatregelen treffen op het gebied

van encryptie, cyberhygiëne en toegangsbeheer. Deze maatregelen dragen ook bij aan het voorkomen van datalekken en het zoveel mogelijk beperken van de gevolgen van datalekken.

Zoals hierboven aangegeven in het antwoord op de onder 6.2 vermelde vraag van de leden van de GroenLinks-PvdA-fractie volgt de eis om die maatregelen te nemen voor CSIRT's uit artikel 11, eerste lid, NIS2-richtlijn.

6.3.1.2 Proportionaliteit

De leden van de GroenLinks-PvdA-fractie zijn kritisch op het aanleggen van een register met IP-adressen. Deze leden vragen om een nadere onderbouwing van de noodzaak hiervan. Tevens willen zij weten welke beveiligingsmaatregelen worden genomen om dit register zo goed mogelijk te beschermen.

De totstandkoming van het nationale register, bedoeld in artikel 43 Cbw, volgt uit het dwingende voorschrift van artikel 3, derde lid, NIS2-richtlijn. Dat geldt ook voor de verplichting voor entiteiten om (ook) de IP-bereiken te verstrekken. Dit wordt dwingend voorgeschreven in artikel 3, vierde lid, onderdeel b, NIS2-richtlijn. Van belang is op te merken dat dergelijke registers met IP-adressen reeds bestaan, zoals de Regionale Internet Registers.

De Minister van Justitie en Veiligheid is verantwoordelijk voor de totstandkoming van het nationale register en het beheer daarvan. Deze taken worden in de praktijk uitgevoerd door het NCSC. Het NCSC neemt de nodige maatregelen om ervoor te zorgen dat de in het register opgenomen informatie veilig, verantwoord en in overeenstemming met de Cbw en – voor zover het persoonsgegevens betreft – met de Avg wordt verwerkt.

Alle door entiteiten aangeleverde gegevens worden als vertrouwelijk behandeld en veilig opgeslagen. Dit betekent dat de gegevens niet leesbaar zijn voor onbevoegden, zowel tijdens de opslag als bij de verzending. Hiervoor maakt het NCSC gebruik van versleuteling, een techniek die informatie beschermt tegen toegang door derden.

Daarnaast maakt het NCSC regelmatig back-ups die veilig worden opgeslagen. Dit zorgt ervoor dat gegevens hersteld kunnen worden bij een technische storing, menselijke fout of cyberaanval. De systemen worden verder beveiligd met geavanceerde netwerkbescherming, zoals firewalls en systemen die verdachte activiteiten detecteren en blokkeren.

De bevoegde autoriteiten en de CSIRT's hebben toegang tot het register ten behoeve van de uitoefening van hun taken uit de Cbw, voor zover de toegang ziet op informatie over de entiteiten waarvoor zij zijn aangewezen als de bevoegde autoriteit respectievelijk het CSIRT. Alleen de medewerkers van deze instanties die de gegevens nodig hebben voor hun functie-uitoefening, krijgen derhalve toegang. Deze toegang is strikt gereguleerd en beperkt tot wat noodzakelijk is voor hun functie. Ditzelfde geldt voor medewerkers van het NCSC die het technisch onderhoud en beheer van het register verzorgen. Om te voorkomen dat toegang onnodig lang blijft bestaan, worden rechten regelmatig gecontroleerd en aangepast. Het NCSC houdt ook een logboek bij van wie toegang heeft gehad tot de gegevens en controleert deze logs om misbruik te voorkomen.

Om ervoor te zorgen dat gegevens altijd beschermd blijven, voert het NCSC regelmatig beveiligingstests uit. Dit omvat onder andere het simuleren van cyberaanvallen en het opsporen van kwetsbaarheden in de systemen. Dankzij deze tests kunnen beveiligingsproblemen vroegtijdig worden gesignaleerd en worden opgelost, zodat gegevens veilig blijven.

6.4. Avg

De leden van de GroenLinks-PvdA-fractie vragen de regering op welke wijze de Autoriteit Persoonsgegevens (AP) is betrokken bij de totstandkoming van deze paragraaf. Kan de toezichthouder zich vinden in de uiteindelijke formulering?

Een concept van dit wetsvoorstel met bijbehorende memorie van toelichting is ter advies voorgelegd aan de AP, zoals dwingend wordt voorgeschreven in artikel 36, vierde lid, Avg. De AP heeft in haar advies geen opmerkingen geplaatst bij de formulering van deze paragraaf van de memorie van toelichting.

6.4.1. Opslagbeperking

De leden van de GroenLinks-PvdA-fractie benadrukken het belang van wettelijke bewaartermijnen. Deze leden lezen dat deze termijnen zullen aansluiten op sectorale wetgeving. Kan de regering aangeven of er wezenlijke verschillen zijn in de bewaartermijnen die gehanteerd worden in verschillende sectoren? Zo ja, zijn deze verschillende bewaartermijnen gerechtvaardigd? Zij willen weten of het hanteren van één bewaartermijn voor alle data-opslag van CSIRT's mogelijke voordelen heeft.

Anders dan de leden van de GroenLinks-PvdA-fractie veronderstellen is ten aanzien van de wettelijke bewaartermijnen niet aangesloten op sectorale wetgeving. De CSIRT's en bevoegde autoriteiten zullen voor verschillende processen verschillende bewaartermijnen hanteren, vanwege de verschillende taken en de verschillende doelen van die processen.

De leden van de GroenLinks-PvdA-fractie vinden het niet duidelijk omschreven waarom de CSIRT bijzondere persoonsgegevens moet kunnen analyseren. Deze leden vragen de regering om nader toe te lichten waarom een uitzondering van bijzondere persoonsgegevens niet mogelijk is.

Het CSIRT kan bij het analyseren van informatie stuiten op bijzondere persoonsgegevens, zoals een dataset die inloggegevens (*credentials*) bevat waarin ook e-mailadressen zitten waaruit het lidmaatschap van een vakbond, vereniging voor LHBTI-rechten of politieke partij blijkt. Te denken valt aan e-mailadressen waarin de naam van een vakbond, vereniging of politieke partij is verwerkt. Daarnaast kan het bijvoorbeeld voorkomen dat een server van een zorginstelling op het internet staat die medische gegevens bevat of andere bijzondere persoonsgegevens, zoals de dieetwensen van cliënten of patiënten waaruit de geloofsovertuiging kan worden afgeleid. De aanwezigheid van zulke gegevens in een dataset kan betekenen dat bij de organisaties waarvan de bijzondere persoonsgegevens afkomstig zijn (zoals een politieke partij of een vakbond), sprake is van een ICT-dreiging of zelfs een ICT-incident. Het CSIRT moet in het kader van haar taakuitoefening bijzondere persoonsgegevens kunnen analyseren, omdat zij anders die organisaties niet meer kan waarschuwen over cyberdreigingen of -incidenten.

7. Verhouding tot nationale regelgeving

7.1. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen welke rol de coördinerende staatssecretaris voor Digitalisering en Koninkrijksrelaties heeft voor het naleven van de NIS2-richtlijn bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties wordt in de context van de Cbw beschouwd als het bestuur van de entiteit Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De Minister van Binnenlandse Zaken en Koninkrijksrelaties is tevens de bevoegde autoriteit voor de gehele sector overheid. Op grond van de huidige taakomschrijving is de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties belast met de coördinerende verantwoordelijkheid voor digitalisering en met de digitale rijksdienst en digitale veiligheid van de overheid.[47]

7.2. Ministerie van Economische Zaken

De leden van de GroenLinks-PvdA-fractie wijzen er op dat mkb'ers, die in een toeleveringsketen zitten met essentiële en belangrijke entiteiten, ook beschikken over informatie die ze mogelijk een doelwit maken voor kwaadwillenden. Welke maatregelen treft de regering om dit risico te mitigeren en ook deze bedrijven weerbaar te maken?

[47] *Stcrt.* 2025, 23904.

Organisaties kunnen inderdaad worden geconfronteerd met cyberaanvallen door kwaadwillenden via hun toeleveringsketen. Eén van de maatregelen die essentiële entiteiten en belangrijke entiteiten moeten nemen om te voldoen aan de zorgplicht uit de Cbw ziet op maatregelen in het kader van de beveiliging van hun toeleveringsketen, zie artikel 21, derde lid, onderdeel d, Cbw. Deze maatregel is nader uitgewerkt in artikel 10 Cbb. Dit artikel verplicht essentiële entiteiten en belangrijke entiteiten om te toetsen of hun rechtstreekse leveranciers en rechtstreekse dienstverleners voldoen aan de beveiligingseisen van de betreffende entiteit. Dit betekent concreet dat niet de regering, maar entiteiten zelf maatregelen dienen te treffen om risico's te mitigeren en om henzelf weerbaar te maken.

Daarnaast zijn er bedrijven die in de toeleveringsketen zitten maar tegelijkertijd zelf ook een essentiële entiteit of belangrijke entiteit zijn onder de Cbw en daarmee ook moeten voldoen aan de zorgplicht onder de Cbw.

Voor het midden- en kleinbedrijf (hierna: mkb) geldt dat indien zij niet als een essentiële entiteit of belangrijke entiteit kwalificeren en daarmee niet onder de Cbw vallen, zij behoren tot de doelgroep van het DTC. Het DTC heeft op grond van de Wbdwb onder andere tot taak het mkb te voorzien van informatie met het oog op het verhogen van de cyberweerbaarheid van het mkb in Nederland.

De leden van de NSC-fractie vragen de regering op welke wijze de samenwerking tussen de Cyberbeveiligingswet en de Wet bevordering digitale weerbaarheid (Wbdw) wordt geborgd. Wordt er voorzien in een geïntegreerd meld- en toezichtkader voor organisaties die onder beide wetten vallen? Daarnaast vragen deze leden hoe wordt voorkomen dat organisaties met dubbele toezichthouders te maken krijgen en of het risico van overlappende verplichtingen voldoende wordt ondervangen.

Met de komst van de Cbw zal de Wbdwb naast de Cbw blijven bestaan en de Cbw en Wbdwb zullen elkaar aanvullen. Waar de Cbw zich richt op essentiële entiteiten en belangrijke entiteiten in de zin van de Cbw, richt de Wbdwb zich op alle bedrijven met uitzondering van de hiervoor bedoelde entiteiten. In de maatschappelijke discussie is er vaak focus op essentiële entiteiten en belangrijke entiteiten vanwege de maatschappelijke impact die cyberincidenten bij hen kunnen veroorzaken. Met de Wbdwb zijn er capaciteiten beschikbaar gesteld die specifiek gericht zijn om juist ook het mkb goed te informeren en cyberweerbaarder te maken.

De Cbw bevat verplichtingen voor (onder meer) essentiële entiteiten en belangrijke entiteiten, terwijl de Wbdwb geen verplichtingen bevat voor haar doelgroep. Er is onder de Wbdwb dan ook geen sprake van toezicht en handhaving.

De verschillende doelgroepen tussen de Cbw en de Wbdwb en het ontbreken van verplichtingen onder de Wbdwb zorgen ervoor dat er geen risico bestaat op overlappende verplichtingen tussen die twee wetten. De Cbw en de Wbdwb vormen samen een integraal kader voor digitale veiligheid, maar hebben onderscheidenlijke doelgroepen en benaderingen.

7.3 Ministerie van Volksgezondheid, Welzijn en Sport

De leden van de GroenLinks-PvdA-fractie benadrukken dat de Inspectie Gezondheidszorg en Jeugd (IGJ) een essentiële taak heeft om de cyberveiligheid van de zorgsector te controleren. Het is echter niet duidelijk of de IGJ beschikt over de capaciteit om dit naar wens te doen. Graag vernemen zij welke extra belasting de IGJ krijgt onder de NIS2-richtlijn en of de IGJ daarin tegemoet wordt gekomen.

De IGJ is reeds voorzien in aanvullende capaciteit die haar in de gelegenheid stelt zich voor te bereiden op de aanwijzing van de ambtenaren van de IGJ die worden belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw. Wat de daadwerkelijke toezichtbelasting voor de IGJ zal zijn nadat de Cbw in werking is getreden en of de beschikbaar gestelde middelen voldoende zijn voor effectief toezicht kan in deze fase nog niet worden voorspeld.

8. Gevolgen

8.1. Gevolgen voor burgers en bedrijven

8.1.1. Inleiding

De leden van de GroenLinks-PvdA-fractie vragen aan de regering hoe zij tot de inschatting is gekomen dat 8.100 entiteiten onder de Cyberbeveiligingswet zullen vallen. Worden deze 8.100 entiteiten op de hoogte gesteld van hun mogelijke aanwijzing als essentiële of belangrijke entiteit?

Aanvankelijk was de schatting dat circa 10.000 entiteiten onder de Cbw zouden vallen, op basis van de toenmalige gegevens van het Centraal Bureau voor de Statistiek (CBS). Na de zomer van 2023 hebben de betrokken vakdepartementen een eigen schatting gemaakt van het aantal organisaties dat naar verwachting onder het toepassingsbereik van de Cbw komt te vallen, in de sectoren waar zij beleidsverantwoordelijk voor zijn. De uitkomst daarvan is dat de Cbw naar verwachting van toepassing zal zijn op circa 8.100 organisaties.

Het voorgaande betreft een schatting. Pas zodra entiteiten die kwalificeren als essentiële entiteit, belangrijke entiteit of entiteit die domeinnaamregistratiediensten verleent in de zin van de Cbw zich geregistreerd hebben, weet de regering exact hoeveel entiteiten onder het toepassingsbereik van de Cbw vallen.

Voor de meeste entiteiten die onder het toepassingsbereik van de Cbw vallen geldt dat zij niet bij regeling of besluit aangewezen worden als essentiële entiteit of belangrijke entiteit in de zin van de Cbw, maar dat zij van rechtswege onder de Cbw vallen. Zij worden niet op de hoogte gesteld dat zij onder de Cbw vallen en zijn zelf verantwoordelijk om te beoordelen of zij onder de Cbw vallen. Hiervoor heeft de rijksoverheid een zelfevaluatietool beschikbaar gesteld.

Voor een kleinere groep entiteiten geldt dat zij wel ervan op de hoogte zullen worden gesteld dat de Cbw op hen van toepassing is, omdat zij bij regeling of besluit worden aangewezen als essentiële entiteit of belangrijke entiteit.

De leden van de NSC-fractie vragen de regering of uit artikel 8, eerste lid, onderdeel h, van de Cyberbeveiligingswet voldoende duidelijk blijkt dat wordt gedoeld op gemeenschappelijke regelingen als bedoeld in de Wet gemeenschappelijke regelingen. Voorts vragen deze leden of het voldoende helder is dat niet de regeling zelf, maar de bij die regeling ingestelde openbare lichamen, bedrijfsvoeringsorganisaties en gemeenschappelijke organen als entiteiten onder de Cyberbeveiligingswet vallen.

In paragraaf 5.1.2 van de memorie van toelichting op het wetsvoorstel is aangegeven dat het bij de in artikel 8, eerste lid, onderdeel h, Cbw als essentiële entiteit aangewezen gemeenschappelijke regelingen (voor zover deze kwalificeren als overheidsinstantie) specifiek gaat om openbare lichamen, bedrijfsvoeringsorganisaties en gemeenschappelijke organen als bedoeld in de Wet gemeenschappelijke regelingen. Om misverstanden te voorkomen worden bij nota van wijziging artikel 8, eerste lid, onderdeel h, Cbw en bijlage 1 van de Cbw aangepast, zodat duidelijk is dat het gaat om openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties als bedoeld in artikel 8, eerste, tweede, onderscheidenlijk derde lid, Wet gemeenschappelijke regelingen, voor zover deze openbare lichamen, gemeenschappelijke organen en bedrijfsvoeringsorganisaties kwalificeren als overheidsinstantie.

8.1.2. Zorgplicht

De leden van de GroenLinks-PvdA-fractie zijn kritisch op het feit dat de cyberveiligheidsmaatregelen in algemene maatregelen van bestuur (AMvB) worden beschreven. Deze leden vragen de regering waarom deze uitwerking in lagere regelgeving wordt gedaan en hoe daarbij de betrokkenheid van de volksvertegenwoordiging en de entiteiten zelf wordt gewaarborgd.

De zorgplicht is één van de hoofdelementen van de Cbw en is daarom geregeld op het niveau van een wet. De maatregelen die entiteiten moeten nemen in het kader van de wettelijke zorgplicht betreffen uitwerkingen van de zorgplicht. Daarom zijn de regels daarover opgenomen op het niveau van een

algemene maatregel van bestuur. Deze verdeling is in lijn met Aanwijzing 2.19 van de Aanwijzingen voor de regelgeving.

Voor wat betreft de betrokkenheid van de volksvertegenwoordiging wordt erop gewezen dat ervoor is gekozen om het concept van het Cbb, waarin de zorgplichtmaatregelen zijn uitgewerkt, naar de Tweede Kamer te zenden, zodat de Tweede Kamer deze algemene maatregel van bestuur kan betrekken bij de behandeling van het wetsvoorstel Cbw.[48]

Voor wat betreft de betrokkenheid van entiteiten wordt erop gewezen dat toekomstige wijzigingen van het Cbb zullen worden geconsulteerd, zoals dat ook is gedaan met het huidige concept van het Cbb. Hierdoor kan een ieder, waaronder entiteiten waarop de Cbw van toepassing is, reageren op de voorgenomen regelgeving.

De leden van de GroenLinks-PvdA-fractie hebben zorgen over de hoge regeldruk voor entiteiten. Die moeten allemaal de gelegenheid hebben om zich goed voor te bereiden op de nieuwe regelgeving. Kan de regering toelichten hoe zij (potentiële) entiteiten heeft geholpen bij het treffen van voorbereidingen voor deze wet?

Vanuit de rijksoverheid zijn door diverse organisaties tools en kennisproducten opgesteld die kunnen helpen bij het treffen van voorbereidingen op de komst van de Cbw, om daarmee de regeldruk te beperken. Hieronder volgt een overzicht daarvan:

- De rijksoverheid heeft een informatiebrochure uitgebracht die kan helpen bij het voorbereiden op de komst van de Cbw.
- Op de website van het NCSC zijn meerdere infosheets te vinden, waaronder over de zorgplicht uit de Cbw. Hierin wordt stap voor stap uitgelegd wat een entiteit kan doen om invulling te geven aan de zorgplicht uit de Cbw. Ook worden er met enige regelmaat Q&A's op de website van het NCSC geplaatst. Dat geldt ook voor de andere CSIRT's ten aanzien van sectorspecifieke Q&A's.
- Op de website van het DTC is informatie te vinden over welke maatregelen entiteiten moeten nemen om hun netwerk- en informatiesystemen te beschermen tegen incidenten.
- De RDI heeft twee tools gelanceerd om entiteiten te helpen in hun voorbereiding op de Cbw: een zelfevaluatietool[49] om te bezien of een entiteit onder de NIS2-richtlijn valt en een quickscan[50] om middels 40 vragen te beoordelen hoe de cyberbeveiliging van de entiteit ervoor staat.
- De Auditdienst Rijk (ADR) en NOREA, de beroepsorganisatie van IT-auditors in Nederland, hebben in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een *NIS2 Control Framework* ontwikkeld. Dit is bedoeld als praktisch hulpmiddel voor organisaties en IT-auditors om inzicht te krijgen in hun aanpak voor het voldoen aan de zorgplicht van de Cbw, het Cbb, relevante sectorale normen zoals de Baseline Informatiebeveiliging Overheid versie 2.0 (BIO2), en sectorale wet- en regelgeving zoals de DORA.
- Het Ministerie van Justitie en Veiligheid heeft een handreiking opgesteld om organisaties met een complexe bedrijfsstructuur te ondersteunen bij het bepalen of deze organisaties onder de Cbw vallen.

Voor sectorspecifieke vragen kunnen entiteiten te allen tijde terecht bij het ministerie dat verantwoordelijk is voor de sector waarin de entiteit actief is. De verschillende ministeries hebben hiervoor allen een webpagina ingericht.

De leden van de CDA-fractie lezen dat voor entiteiten die niet reeds onder de Wet beveiliging netwerk- en informatiesystemen (Wbni) vallen de schatting is dat zij een toename van 22% aan ICT-beveiligingskosten nodig hebben om aan de zorgplicht te voldoen. Deze leden vinden dit een stevige toename. Zij vragen of de regering met een voorbeeld wil verduidelijken hoe dit er in de praktijk voor een dergelijke entiteit uitziet. De leden vragen ook of het uiteindelijke voorstel, dat op punten afwijkt, leidt tot een extra toename van kosten en zo ja, hoeveel.

---

[48] *Kamerstukken II* 2024/25, 36765, nr. 6.

[49] Te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS-2-NL/.

[50] Te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/.

Dit percentage komt uit het impactassessment van de NIS2-richtlijn, opgesteld door de Europese Commissie.[51] De toename van 22% is gebaseerd op de toename van ICT-beveiligingskosten voor partijen die in 2017 onder het toepassingsbereik van de NIS1-richtlijn kwamen te vallen. Daarbij is aangenomen dat de implementatie van de NIS2-richtlijn voor partijen die hier nu nog niet onder vallen gelijkwaardig is. Hierbij wordt door de Europese Commissie wel de kanttekening geplaatst dat dit een conservatieve inschatting is nu er gekeken is naar de totale stijging van de kosten die niet alleen worden veroorzaakt door de implementatie van de NIS1-richtlijn. Dit betekent dat er waarschijnlijk sprake is van een overschatting van de toename van de ICT-beveiligingskosten.

In de nota van toelichting op het Cbb zijn de regeldrukkosten die bedrijven verwachten om te voldoen aan de Cbw en het Cbb uiteengezet. Daarin wordt beschreven hoe die kosten er in de praktijk uitzien voor essentiële entiteiten en belangrijke entiteiten. Er wordt onderscheid gemaakt tussen eenmalige en structurele kosten. De eenmalige kosten zijn primair het gevolg van de voorbereidingen die bedrijven moeten treffen om de voorgeschreven maatregelen ten aanzien van de zorgplicht uit te voeren, en de eenmalige meerkosten bij de implementatie van deze maatregelen. Voor de meeste bedrijven vormt het uitvoeren van een *gap assessment* en het herzien van de overeenkomsten met ketenpartners het meest kostbare onderdeel van deze voorbereiding. Gemiddeld verwachten middelgrote ondernemingen 614 uur per onderneming aan eenmalige extra tijdbesteding nodig te hebben voor de voorbereiding en implementatie van de te nemen maatregelen ten aanzien van de zorgplicht. Voor grote ondernemingen ligt dit getal aanzienlijk hoger, namelijk op gemiddeld 6.708 uur per onderneming. Naast tijdbesteding zullen bedrijven ook *out-of-pocket*-investeringen moeten doen. Wederom verwachten middelgrote ondernemingen gemiddeld lagere kosten te moeten maken dan grote ondernemingen: € 25.000,- respectievelijk € 44.400,- per bedrijf.

Naast eenmalige kosten voor het voorbereiden en implementeren van maatregelen in het kader van de zorgplicht verwachten bedrijven ook structurele meerkosten te zullen maken. Bedrijven geven aan dat zij op veel thema's die worden uitgewerkt in het Cbb al staand beleid hebben. De ISO 27001- en NEN7510-standaarden vereisen dit immers al. De structurele meerkosten voor bedrijven volgen dan ook primair uit verplichtingen die meer diepgang of een bredere scope van toepassing vereisen dan de maatregelen die bedrijven op dit moment al nemen. Hierbij gaat het onder meer om meerkosten vanwege de voorschriften over de beveiliging van de toeleveringsketen en de voorschriften op het gebied van incidentenbehandeling. Andere structurele kostenposten zijn de inhuur van een *Chief Information Security Officer* (CISO), de kosten in verband met de voorschriften over logging, en het schriftelijk vastleggen en bijhouden van het beleid in algemene zin.

Op basis van de inschattingen van de bedrijven die voor de regeldruktoets zijn geïnterviewd, zijn de gemiddelde en de totale structurele regeldrukgevolgen als gevolg van de zorgplicht berekend. Bedrijven verwachten zowel kosten te maken als gevolg van tijdbesteding om aan de zorgplicht te voldoen, alsook als gevolg van *out-of-pocket*-investeringen die gedaan zullen moeten worden. Gemiddeld verwachten middelgrote bedrijven structureel 1.246 uur per jaar kwijt te zijn aan tijdbesteding om te voldoen aan de zorgplicht. Bij grote ondernemingen ligt dit aantal aanmerkelijk hoger, namelijk op gemiddeld 3.465 uur per jaar per bedrijf. De structurele *out-of-pocket*-kosten van middelgrote en grote ondernemingen liggen niet ver uit elkaar, deze bedragen gemiddeld € 30.000,- respectievelijk € 32.800,-.

8.1.3. Meldplicht

De leden van de GroenLinks-PvdA-fractie hebben vragen over twee aannames. Ten eerste vragen zij de regering om de verwachting van circa 1.000 incidenten per jaar te onderbouwen. Ten tweede vragen zij om een onderbouwing voor de gemiddelde 480 minuten die voorzien zijn voor het oplossen van een incident.

Uit een eerdere grove schatting komt naar voren dat er circa 1.000 incidenten per jaar onder de meldplicht van de Cbw zouden kunnen vallen. Hierbij wordt wel nadrukkelijk aangetekend dat een betrouwbare schatting van dit aantal op basis van de bestaande uitvoeringspraktijk niet mogelijk is. Dit heeft onder andere te maken met nieuwe sectoren waarmee nog geen ervaring is vanuit de CSIRT's, de snelle ontwikkeling van het (cyber)dreigingslandschap, de ontwikkeling van de weerbaarheid (bijvoorbeeld

[51] Te raadplegen op https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020SC0345.

dankzij de zorgplicht uit de Cbw) en het nog ontbreken van de drempelwaarden voor incidenten die onder de meldplicht zullen vallen.

De schatting van het gemiddelde van 480 minuten voor de tijd die het entiteiten zal kosten om een melding en vervolghandelingen te doen onder de meldplicht van de Cbw is gedaan op basis van de huidige ervaringen met de Wbni en is afgestemd met het NCSC. De schatting is dat entiteiten 380 minuten kwijt zullen zijn aan het doen van de vroegtijdige waarschuwing, melding, update, initiële beoordeling, eventueel tussentijds verslag, eventueel voortgangsverslag en eindverslag en dat entiteiten 100 minuten kwijt zullen zijn aan extra handelingen op het verzoek van het CSIRT of de toezichthoudende instantie.

8.1.4. Overige verplichtingen

De leden van de GroenLinks-PvdA-fractie vragen aan de regering of het bijhouden van een database met domeinnaamregistraties geen onnodige cyberveiligheidsrisico's creëert. Hoe waarborgt de regering dat dit register goed is beveiligd?

De in artikel 49, eerste lid, Cbw opgenomen verplichting om nauwkeurige en volledige domeinnaamregistratiegegevens in een database te verzamelen en die gegevens bij te houden, geldt alleen voor registers voor topleveldomeinnamen en entiteiten die domeinnaamregistratiediensten verlenen. Aanbieders van registers voor topleveldomeinnamen, waaronder Stichting Internet Domeinregistratie Nederland (SIDN), zijn op grond van artikel 8, eerste lid, onderdeel b, Cbw van rechtswege essentiële entiteit, met als gevolg dat op hen de zorgplicht uit de Cbw (artikel 21 Cbw) van toepassing is. Daarnaast geldt voor deze aanbieders dat zij op grond van de Avg de persoonsgegevens in de database goed moeten beschermen en beveiligen.

Naar mening van de regering creëert het bijhouden van een database met domeinnaamregistraties geen onnodige cyberveiligheidsrisico's, maar komt dit juist ten goede van de cyberveiligheid. Om de beveiliging, stabiliteit en weerbaarheid van het domeinnaamsysteem (DNS) te waarborgen, is het onderhouden van een nauwkeurige en volledige database van domeinnaamregistratiegegevens en het verlenen van rechtmatige toegang tot dergelijke gegevens essentieel. Daarnaast wordt er met deze verplichting geen nieuwe database geïntroduceerd omdat deze al bestaat.

8.1.5. Toezichtslasten

De leden van de GroenLinks-PvdA-fractie plaatsen een kanttekening bij de vierjaarlijkse steekproefsgewijze audit. Deze leden vragen de regering waarom deze frequentie is gekozen, en geen hogere of lagere frequentie. Het lijkt deze leden verstandig om, indien mogelijk, vaker deze audits uit te voeren.

In paragraaf 8.1.7 van de memorie van toelichting op het wetsvoorstel is bij de berekening van de toezichtslasten aangegeven dat een steekproefsgewijze audit naar verwachting eens in de vier jaar zal worden uitgevoerd. In de Cbw is niet dwingend bepaald met welke frequentie deze audits moeten plaatsvinden. De toezichthouders bepalen risicogebaseerd en gezien de beschikbare toezichtscapaciteit wat de frequentie en intensiteit van audits en inspecties bij entiteiten zullen zijn.

De leden van de GroenLinks-PvdA-fractie vragen ook aan welke eisen de onafhankelijke en gekwalificeerde deskundige, die de audits uitvoert, moet voldoen. Is er sprake van één standaardmethodiek voor een audit?

Voor de uitvoering van audits zal worden aangesloten bij internationale standaarden en beste praktijken die passen bij het doel van de betreffende beveiligingsaudit. Er is daarom geen sprake van één standaardmethodiek. De deskundigheid van de uitvoerder van de audit zal moeten aansluiten bij het doel van de audit. Bij het auditen van managementsystemen zou bijvoorbeeld aangesloten kunnen worden bij de algemene kwaliteitseisen zoals opgenomen in de ISO 19011.

8.2. Financiële gevolgen voor de overheid

De leden van de GroenLinks-PvdA-fractie zijn bezorgd over de beschikbare IT-kennis op de arbeidsmarkt en binnen de overheid. Deze leden lezen dat het aantrekken van werknemers voor de CSIRT's de schaarste en kosten verder zal verhogen. Hoe waarborgt de regering dat het inrichten van de CSIRT's niet leidt tot een verzwakking van de IT-capaciteit en -kennis waar overheidsinstanties en entiteiten over beschikken?

De regering heeft veel aandacht voor het opbouwen en vergroten van de IT-capaciteit en -kennis. Dit doet zij door uitvoering te geven aan pijler IV van de NLCS. Pijler IV ziet op de cybersecurity-arbeidsmarkt, onderwijs en digitale weerbaarheid van burgers. Het kabinet werkt in deze pijler samen met onderwijsinstellingen aan bij- en omscholingsprogramma's om de cybersecurity-expertise van werknemers te vergroten. Ook investeert het kabinet in hbo-opleidingen in de bèta-techniek, waar cybersecurity-opleidingen ook onderdeel van zijn. Het doel is om de arbeidsmarkttekorten in te perken.

Daarnaast zet het kabinet zich via de *Human Capital Agenda ICT* in om de instroom van cybersecurityspecialisten en ICT-specialisten te vergroten en de kwaliteit van de instroom te beïnvloeden. Dit wordt in nauwe samenwerking met het bedrijfsleven, regionale en lokale overheidsinstellingen en onderwijsinstellingen opgepakt.

Het CSIRT-stelsel is vormgegeven volgens de uitgangspunten van de NLCS waarbij juist kennis en kunde wordt gebundeld, ten behoeve van een zo efficiënt mogelijke inzet.

9. Adviezen, consulatie en uitvoerings- en handhaafbaarheidstoetsen

De leden van de ChristenUnie-fractie merken voorts op dat in de memorie van toelichting niet wordt ingegaan op het advies van het Interprovinciaal Overleg (IPO) om de uitkomsten van de impactanalyse van de provincies mee te nemen in het vervolg van het wetgevingstraject. Hoe kijkt de regering naar dit advies?

Hier wordt inderdaad in de memorie van toelichting op het wetsvoorstel niet op ingegaan. Dat wil echter niet zeggen dat de bevindingen uit de impactanalyse niet zijn meegenomen. De impactanalyse, die uitwerkt wat de mogelijke gevolgen zijn van de Cbw voor de provincies, is na afronding door het Interprovinciaal Overleg (IPO) ter informatie gestuurd aan het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Waar mogelijk zijn aandachtpunten uit de impactanalyse meegenomen in het verdere wetgevingstraject. Dat is echter niet in alle gevallen even relevant. Een deel van de aandachtspunten in de impactanalyse is gericht aan de provincies zelf en enkele bevindingen zijn met de voortgang op het wetgevingstraject niet meer actueel.

9.1. Advies AP

De leden van de GroenLinks-PvdA-fractie vragen de regering om uit te leggen waarom bevoegde autoriteiten een bewaartermijn van 60 maanden opgelegd krijgen en de CSIRT een termijn van 12 maanden. Waaruit volgt dat dit tijdsbestek proportioneel is?

De regering neemt aan dat de leden van de GroenLinks-PvdA-fractie doelen op de in artikel 65, tweede en derde lid, Cbw opgenomen maximale bewaartermijnen voor de verwerking van bijzondere categorieën van persoonsgegevens door de bevoegde autoriteit en het CSIRT.

Het CSIRT verwerkt in het kader van de uitoefening van haar taken allerlei soorten gegevens, waaronder persoonsgegevens. Het gedurende een periode bewaren van deze gegevens kan in het belang zijn voor de uitoefening van die taken. In artikel 30, eerste lid, van het huidige concept van het Cbb, welke ook naar uw Kamer is gezonden, is opgenomen dat de maximale bewaartermijn voor persoonsgegevens, niet zijnde bijzondere categorieën van persoonsgegevens, die door het CSIRT worden verwerkt 60 maanden betreft. Deze maximale bewaartermijn wordt passend geacht voor de taken van het CSIRT, zoals het monitoren en analyseren van cyberdreigingen waarbij onderzoek over een langere periode noodzakelijk is om goed te kunnen kijken naar trends. Gelet op de aard van bijzondere categorieën van persoonsgegevens acht de regering een dergelijk lange termijn voor de verwerking van zulke persoonsgegevens niet passend. De regering acht een korte maximale bewaartermijn van 12 maanden voor de verwerking van bijzondere

categorieën van persoonsgegevens door het CSIRT voldoende én passend. Dit is geregeld in artikel 65, derde lid, Cbw.

Voor toezicht op en het handhavend kunnen optreden tegen bijvoorbeeld een entiteit of eventueel een bestuurder van de entiteit moet er een dossier worden opgebouwd. Voor de opbouw van een doorlopend toezichtdossier en in het kader daarvan genomen besluiten en de afhandeling van eventuele bestuursrechtelijke procedures kan het nodig zijn om toezichtinformatie lang te bewaren. Persoonsgegevens kunnen daar een onlosmakelijk onderdeel van zijn, bijvoorbeeld als onderdeel van besluiten, gespreksverslagen of opgevraagde documentatie. Het gaat daarbij met name om namen, e-mailadressen en telefoonnummers van werknemers en bestuurders van entiteiten. In artikel 30, derde lid, van het huidige concept van het Cbb is opgenomen dat een uiterlijke bewaartermijn van 120 maanden geldt ten aanzien van de persoonsgegevens, niet zijnde bijzondere categorieën van persoonsgegevens, die door de bevoegde autoriteit bij of krachtens de Cbw worden verwerkt. Dit zorgt voor een uitvoerbare praktijk en zorgt tegelijkertijd voor rechtszekerheid dat persoonsgegevens uiterlijk na 120 maanden verwijderd worden. Gelet op de aard van bijzondere categorieën van persoonsgegevens acht de regering een dergelijk lange termijn voor de verwerking van zulke persoonsgegevens niet passend. De regering acht een kortere maximale bewaartermijn van 60 maanden voor de verwerking van bijzondere categorieën van persoonsgegevens door de bevoegde autoriteit voldoende én passend. Dit is geregeld in artikel 65, tweede lid, Cbw. Dit zorgt voor een uitvoerbare toezichtspraktijk, maar ook voor rechtszekerheid dat bijzondere categorieën van persoonsgegevens uiterlijk na 60 maanden worden verwijderd door de bevoegde autoriteit.

Ten overvloede wordt opgemerkt dat de hiervoor genoemde termijnen uiterlijke en daarmee maximale bewaartermijnen betreffen. Dit laat onverlet dat conform de Cbw, het Cbb en de Avg de verwerkingsverantwoordelijke de persoonsgegevens nooit langer dan noodzakelijk voor diens taakuitvoering op grond van de wet mag bewaren, wat korter kan zijn dan de uiterlijk gestelde termijn.

9.2. Advies ATR
De leden van de GroenLinks-PvdA-fractie vragen de regering om een onderbouwing voor de termijn van vier jaar voor de evaluatiebepaling. Deze leden begrijpen dat één jaar kortdag is, maar horen graag waarom twee of drie jaar geen opties zijn. Het is voor deze leden van belang dat we snel kunnen reageren mocht blijken dat delen van de Cyberbeveiligingswet niet naar behoren werken.

In artikel 94 Cbw is bepaald dat de Cbw uiterlijk vijf jaar na de inwerkingtreding ervan wordt geëvalueerd en vervolgens elke drie jaar. De regering heeft voor deze cyclus gekozen om aan te sluiten bij de evaluatiecyclus van de Europese Commissie van de NIS2-richtlijn. De Europese Commissie zal namelijk uiterlijk op 17 oktober 2027 en vervolgens om de 36 maanden de werking van de NIS2-richtlijn evalueren (zie artikel 40 NIS2-richtlijn). Door voor de hiervoor omschreven evaluatiecyclus te kiezen, kunnen de uitkomsten van de evaluatie van de NIS2-richtlijn worden betrokken bij de evaluatie van de Cbw.

Daarnaast is ervoor gekozen om bepaalde verplichtingen, zoals de zorgplicht en meldplicht, uit te werken in lagere regelgeving. Hierdoor kunnen eventuele wijzigingen sneller worden doorgevoerd en kan er op deze wijze snel gereageerd worden op het dynamische en steeds veranderende cyberlandschap.

De leden van de VVD-fractie vragen naar aanleiding van het advies van het Adviescollege toetsing regeldruk (ATR) toe te lichten dat er op geen enkele wijze gekozen is voor zwaardere eisen dan de minimumvoorschriften uit de NIS2-richtlijn.

De regering heeft geen aanleiding gezien om te kiezen voor zwaardere eisen dan de minimumeisen van de NIS2-richtlijn. Dit wetsvoorstel bevat dan ook geen onderdelen die verder gaan dan de minimumeisen van de NIS2-richtlijn.

Ook vragen ze de mkb-toets of de AMvB tijdig kan worden gedeeld met de Kamer en waarom niet is gekozen ook om een mkb-toets op het wetsvoorstel uit te voeren.

Het Adviescollege toetsing regeldruk heeft geadviseerd om een mkb-toets uit te laten voeren voor de lagere regelgeving waarmee de verplichtingen uit de Cbw nader worden uitgewerkt. In lijn met het advies van het Adviescollege toetsing regeldruk is een mkb-toets uitgevoerd op het concept van het Cbb. Het zwaartepunt van de verplichtingen uit de Cbw die regeldruk opleveren, te weten de zorgplicht en de opleidingsverplichting voor bestuursleden, zijn namelijk uitgewerkt het Cbb.

In paragraaf 3.4 van de nota van toelichting op het Cbb is beschreven wat de belangrijkste uitkomsten van de mkb-toets zijn en op welke punten het Cbb naar aanleiding van die uitkomsten is aangepast. De toets is uitgevoerd met een panel van mkb-ondernemers die in een open en vertrouwelijk gesprek hebben meegedacht over de regelgeving. De ondernemers konden op basis van hun praktijkervaring aangeven of de plannen volgens hen werkbaar zijn, waar eventuele knelpunten zitten en hoe regeldruk voor het mkb zo veel mogelijk beperkt of voorkomen kan worden. Gezien het doel van de toets en de vertrouwelijkheid van het gesprek kan de toets niet openbaar worden gemaakt.

Overigens is de Cbw, behoudens enkele soorten entiteiten, niet van toepassing op micro- en kleine ondernemingen omdat deze niet voldoen aan de in de Cbw vereiste omvang om onder het toepassingsbereik van deze wet te vallen.

Deze leden lezen voorts dat er handreikingen zullen worden gepubliceerd die begeleiding bieden bij de implementatie van de vereisten die de Cyberbeveiligingswet bevat. Kan de regering concretiseren hoe deze handreikingen eruit zien en toezeggen dat deze na aanname van het wetsvoorstel door de Tweede Kamer zo snel mogelijk worden gepubliceerd? Wordt hierin ook aandacht besteed aan de samenloop met de implementatie van de CER-richtlijn?

Vanuit de rijksoverheid zijn, anticiperend op de komst van de Cbw, door diverse organisaties tools gelanceerd en kennisproducten gepubliceerd, die organisaties kunnen helpen bij het treffen van voorbereidingen op de komst van de Cbw. Hieronder volgt een overzicht daarvan:

- De rijksoverheid heeft een informatiebrochure uitgebracht die kan helpen bij het voorbereiden op de komst van de Cbw.
- Op de website van het NCSC zijn meerdere infosheets te vinden, waaronder over de zorgplicht uit de Cbw. Hierin wordt stap voor stap uitgelegd wat een entiteit kan doen om invulling te geven aan de zorgplicht uit de Cbw. Ook worden er met enige regelmaat Q&A's op de website van het NCSC geplaatst. Dat geldt ook voor de andere CSIRT's ten aanzien van sectorspecifieke Q&A's.
- Op de website van het DTC is informatie te vinden over welke maatregelen entiteiten moeten nemen om hun netwerk- en informatiesystemen te beschermen tegen incidenten.
- De RDI heeft twee tools gelanceerd om entiteiten te helpen in hun voorbereiding op de Cbw: een zelfevaluatietool[52] om te bezien of een entiteit onder de NIS2-richtlijn valt en een quickscan[53] om middels 40 vragen te beoordelen hoe de cyberbeveiliging van de entiteit ervoor staat.
- De Auditdienst Rijk (ADR) en NOREA, de beroepsorganisatie van IT-auditors in Nederland, hebben in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties een *NIS2 Control Framework* ontwikkeld. Dit is bedoeld als praktisch hulpmiddel voor organisaties en IT-auditors om inzicht te krijgen in hun aanpak voor het voldoen aan de zorgplicht van de Cbw, het Cbb, relevante sectorale normen zoals de Baseline Informatiebeveiliging Overheid versie 2.0 (BIO2), en sectorale wet- en regelgeving zoals de DORA.
- Het Ministerie van Justitie en Veiligheid heeft een handreiking opgesteld om organisaties met een complexe bedrijfsstructuur te ondersteunen bij het bepalen of deze organisaties onder de Cbw vallen.

Voor sectorspecifieke vragen kunnen entiteiten te allen tijde terecht bij het ministerie dat verantwoordelijk is voor de sector waarin de entiteit actief is. De verschillende ministeries hebben hiervoor allen een webpagina ingericht.

In bovenstaande tools en kennisproducten komt de samenloop met de Wwke en onderliggende regelgeving, waarin de CER-richtlijn wordt geïmplementeerd, niet aan bod. Dit wordt wél nader toegelicht

[52] Te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS-2-NL/.

[53] Te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/.

in paragraaf 2.3 van de memorie van toelichting op het wetsvoorstel Cbw. Dit komt ook aan de orde in paragraaf 2.3 van de memorie van toelichting op het wetsvoorstel Wwke.

De leden van de VVD-fractie benadrukken het belang van voldoende informatie, aangezien het onderhavige wetsvoorstel, ook in samenhang met het wetsvoorstel tot implementatie van de CER-richtlijn, ervoor kan zorgen dat entiteiten onder de verantwoordelijkheid vallen van verschillende ministers, vervolgens te maken krijgen met verschillende Computer Security Incident Response Teams (CSIRT's), verschillende toezichthouders, verschillende AMvB's en ministeriële regelingen. Dat brengt voor de uitvoerbaarheid, handhaafbaarheid, werklast en regeldruk gevolgen met zich mee. Welke aanvullende maatregelen treft de regering in aanloop naar inwerkingtreding van de twee wetsvoorstellen om zoveel mogelijk helderheid en duidelijkheid te verschaffen?

Entiteiten kunnen onder meerdere sectoren vallen en daardoor te maken hebben met verschillende bevoegde autoriteiten, verschillende CSIRT's en verschillende lagere regelgeving. Het ligt in de rede dat de instanties waarvan de ambtenaren door de vakministers worden belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw onderling werkafspraken maken om ervoor te zorgen dat zij doeltreffend en doelmatig uitvoering geven aan hun taken. Hierbij wordt onder meer gedacht aan afspraken over samenloop van toezicht op eenzelfde entiteit, het voorkomen van onevenredige toezichtslasten en de uitwisseling van gegevens. Het heeft daarbij de voorkeur dat deze afspraken worden vastgelegd in een samenwerkafspraak of een vergelijkbaar instrument en dat deze wordt gepubliceerd. Dit zorgt voor transparantie over de gemaakte afspraken en maakt voor entiteiten die onder toezicht staan helder op welke wijze invulling wordt gegeven aan voorgenoemde aspecten.

Om de doeltreffende en doelmatige uitvoering van de Cbw te borgen, moeten de CSIRT's onderling afspraken maken over gemeenschappelijke aangelegenheden. Deze afspraken worden vastgelegd in een samenwerkingsprotocol. Dit zorgt voor transparantie over de gemaakte afspraken en maakt voor de betrokken entiteiten helder op welke wijze de CSIRT's invulling geven aan voorgenoemde aspecten. Na de initiële publicatie wordt het samenwerkingsprotocol voor zover nodig geactualiseerd, bijvoorbeeld als er aanvullende CSIRT's actief worden in (sub)sectoren waar voorheen nog geen CSIRT-taken werden verricht.

De leden van de NSC-fractie lezen dat het ATR adviseert om het nut en de noodzaak van het wetsvoorstel Cyberbeveiligingswet in de memorie van toelichting beter te onderbouwen, door te verduidelijken op welke onderdelen de bestaande wetgeving tekortschiet. Deze leden vragen de regering hoe en waar in paragraaf 2.2 van de memorie van toelichting de onderbouwing is opgenomen dat de bestaande wetgeving tekortschiet. Zij vragen de regering hierbij concrete voorbeelden te geven van bestaande lacunes die met dit wetsvoorstel worden geadresseerd.

In paragraaf 2.1 van de memorie van toelichting op het wetsvoorstel is toegelicht dat de NIS1-richtlijn veel discretionaire ruimte overlaat aan de lidstaten van de Europese Unie bij de uitvoering van de richtlijn. Door die ruimte zijn er tussen lidstaten aanzienlijke verschillen ten aanzien van de implementatie van de richtlijn in de lidstaten. Zo zijn er tussen lidstaten aanzienlijke verschillen op het gebied van de afbakening van het toepassingsgebied van de NIS1-richtlijn. Dat verschil betekent concreet dat een aanbieder in de ene lidstaat wel onder de werking van de NIS1-richtlijn valt, terwijl een nagenoeg identieke aanbieder (dezelfde sector, met een soortgelijke dienstverlening, werkzaam in een soortgelijke context) uit een andere lidstaat niet onder de werking van de NIS1-richtlijn valt. Ook bestaan er aanzienlijke verschillen ten aanzien van de uitvoering van de verplichtingen op nationaal niveau, zoals het soort cyberbeveiligingseisen en de mate van gedetailleerdheid, en het toezicht op de naleving van de verplichtingen die uit de richtlijn volgen. Deze verschillen kunnen nadelige effecten hebben op de werking van de interne markt en kunnen sommige lidstaten meer kwetsbaar maken voor cyberdreigingen, met mogelijke overloopeffecten in de hele Europese Unie. Met de NIS2-richtlijn is op de hiervoor genoemde onderwerpen een eenduidig beleid gekomen, wat zorgt voor minimumharmonisatie en bijdraagt aan het bereiken van een hoog gemeenschappelijk niveau van cyberbeveiliging in de Europese Unie.[54]

9.3. Digitale sector

[54] Zie ook het fiche van de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC) over de herziening van de NIS1-richtlijn: *Kamerstukken II* 2020/21, 22112, nr. 3053.

9.3.1. Database met domeinregistratiegegevens

De leden van de GroenLinks-PvdA-fractie vragen aan de regering per wanneer afspraken worden gemaakt met de sector over de procedure rondom verificatie van domeinregistratiegegevens.

Het Ministerie van Economische Zaken voert op dit moment gesprekken met de sector over de implementatie van de artikelen 49 en 50 Cbw. De entiteiten die domeinnaamregistratiediensten verlenen hebben ook nu, vanuit contractuele verplichtingen, vaak al verificatieprocedures voor domeinnaamregistratiegegevens. De implementatie van de Cbw vereist weinig tot geen additionele procedures. Daarom worden geen problemen verwacht met betrekking tot een tijdige implementatie van de afspraken.

9.4. Zorgplicht

De leden van de GroenLinks-PvdA-fractie uiten hun twijfel over het per AMvB vastleggen van maatregelen in het kader van de zorgplicht. Hoe zorgt de regering ervoor dat zowel de Tweede Kamer als de sector betrokken blijven bij het opstellen van deze AMvB?

In het kader van de betrokkenheid van de volksvertegenwoordiging is het concept van het Cbb, waarin de zorgplichtmaatregelen zijn uitgewerkt, naar de Tweede Kamer gezonden, zodat de Tweede Kamer deze algemene maatregel van bestuur kan betrekken bij de behandeling van het wetsvoorstel Cbw.[55]

Voor wat betreft de betrokkenheid van entiteiten wordt erop gewezen dat toekomstige wijzigingen van het Cbb zullen worden geconsulteerd, zoals dat ook is gedaan met het huidige concept van het Cbb. Hierdoor kan eenieder, waaronder entiteiten waarop de Cbw van toepassing is, reageren op de voorgenomen regelgeving.

9.5. Governance

De leden van de GroenLinks-PvdA-fractie vernemen graag of de onduidelijkheden rondom de definities van bestuur reeds zijn weggenomen. Bevestigen de organisaties die hier kanttekeningen bij plaatsten dat dit nu voldoende duidelijk is?

In de consultatie van een concept van dit wetsvoorstel hebben diverse partijen specifiek gereageerd op het voorgestelde artikel met bijbehorende toelichting over de verplichting voor leden van het bestuur om een opleiding te volgen (artikel 24 van het ingediende wetsvoorstel). Naar aanleiding van die reacties is het artikel op punten aangepast en is de toelichting op het artikel aangevuld en verduidelijkt.

9.6. Meldplicht

De leden van de GroenLinks-PvdA-fractie vernemen graag van de regering aan welke randvoorwaarden voldaan moet worden om één meldportaal in te richten voor verschillende wetgeving. Is dit volgens de regering wenselijk?

De regering vindt het wenselijk om één meldportaal in te richten, zodat de regeldruk voor entiteiten zo beperkt mogelijk kan worden gehouden. De randvoorwaarden voor het inrichten van één meldportaal zien op de gebruiksvriendelijkheid, de haalbaarheid van het samenvoegen van meerdere sectorale wet- en regelgeving in het portaal, de beheerbaarheid en de beveiliging.

9.7. Handhaving

De leden van de GroenLinks-PvdA-fractie lezen dat toezichthouders een afwegingskader zullen hanteren voor het inzetten van hun handhavingsmaatregelen. Op welke wijze wordt deze vastgesteld en gepubliceerd? Deze leden hechten belang aan tijdige openbaarmaking van de afwegingskaders, om de rechtszekerheid van entiteiten te vergroten.

---

[55] *Kamerstukken II* 2024/25, 36765, nr. 6.

De instanties waarvan de ambtenaren door de vakministers worden belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw hanteren een interventiebeleid. In dat interventiebeleid wordt bepaald hoe gegeven bepaalde omstandigheden in beginsel zal worden opgetreden.

Sinds de komst van de Wbni in 2019 werken de (toezichthoudende ambtenaren van) instanties op cybersecurity van vitale processen samen in het Samenwerkend Toezicht Digitale Weerbaarheid (STDW). Met de aanstaande komst van de Cbw en Wwke heeft de RDI het initiatief genomen de samenwerking te intensiveren en is dit in de vorm van een directeurenoverleg (DTWD) opgericht. Het DTDW richt zich op de uitvoering van effectief toezicht op de (digitale) weerbaarheid.

In het STDW en DTDW werken de volgende toezichthouders samen:
- Autoriteit Nucleaire Veiligheid en Stralingsbescherming (ANVS)
- Autoriteit persoonsgegevens (AP)
- De Nederlandsche Bank (DNB)
- Inspectie Gezondheidszorg en Jeugd (IGJ)
- Inspectie Leefomgeving en Transport (ILT)
- Inspectie Justitie en Veiligheid (Inspectie JenV)
- Inspectie van het Onderwijs (IvhO)
- Nederlandse Voedsel- en Warenautoriteit (NVWA)
- Rijksinspectie Digitale Infrastructuur (RDI)
- Staatstoezicht op de Mijnen (SodM)

In de samenwerkingsverbanden STDW en DTDW stemmen de daaraan deelnemende instanties hun interventiebeleid voor de Cbw op elkaar af. Het is op dit moment nog niet bekend wanneer de instanties hun beleid zullen publiceren.

9.8. Overige opmerkingen

De leden van de GroenLinks-PvdA-fractie merken op dat er bezwaren zijn gemaakt tegen het gebrek aan een uitvoeringstoets naar het Cyberbeveiligingsbesluit. Daarmee blijven de gevolgen van de praktische uitwerking van de Cyberbeveiligingswet ongewis. Kan de regering toezeggen alsnog een nadere uitvoeringstoets uit te voeren, zodat entiteiten en medeoverheden meer zekerheid hebben vooraf aan de inwerkingtreding van de Cyberbeveiligingswet en het daarbij behorende besluit?

De betrokken vakdepartementen hebben uitvoerings- en handhaafbaarheidstoetsen laten uitvoeren op een concept van het Cbb. Een samenvatting van deze toetsen is te vinden in paragraaf 4.10 van de nota van toelichting op het Cbb. Daarnaast hebben ook de AP (zie paragraaf 4.2 van de nota van toelichting op het Cbb) en het Adviescollege toetsing regeldruk (zie paragraaf 4.3 van de nota van toelichting op het Cbb) een advies uitgebracht op een concept van het Cbb en is een concept van het Cbb geconsulteerd (zie de paragrafen 4.4 tot en met 4.9 van de nota van toelichting op het Cbb). De regering acht het dus niet nodig om een nadere uitvoeringstoets uit te voeren.

9.9. Advies Raad voor de rechtspraak

De leden van de VVD-fractie vragen of de regering nader kan toelichten waarom is gekozen voor concentratie van beroepszaken bij de rechtbank Rotterdam voor de gezondheidszorgsector, terwijl dat in andere sectoren niet het geval is? Deze leden vernemen graag een reactie van de regering.

De regering heeft er aanvankelijk voor gekozen om de beroepszaken in eerste aanleg over besluiten met betrekking tot entiteiten uit de sector gezondheidszorg te concentreren bij de rechtbank Rotterdam. De Raad voor de rechtspraak heeft echter geadviseerd om voor deze sector geen concentratiebepaling op te nemen. De regering heeft dat advies opgevolgd en door die opvolging voorziet het ingediende wetsvoorstel niet in de concentratie van beroepszaken in eerste aanleg bij de rechtbank Rotterdam, voor zover het een besluit betreft dat betrekking heeft op entiteiten uit de sector gezondheidszorg.

Het wetsvoorstel voorziet wel in de volgende bijzondere bevoegdheidsregeling:

- Voor de volgende sectoren wordt de rechtbank Rotterdam aangewezen als bevoegde rechtbank voor beroep in eerste instantie: energie, bankwezen, infrastructuur voor de financiële markt, digitale infrastructuur, beheer van ICT-diensten (business-to-business), post- en koeriersdiensten en productie, verwerking en distributie van levensmiddelen. Dit geldt ook voor de subsector spoor en de subsector vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek.
- Voor de volgende sectoren wordt het College van Beroep voor het bedrijfsleven aangewezen als hoger beroepsinstantie: energie, bankwezen, infrastructuur voor de financiële markt, digitale infrastructuur, beheer van ICT-diensten (business-to-business), post- en koeriersdiensten en productie, verwerking en distributie van levensmiddelen. Dit geldt ook voor de subsector spoor.

De reden voor deze bijzondere bevoegdheidsregeling is als volgt. Het is aannemelijk dat besluiten op grond van de Cbw in veel gevallen in samenhang met besluiten op grond van betrokken sectorale wet- en regelgeving zullen worden genomen, zoals de Postwet 2009 voor wat betreft de sector post- en koeriersdiensten. In die gevallen is het niet wenselijk dat voor besluiten op grond van sectorale wetten een bijzondere bestuursrechter bevoegd is (zoals dat bijvoorbeeld het geval is bij bepaalde besluiten op grond van de Postwet 2009, waarvan in de Awb is geregeld dat beroep kan worden ingesteld bij de rechtbank Rotterdam en hoger beroep bij het College van Beroep voor het bedrijfsleven), terwijl voor besluiten op grond van de Cbw de gewone bevoegdheidsregeling zou gelden. Voorts zal in het algemeen een goed oordeel over besluiten op grond van de Cbw niet gevormd kunnen worden zonder inzicht in de betrokken sector. Indien voor die sector een bijzondere bestuursrechter bevoegd is verklaard, zal die rechter inhoudelijke deskundigheid hebben opgebouwd ten aanzien van die sector. Het ligt dan voor de hand die rechter ook te laten oordelen over besluiten ten aanzien van die sector op grond van de Cbw.

10. Overgangsrecht en inwerktreding

De leden van de CDA-fractie vragen waarom het advies van het ATR om één jaar na invoering een invoeringstoets uit te voeren niet is overgenomen. Deze leden vragen of de regering deelt dat een evaluatie na vijf jaar iets anders is dan een invoeringstoets. Zij vragen tevens of de regering deelt dat een invoeringstoets van meerwaarde is, gezien de complexe aard van de wet en de aanzienlijke administratieve lasten die de wet met zich mee brengt.

De regering deelt de vaststelling van de leden van de CDA-fractie dat een evaluatie iets anders is dan een invoeringstoets. Een invoeringstoets is een beknopte bestudering van de werking van nieuwe regelgeving in de praktijk, met bijzondere aandacht voor de gevolgen voor de doelgroep en de uitvoering. De regering acht het wenselijk om geen lichte toets te doen zoals de invoeringstoets, maar een uitgebreidere en diepgaandere wetsevaluatie waarin onder meer elementen als doeltreffendheid en efficiëntie aan de orde zullen komen. De Cbw treft immers een aanmerkelijk deel van de Nederlandse bedrijven en organisaties. In die uitgebreidere en diepgaande wetsevaluatie zullen ook de elementen worden behandeld die in een invoeringstoets aan de orde zouden komen.

De regering kiest ervoor om in artikel 94 Cbw voor te schrijven dat de evaluatie van de Cbw binnen vijf jaar na de inwerkingtreding van de Cbw plaatsvindt en vervolgens elke drie jaar. De regering heeft hiervoor gekozen om aan te sluiten bij de evaluatiecyclus van de NIS2-richtlijn. Uit artikel 40 NIS2-richtlijn volgt dat de Europese Commissie uiterlijk op 17 oktober 2027 en vervolgens om de 36 maanden de werking van de NIS2-richtlijn evalueert.

ARTIKELSGEWIJZE TOELICHTING

Artikel 3

De leden van de GroenLinks-PvdA-fractie vragen de regering om de afweging te duiden tussen het vastleggen van maatregelen per AMvB, in plaats van deze wettelijk vast leggen. Welke voor- en nadelen heeft deze werkwijze?

De regering gaat ervan uit dat in deze vraag wordt gedoeld op de maatregelen in het kader van de zorgplicht, die zijn opgenomen in artikel 21, derde lid, Cbw en die worden uitgewerkt in het Cbb.

De zorgplicht is één van de hoofdelementen van de Cbw en is daarom geregeld op het niveau van een wet. De maatregelen die entiteiten moeten nemen in het kader van de wettelijke zorgplicht betreffen uitwerkingen van de zorgplicht. Daarom zijn de regels daarover opgenomen op het niveau van een algemene maatregel van bestuur. Deze verdeling is in lijn met Aanwijzing 2.19 van de Aanwijzingen voor de regelgeving.

Het uitwerken van de maatregelen bij algemene maatregel van bestuur heeft onder meer flexibiliteit als voordeel. Die flexibiliteit kan nodig zijn als actuele ontwikkelingen nopen tot (snelle) aanpassing van een bij algemene maatregel van bestuur uitgewerkte maatregel. Uiteraard geldt hierbij dat een algemene maatregel van bestuur tot wijziging van een bestaande algemene maatregel van bestuur, net als alle wetsvoorstellen, ter advies moet worden voorgelegd aan de Afdeling advisering van de Raad van State.

Artikel 5
De leden van de GroenLinks-PvdA-fractie vragen de regering of de uitgezonderde organisaties momenteel voldoen aan een adequate mate van beveiliging. Deze leden benadrukken dat de cyberveiligheid van deze organisaties van essentieel belang is en dat een hoog niveau van veiligheid betracht moet worden.

De meeste van de Cbw uitgezonderde organisaties vallen onder de rijksoverheid en dienen daarom te voldoen aan de Baseline Informatiebeveiliging Overheid versie 2 (BIO2), die is gebaseerd op ISO 27001 en 27002.

Artikel 4, eerste lid
De leden van de NSC-fractie lezen in artikel 4.1 dat sectorale regels geregeld kunnen worden via AMvB's. Deze leden vragen de regering hoe wordt gewaarborgd dat sectorale regels die via AMvB's worden vastgesteld op een transparante en toegankelijke wijze tot stand komen. Zij vragen daarnaast hoe betrokken organisaties invloed kunnen uitoefenen op de totstandkoming van sectorspecifieke verplichtingen. Tevens vragen zij hoe de regering voorkomt dat grote verschillen ontstaan in uitvoerbaarheid en proportionaliteit tussen sectoren.

De regering merkt op dat voor zover naar artikel 4, eerste lid, Cbw wordt verwezen, deze bepaling niet voorziet in de grondslag om sectorale regels te stellen bij algemene maatregel van bestuur.

Als het gaat om de regels die van toepassing zijn op specifieke sectoren, licht de regering het volgende toe. De Cbw en het Cbb zijn van toepassing op alle essentiële entiteiten en belangrijke entiteiten in de sectoren waarop de Cbw van toepassing is. In het Cbb staan onder meer nadere regels over de maatregelen die al deze entiteiten in het kader van de zorgplicht moeten nemen.[56] Hiermee wordt in de Cbw en het Cbb voorzien in een generiek kader voor wat betreft de zorgplicht.[57] Het is in dit kader nadrukkelijk niet het uitgangspunt dat het Cbb voorziet in regels die alleen van toepassing zijn op entiteiten in specifieke sectoren.

Artikel 20 Cbb regelt de mogelijkheid om bij ministeriële regeling van de minister die het aangaat, indien nodig, sectorspecifieke regels te stellen over de maatregelen. Dit biedt de mogelijkheid om met nadere regels te komen die nodig zijn voor een bepaalde sector.

Over de transparante en toegankelijke wijze van de totstandkoming van sectorspecifieke regelgeving – dat zal in dit geval het regelgevingsniveau van een ministeriële regeling zijn – en voor wat betreft de vraag hoe

[56] Hiervan zijn uitgezonderd: de entiteiten die in artikel 4 Cbb staan vermeld, in verband met de Uitvoeringsverordening (EU) 2024/2690 van de Commissie van 17 oktober 2024 tot vaststelling van regels voor de toepassing van Richtlijn (EU) 2022/2555 wat betreft de technische en methodologische vereisten van de maatregelen voor het beheer van cyberbeveiligingsrisico's en nadere specificatie van de gevallen waarin een incident als significant wordt beschouwd met betrekking tot DNS-dienstverleners, registers voor topleveldomeinnamen, aanbieders van cloudcomputingdiensten, aanbieders van datacentrumdiensten, aanbieders van netwerken voor de levering van inhoud, aanbieders van beheerde diensten, aanbieders van beheerde beveiligingsdiensten, aanbieders van onlinemarktplaatsen, van onlinezoekmachines en van platforms voor socialenetwerkdiensten, en verleners van vertrouwensdiensten (*PbEU* L 2024/2690).

[57] Dit behoudens de artikelen over de zorgplicht die niet van toepassing zijn op bepaalde entiteiten, geregeld in artikel 4 Cbb.

betrokken organisaties invloed kunnen uitoefenen, wordt het volgende toegelicht. De betrokken vakministers zullen, zoals dat bij alle nieuwe wet- en regelgeving wordt verlangd, bij het opstellen van de nadere sectorspecifieke regels bij ministeriële regeling telkens nadrukkelijk de aandacht hebben voor de uitvoerbaarheid van die regels, evenals de gevolgen daarvan voor sectoren. De ministeriele regelingen worden in samenspraak met de desbetreffende sectoren opgesteld en zullen ook worden geconsulteerd, waardoor betrokken organisaties de mogelijkheid krijgen om te reageren op de voorgenomen nieuwe regelgeving.

Met betrekking tot het voorkomen van het ontstaan van grote verschillen in uitvoerbaarheid en proportionaliteit tussen sectoren merkt de regering het volgende op. De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op cybersecurity en nationale veiligheid. In de praktijk betekent dit dat wanneer in de Cbw is voorgeschreven dat de vakminister nadere regels of besluiten voor zijn sector na overleg met of in overeenstemming met de Minister van Justitie en Veiligheid moet vaststellen, de Minister van Justitie en Veiligheid zal toetsen en adviseren op onder meer sectoroverstijgende effecten, de druk op het cybersecuritystelsel en de bredere impact op de nationale veiligheid. Hiermee worden grote verschillen in de uitvoerbaarheid en proportionaliteit voorkomen.

Artikel 11
De leden van de GroenLinks-PvdA-fractie vragen de regering of zij heeft overwogen de bevoegdheid tot het benomen van essentiële entiteiten binnen het hoger onderwijs bij de minister van Justitie en Veiligheid te beleggen.

De regering heeft dat niet overwogen. Bij de implementatie van de NIS2-richtlijn is er namelijk voor gekozen om aan te sluiten bij de huidige verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid, waarbij elke minister verantwoordelijk is voor de digitale weerbaarheid en de continuïteit van de sectoren binnen zijn portefeuille. Voor wat betreft het hoger onderwijs ligt die verantwoordelijkheid bij de Minister van Onderwijs, Cultuur en Wetenschap. Voorafgaand aan de aanwijzing van onderwijsinstellingen als belangrijke entiteit of als essentiële entiteit als bedoeld in de Cbw heeft de Minister van Onderwijs, Cultuur en Wetenschap overleg met de Minister van Justitie en Veiligheid, vanwege de rol van de laatstgenoemde als coördinerend bewindspersoon op het terrein van cybersecurity.

Artikel 11 & 13
Deze artikelen bevatten een grondslag voor de minister van Onderwijs, Cultuur en Wetenschap (OCW) om via een besluit of een regeling het hoger onderwijs onder de werking van de Cyberbeveiligingswet te brengen. De oud-minister van OCW heeft in het voorjaar van 2025 al aangekondigd gebruik te maken van deze regeling. De leden van de NSC-fractie vragen de regering waarom het hoger onderwijs niet direct in de wet is opgenomen als sector onder de werking van de Cyberbeveiligingswet . Zij vragen of overwogen is om het hoger onderwijs wettelijk als essentiële entiteit aan te merken, gezien de eerder aangekondigde voornemens van de minister van OCW.

Artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn biedt de lidstaten van de Europese Unie de mogelijkheid om onderwijsinstellingen onder het toepassingsbereik van de NIS2-richtlijn te brengen. In het wetsvoorstel is gebruik gemaakt van die ruimte die de NIS2-richtlijn biedt, aangezien het van belang kan zijn om deze instellingen onder de reikwijdte van de Cbw te brengen omdat het verkrijgen van hoogwaardige kennis en technologie een belangrijk doel is van statelijke actoren. Het wetsvoorstel voorziet daartoe in de bevoegdheid van de Minister van Onderwijs, Cultuur en Wetenschap om bij regeling of besluit een instelling voor hoger onderwijs aan te wijzen als belangrijke entiteit of essentiële entiteit in de zin van de Cbw. De regering heeft ervoor gekozen om de ho- en wo-instellingen niet bij wet aan te wijzen maar te voorzien in de bevoegdheid van de Minister van Onderwijs, Cultuur en Wetenschap om bij regeling of besluit aan te wijzen, om aan die minister de flexibiliteit en ruimte te bieden om naar eigen inzicht, op basis van de actuele ontwikkelingen, en na overleg met de Minister van Justitie en Veiligheid, invulling te geven aan de ruimte die de NIS2-richtlijn biedt ten aanzien van onderwijsinstellingen.

Anders dan wat de leden van de NSC-fractie veronderstellen, is door de Minister van Onderwijs, Cultuur en Wetenschap niet het voornemen aangekondigd om het hoger onderwijs aan te merken als essentiële entiteit.[58] De regering hecht eraan te benadrukken dat het besluit om de bekostigde hbo- en wo-

[58] *Kamerstukken II* 2024/25, 31288, nr. 1189.

instellingen als belangrijke entiteit of als essentiële entiteit aan te wijzen, nog moet worden genomen. Dit is onderdeel van de nadere uitwerking van het besluit om de instellingen onder de toepasselijkheid van de Cbw te brengen. De regering zal uw Kamer naar verwachting begin 2026 van de inhoud van dit besluit op de hoogte brengen.

Artikel 14
De leden van de GroenLinks-PvdA-fractie vragen de regering of de NCSC beschikt over voldoende capaciteit en kennis om hun taken naar behoren uit te voeren. Weegt de capaciteit van het NCSC mee in de keuze om vakministers verantwoordelijk te maken voor hun eigen sectoren, in plaats van de minister van Justitie en Veiligheid?

Het NCSC zal op het moment dat de Cbw in werking treedt over voldoende capaciteit en kennis beschikken om de CSIRT-taken naar behoren te kunnen uitvoeren. Hiertoe is het NCSC momenteel bezig met het uitbreiden van de capaciteit.

Bij de implementatie van de NIS2-richtlijn is ervoor gekozen om aan te sluiten bij de huidige verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid, waarbij elke minister verantwoordelijk is voor de digitale weerbaarheid en de continuïteit van de sectoren binnen zijn portefeuille. De capaciteit van het NCSC heeft geen rol gespeeld bij deze keuze.

Artikel 16
De leden van de GroenLinks-PvdA-fractie vragen de regering welke gevolgen artikel 16 heeft op de bestaande schakelorganisaties, de zogenaamde 'OKTT'-organisaties. Het is hen onduidelijk hoe de Cyberbeveiligingswet de bewezen effectieve manier van samenwerking met OKTT's beïnvloedt. Ziet de regering de mogelijkheid om de werkzaamheden van OKTT's door te zetten en in te passen in het regime dat voortvloeit uit de Cyberbeveiligingswet? De leden vragen om zo snel mogelijk inzicht te bieden in welke organisaties als 'relevante partijen' worden aangewezen per AMvB.

Een CSIRT heeft op grond van artikel 16, tweede lid, onderdeel b, Cbw de taak om vroegtijdige waarschuwingen, meldingen en aankondigingen te verstrekken en informatie te verspreiden aan essentiële entiteiten, belangrijke entiteiten, de Minister van Economische Zaken ten behoeve van de uitvoering van diens taken op grond van de Wbdwb en andere relevante partijen over cyberdreigingen, kwetsbaarheden en incidenten. De organisaties die nu op grond van de artikelen 3, tweede lid, onderdeel a, en 20, tweede lid, onderdeel a, Wbni zijn aangewezen als zogeheten OKTT (organisatie die objectief kenbaar tot taak heeft om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen) fungeren als schakelorganisatie voor een achterban van aanbieders en kunnen onder omstandigheden worden gekwalificeerd als een andere relevante partij als bedoeld in artikel 16, tweede lid, onderdeel b, Cbw. Voor het kunnen aanmerken van een schakelorganisatie als andere relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw is met name bepalend of de achterban van aanbieders bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel andere relevante partijen én of de schakelorganisatie tot taak heeft om die achterban over cyberdreigingen en -incidenten te informeren. De door het CSIRT aan een schakelorganisatie te verstrekken informatie over cyberdreigingen, kwetsbaarheden en incidenten moet immers wel verband houden met de taak van die organisatie om een achterban van die voor hen relevante informatie te voorzien. Het voorgaande betekent dat met de in artikel 16, tweede lid, onderdeel b, Cbw opgenomen mogelijkheid van het CSIRT om informatie te verstrekken aan andere relevante partijen, de bestaande samenwerking tussen het CSIRT en OKTT's kan worden gecontinueerd.

De Cbw voorziet niet in de aanwijzing van de organisaties die kwalificeren als relevante partijen in de zin van artikel 16, tweede lid, onderdeel b, Cbw. Een dergelijke aanwijzing is ook niet mogelijk, aangezien per geval moet worden bezien voor welke partij de desbetreffende informatie relevant is. Een dergelijke aanwijzing is overigens ook niet wenselijk, omdat daarmee de informatieverstrekking door CSIRT's in grote mate beperkt zal worden. Het is immers niet ondenkbaar dat informatie wel degelijk relevant blijkt te zijn voor een partij die niet formeel is aangewezen als relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw. Indien alleen informatie kan worden verstrekt aan aangewezen relevante partijen, levert

dat het risico op dat informatie niet kan belanden bij andere relevante partijen, hetgeen vervolgens kan leiden tot cyberrisico's voor die partijen.

De leden van de NSC-fractie lezen dat op grond van de Wbni bepaalde organisaties zijn aangewezen als partijen met een objectief kenbare taak (OKTT) om andere organisaties of het publiek te informeren over dreigingen en incidenten betreffende netwerk- en informatiesystemen, of als CSIRT. Deze leden willen de regering vragen om uiteen te zetten waarom deze aanwijzingen met de Cyberbeveiligingswet worden ingetrokken. Welke belemmeringen ziet de regering om de deling van dreigings- en incidentinformatie via OKTT's te continueren?

Zogeheten OKTT's (organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen) zijn op grond van de artikelen 3, tweede lid, onderdeel a, en 20, tweede lid, onderdeel a, Wbni als zodanig aangewezen in de Regeling aanwijzing schakelorganisaties cybersecurity. De Cbw regelt de intrekking van de Wbni. Dit betekent dat ook het onderliggend besluit (Besluit beveiliging netwerk- en informatiesystemen) en de onderliggende regelingen (waaronder de Regeling aanwijzing schakelorganisaties cybersecurity) komen te vervallen. Met het verval van de Regeling aanwijzing schakelorganisaties cybersecurity komt er een einde aan de formele aanwijzing van organisaties als OKTT in de zin van de Wbni.

Het voorgaande betekent echter niet dat CSIRT's geen informatie meer kunnen delen met schakelorganisaties, zoals de organisaties die op dit moment onder de Wbni zijn aangewezen als OKTT. Een CSIRT heeft op grond van artikel 16, tweede lid, onderdeel b, Cbw onder meer de taak om informatie over cyberdreigingen, kwetsbaarheden en incidenten te verspreiden aan essentiële entiteiten, belangrijke entiteiten, de Minister van Economische Zaken ten behoeve van de uitvoering van diens taken op grond van de Wbdwb en andere relevante partijen. De organisaties die nu op grond van de Wbni zijn aangewezen als OKTT fungeren als schakelorganisatie voor een achterban van aanbieders en kunnen onder omstandigheden worden gekwalificeerd als een andere relevante partij als bedoeld in artikel 16, tweede lid, onderdeel b, Cbw. Voor het kunnen aanmerken van een schakelorganisatie als andere relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw is met name bepalend of de achterban van aanbieders bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel andere relevante partijen én of de schakelorganisatie tot taak heeft om die achterban over cyberdreigingen en -incidenten te informeren. De door het CSIRT aan een schakelorganisatie te verstrekken informatie moet immers wel verband houden met de taak van die organisatie om een achterban van die voor hen relevante informatie te voorzien. Het voorgaande betekent dat met de in artikel 16, tweede lid, onderdeel b, Cbw opgenomen mogelijkheid van het CSIRT om informatie te verstrekken aan andere relevante partijen, de bestaande samenwerking tussen het CSIRT en OKTT's kan worden gecontinueerd.

Ook vragen de leden van de NSC-fractie of de regering erkent dat informatiedeling een belangrijke preventieve werking heeft en daarom zo proactief mogelijk moet plaatsvinden, ongeacht of de betrokken partijen onder de Cyberbeveiligingswet vallen. Is de regering zich ervan bewust dat het schrappen van de OKTT-status het proactieve karakter van informatiedeling voor een belangrijke doelgroep ontneemt? Acht de regering het, vanuit het perspectief van robuustheid, verstandig om bestaande structuren voor informatiedeling te behouden? Kan de regering toelichten onder welke voorwaarden organisaties die op grond van de Wbni als OKTT zijn aangewezen, kunnen worden aangemerkt als 'relevante partij'? Welke definitie hanteert de regering voor 'relevante partij'? Waarom is er niet voor gekozen om wettelijk vast te leggen dat bestaande OKTT's altijd als 'relevante partij' kwalificeren? Waarom is ervoor gekozen om de kwalificatie-eisen voor 'relevante partij' niet nader te specificeren in een AMvB?

De regering onderschrijft het belang van het delen van informatie over onder meer cyberdreigingen en kwetsbaarheden aan bedrijven en organisaties en acht gelet daarop dan ook de in artikel 16, tweede lid, onderdeel b, Cbw opgenomen taak van het CSIRT om informatie over cyberdreigingen, kwetsbaarheden en incidenten te delen met essentiële entiteiten, belangrijke entiteiten, de Minister van Economische Zaken ten behoeve van de uitvoering van diens taken op grond van de Wbdwb en andere relevante partijen van grote betekenis. De regering is het er echter niet mee eens dat met het verval van de formele aanwijzing van schakelorganisaties als zogeheten OKTT het proactieve karakter van informatiedeling wordt ontnomen. De organisaties die nu op grond van de Wbni zijn aangewezen als OKTT fungeren als

schakelorganisatie voor een achterban van aanbieders en kunnen onder voorwaarden kwalificeren als een andere relevante partij als bedoeld in artikel 16, tweede lid, onderdeel b, Cbw. Daarmee is nog steeds proactieve informatiedeling mogelijk door een CSIRT aan een dergelijke schakelorganisatie. Voor het kunnen aanmerken van een schakelorganisatie als andere relevante partij in vorenbedoelde zin, is met name bepalend of de achterban van die organisatie bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel andere relevante partijen én of de schakelorganisatie tot taak heeft om die achterban over cyberdreigingen en -incidenten te informeren. De door het CSIRT aan een schakelorganisatie te verstrekken informatie moet immers wel verband houden met de taak van die organisatie om een achterban van die voor hen relevante informatie te voorzien.

Ten aanzien van proactieve informatiedeling met het bedrijfsleven is daarnaast van belang dat de Minister van Economische Zaken op grond van de Wbdwb onverminderd tot taak zal hebben om bedrijven als bedoeld in die wet, waaronder in het bijzonder ook het mkb, informatie en advies te verstrekken over voor hen relevante dreigingen en incidenten. Een CSIRT zal op grond van artikel 16, tweede lid, onderdeel b, Cbw, net als nu geldt krachtens de Wbni, nadrukkelijk de Minister van Economische Zaken informatie verstrekken die voor de uitvoering van die taak van belang is. Daarmee blijft dus ook deze bestaande structuur voor proactieve informatiedeling behouden.

Welke partijen kwalificeren als andere relevante partij, moet per geval worden bezien. De regering hanteert hierbij geen definitie en heeft evenmin gekozen voor het in regelgeving nader specificeren van welke partijen kwalificeren als andere relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw. Dit is niet mogelijk, aangezien per geval moet worden bezien voor welke partij de desbetreffende informatie relevant is. Een dergelijke aanwijzing is ook niet wenselijk, omdat daarmee de informatieverstrekking door CSIRT's in grote mate beperkt zal worden. Het is immers niet ondenkbaar dat informatie wel degelijk relevant blijkt te zijn voor een partij die niet voldoet aan een wettelijk geregelde definitie of specificatie van relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw. Indien alleen informatie zou kunnen worden verstrekt aan partijen die voldoen aan een dergelijke definitie of specificatie, levert dat het risico op dat informatie niet kan belanden bij partijen waarvoor die informatie relevant is, hetgeen vervolgens kan leiden tot cyberrisico's voor die partijen.

De leden van de NSC-fractie vragen de regering om nader toe te lichten waarom niet is gekozen om de Wbdw zodanig te wijzigen dat OKTT's dreigings- en incidentgegevens van het NCSC kunnen blijven ontvangen, zodat zij hun informatievoorzienende rol richting het mkb kunnen blijven vervullen?

Er is geen aanleiding gezien om de Wbdwb als voorgesteld aan te passen, nu de Cbw met artikel 16, tweede lid, onderdeel b, Cbw reeds voorziet in de mogelijkheid voor een CSIRT, zoals het NCSC, om – naast essentiële entiteiten, belangrijke entiteiten en de Minister van Economische Zaken ten behoeve van de uitvoering van diens taken op grond van de Wbdwb – informatie over cyberdreigingen, kwetsbaarheden en incidenten te verstrekken aan andere relevante partijen. De organisaties die nu op grond van de Wbni zijn aangewezen als OKTT kunnen onder voorwaarden als relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw worden aangemerkt. Daarvoor is met name bepalend of de achterban van die organisatie bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel relevante partijen én of de schakelorganisatie tot taak heeft om die achterban over cyberdreigingen en -incidenten te informeren. Van belang is daarnaast dat de Minister van Economische Zaken op grond van de Wbdwb als taak blijft hebben om bedrijven als bedoeld in die wet, waaronder in het bijzonder ook het mkb, van informatie en advies te voorzien over voor hen relevante dreigingen en incidenten.

De leden van de D66-fractie vragen of de regering kan aangeven op welke manier zij uitvoering gaat geven aan artikel 16, tweede lid, onderdeel e en artikel 16, derde lid over het proactief en niet-intrusief scannen van netwerk- en informatiesystemen met het oog op het opsporen van kwetsbare of onveilig geconfigureerde systemen.

Op dit moment scant het NCSC in het kader van het vervullen van de taak als bedoeld in artikel 3, eerste lid, onderdeel e, Wbni al in bepaalde gevallen netwerk- en informatiesystemen van organisaties op kwetsbaarheden. Die scans vinden telkens plaats zonder daarbij binnen te treden in de systemen van de betrokken organisaties. Op grond van de Cbw krijgen CSIRT's de bevoegdheid om openbaar toegankelijke

netwerk- en informatiesystemen van essentiële entiteiten of belangrijke entiteiten proactief en niet-intrusief te scannen, maar ook de bevoegdheid om op verzoek van die entiteiten hun systemen te scannen op kwetsbaarheden. Op dit moment worden nadere (beleids)kaders uitgewerkt over het op grond van deze taken in de Cbw scannen naar kwetsbaarheden door een CSIRT.

De leden van de D66-fractie constateren dat de bestaande aanwijzing van organisaties die objectief kenbaar tot taak hebben om dreigingsinformatie te delen (OKTT's) vervalt en wordt vervangen door de categorie 'relevante partijen'. Deze leden vragen op welke gronden besloten is de OKTT-systematiek los te laten, welke criteria gelden exact voor aanwijzing als "relevante partij", waarom er niet voor is gekozen bestaande OKTT's bij wet automatisch onder deze nieuwe categorie te laten vallen en waarom er niet voor is gekozen de eisen voor "relevante partijen" bij AMvB te definiëren, zodat vooraf helder is wie kwalificeert? Is de regering zich ervan bewust dat door de OKTT-status te schrappen, het proactieve karakter van informatiedeling voor een doelgroep komt te vervallen?

Met betrekking tot de vraag van de leden van de D66-fractie over het loslaten van de OKTT-systematiek licht de regering het volgende toe. OKTT's (organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek te informeren over dreigingen en incidenten met betrekking tot hun netwerk- en informatiesystemen) zijn op grond van de artikelen 3, tweede lid, onderdeel a, en 20, tweede lid, onderdeel a, Wbni als zodanig aangewezen in de Regeling aanwijzing schakelorganisaties cybersecurity. De Cbw regelt de intrekking van de Wbni. Dit betekent dat ook het onderliggend besluit (Besluit beveiliging netwerk- en informatiesystemen) en de onderliggende regelingen (waaronder de Regeling aanwijzing schakelorganisaties cybersecurity) komen te vervallen. Met het verval van de Regeling aanwijzing schakelorganisaties cybersecurity komt er een einde aan de formele aanwijzing van organisaties als OKTT in de zin van de Wbni. Dit betekent echter niet dat CSIRT's geen informatie meer kunnen delen met schakelorganisaties, zoals de organisaties die op dit moment onder de Wbni zijn aangewezen als OKTT. Een CSIRT heeft op grond van artikel 16, tweede lid, onderdeel b, Cbw de taak om informatie over cyberdreigingen, kwetsbaarheden en incidenten te verspreiden aan essentiële entiteiten, belangrijke entiteiten, de Minister van Economische Zaken ten behoeve van de uitvoering van diens taken op grond van de Wbdwb en andere relevante partijen. De organisaties die nu op grond van de Wbni zijn aangewezen als OKTT fungeren als schakelorganisatie voor een achterban van aanbieders en kunnen onder omstandigheden worden gekwalificeerd als een relevante partij als bedoeld in artikel 16, tweede lid, onderdeel b, Cbw.

Op de vragen van de leden van de D66-fractie over de criteria voor aanwijzing als relevante partij en het definiëren van de eisen voor relevante partijen bij amvb is de reactie van de regering als volgt. Welke partijen kwalificeren als relevante partij, moet per geval worden bezien. De regering hanteert hierbij geen definitie en heeft evenmin gekozen voor het in regelgeving vastleggen van criteria hiervoor. Dit is niet mogelijk, aangezien per geval moet worden bezien voor welke partij de desbetreffende informatie relevant is. Dit is ook niet wenselijk, omdat daarmee de informatieverstrekking door CSIRT's in grote mate beperkt zal worden. Het is immers niet ondenkbaar dat informatie wel degelijk relevant blijkt te zijn voor een partij die niet voldoet aan een wettelijk geregelde definitie of criteria van relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw. Indien alleen informatie zou kunnen worden verstrekt aan partijen die voldoen aan een dergelijke definitie of dergelijke criteria, levert dat het risico op dat informatie niet kan belanden bij partijen waarvoor die informatie relevant is, hetgeen vervolgens kan leiden tot cyberrisico's voor die partijen.

Met betrekking tot de vraag van de leden van de D66-fractie over de keuze om bestaande OKTT's niet bij wet van rechtswege te kwalificeren als andere relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw, is de reactie als volgt. Voor het kunnen aanmerken van een schakelorganisatie als andere relevante partij in de zin van artikel 16, tweede lid, onderdeel b, Cbw is met name bepalend of de achterban van aanbieders bestaat uit essentiële entiteiten, belangrijke entiteiten dan wel relevante partijen én of de schakelorganisatie objectief kenbaar tot taak heeft om die achterban over cyberdreigingen en -incidenten te informeren. De door het CSIRT aan een schakelorganisatie te verstrekken informatie over cyberdreigingen, kwetsbaarheden en incidenten moet immers wel verband houden met de taak van die organisatie om een achterban van die voor hen relevante informatie te voorzien.

Met betrekking tot de vraag van de leden van de D66-fractie over het verval van het proactieve karakter van informatiedeling door het schrappen van de OKTT-status reageert de regering als volgt. De regering is het er niet mee eens dat met het verval van de formele aanwijzing van schakelorganisaties als zogeheten OKTT het proactieve karakter van informatiedeling wordt ontnomen. De organisaties die nu op grond van de Wbni zijn aangewezen als OKTT fungeren als schakelorganisatie voor een achterban van aanbieders en kunnen onder voorwaarden kwalificeren als een andere relevante partij als bedoeld in artikel 16, tweede lid, onderdeel b, Cbw. Daarmee is nog steeds sprake van proactieve informatiedeling door een CSIRT aan een schakelorganisatie mogelijk. Daarnaast blijft op grond van de Wbdwb gelden dat de Minister van Economische Zaken tot taak heeft om al dan niet proactief bedrijven als bedoeld in die wet informatie en advies te verstrekken over voor hen relevante dreigingen en incidenten. Hiermee blijft dus ook deze bestaande structuur voor proactieve informatiedeling behouden.

Artikel 19
De leden van de GroenLinks-PvdA-fractie vragen de regering of er, door de spreiding van verantwoordelijkheden over vakministers, aanleiding is om ook Cyberbeveiligingsstrategieën per sector vast te stellen, bovenop de nationale strategie.

De NLCS is een generiek kader. In het kader hiervan is er ruimte voor een specifieke invulling, onder andere door sectorale beleidskaders, strategieën, agenda's, routekaarten op deelonderwerpen of aanvullende normenkaders. Strategische of beleidsmatige onderwerpen dan wel onderdelen van de onderwerpen die worden genoemd in artikel 7, tweede lid, onderdeel a tot en met j, NIS2-richtlijn kunnen dan ook onder verantwoordelijkheid van andere ministers dan de Minister van Justitie en Veiligheid tot stand komen. Hiermee wordt aansluiting gezocht bij de beleidsverantwoordelijkheden van ministers zoals die op dat moment gelden. Omdat de NLCS door de Minister van Justitie en Veiligheid in overeenstemming met de betrokken vakministers wordt vastgesteld, ziet de regering geen aanleiding om ook cyberbeveiligingsstrategieën per sector vast te stellen.

Artikel 21
De leden van de GroenLinks-PvdA-fractie achten de bevoegdheid om entiteiten op te dragen om specifieke leveranciers te weren een zwaar middel. De proportionaliteit van deze maatregel vraagt om een zorgvuldige uitwerking en toelichting over hoe, wanneer en waarom de regering over zou gaan tot deze beslissing. Kan de regering een scenario schetsen waarin deze bevoegdheid wordt ingezet? Deze leden sporen de regering aan om dit de verduidelijken en begrenzing van dit artikel zo snel mogelijk per AMvB vast te leggen, zodat helderheid bestaat over de bedoeling en handhaving van dit artikel.

Artikel 18, eerste lid, Cbb voorziet in de bevoegdheid van de betrokken vakminister om een essentiële entiteit of belangrijke entiteit de verplichting op te leggen om in onderdelen van haar netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren. De regering beaamt dat de verplichting een zwaar middel betreft en benadrukt dan ook dat de verplichting alleen kan worden opgelegd als dit naar het oordeel van de vakminister noodzakelijk is om risico's voor de beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen, of om incidenten die de nationale veiligheid raken te voorkomen.

Bij de inzet van de bevoegdheid zal het moeten gaan om leveranciers die ofwel zelf de intentie hebben om de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten of belangrijke entiteiten aan te tasten of incidenten bij die entiteiten te veroorzaken, dan wel leveranciers die nauwe banden hebben met of onder controle staan van een partij met een dergelijke intentie. Hierbij is het niet van belang of een partij in laatstbedoelde zin een statelijke actor is of een andere entiteit. Van nauwe banden of controle in bovenbedoelde zin kan in het eerste geval bijvoorbeeld sprake zijn indien de leverancier afkomstig is, of onder controle staat van een partij, uit een land met wetgeving die particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder staatsorganen die zijn belast met een inlichtingen- of militaire taak. Van de intentie in bovenbedoelde zin zal in datzelfde geval sprake kunnen zijn als het land, waaruit de leverancier zelf of de partij die controle heeft over die leverancier, een actief offensief programma heeft dat is gericht op Nederland en Nederlandse belangen of een gespannen relatie met Nederland heeft, die acties die Nederlandse belangen aantasten voorstelbaar maken.

Bij de beoordeling van risico's ten aanzien van onder meer spionage en sabotage door statelijke actoren bij digitale producten en diensten hanteert het kabinet de overwegingen die zijn vermeld in de brief van de Minister van Justitie en Veiligheid aan de Tweede Kamer over C2000.[59] De criteria die in artikel 18, eerste lid, Cbb zijn vermeld zijn in lijn met de overwegingen in genoemde Kamerbrief, met dien verstande dat in overweging 3A de term "vitale infrastructurele installaties of werken" is geactualiseerd naar "kritieke infrastructuur". Het gaat om de volgende overwegingen:

1. Is de partij die de dienst of het product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of het product levert afkomstig uit een land met een actief offensief programma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

Indien het antwoord op de in bovenstaande overwegingen geformuleerde vragen positief is, zal er sprake zijn van een partij die nauwe banden heeft met of onder controle staat van een staat of entiteit die de intentie heeft om de beveiliging van de netwerk- of informatiesystemen van een essentiële entiteit of belangrijke entiteit aan te tasten of om incidenten bij die entiteit te veroorzaken, of waarvoor gronden zijn om dergelijke banden of controle te vermoeden. Dan komen de volgende overwegingen aan de orde:

3A. Krijgt de partij die de dienst of het product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of de kritieke infrastructuur, waarbij misbruik een nationaal veiligheidsrisico kan vormen?
3B. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

De reikwijdte van de op te leggen verplichting is beperkt tot die onderdelen die in de beschikking worden aangewezen. Bij de afweging welke onderdelen in de beschikking worden aangewezen, komen bovenstaande overwegingen als volgt aan bod. Eerst worden de kritieke onderdelen van de entiteit in kaart gebracht. Dit zijn de onderdelen waarvoor geldt dat de leverancier uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of de kritieke infrastructuur krijgt, waarbij misbruik een nationaal veiligheidsrisico kan vormen (overweging 3A). Vervolgens wordt beoordeeld of het opleggen van de verplichting in relatie tot die onderdelen noodzakelijk is om risico's die de nationale veiligheid raken te beheersen: dit houdt in dat er geen andere maatregelen mogelijk en realiseerbaar zijn om deze risico's voldoende te beheersen (overweging 3B). Hiertoe wordt met name de toereikendheid van de maatregelen die de essentiële entiteit of belangrijke entiteit in het kader van de wettelijke zorgplicht reeds heeft genomen of nog geacht wordt te moeten nemen in ogenschouw genomen. De kritieke onderdelen waarvoor geldt dat er geen andere beheersmaatregelen zijn om het risico voldoende te beheersen worden vervolgens aangewezen in de beschikking, waarmee de reikwijdte van de verplichting om uitsluitend gebruik te maken van vertrouwde leveranciers tot die aangewezen onderdelen is beperkt.

De volgende procesmatige stappen worden in het kader van de beoordeling in elk geval doorlopen: 1. het bepalen van het risico; 2. het plan van aanpak voor het (technisch) onderzoek; 3. het vaststellen van de kritieke onderdelen; en 4. het identificeren van de reeds getroffen en aanvullend mogelijke beveiligingsmaatregelen. De betrokken entiteit wordt hierbij zo veel als mogelijk betrokken en in de gelegenheid gesteld een zienswijze hierop te geven.

Het hiervoor geschetste beoordelingskader is ook opgenomen in de nota van toelichting op het Cbb, meer specifiek in de artikelsgewijze toelichting op artikel 18 Cbb.

Een voorbeeld van een situatie waarin de bevoegdheid uit artikel 18, eerste lid, Cbb mogelijk kan worden ingezet, is een signaal waaruit blijkt dat een type piepers die veelal in ziekenhuizen in Nederland worden gebruikt, op afstand gesaboteerd kunnen worden en door dergelijke sabotage er risico's zijn voor de

[59] *Kamerstukken II* 2018/19, 25124, nr. 96.

beveiliging van de netwerk- en informatiesystemen die de nationale veiligheid raken, of door dergelijke sabotage incidenten kunnen plaatsvinden die de nationale veiligheid raken.

Artikel 33
De leden van de GroenLinks-PvdA-fractie vragen de regering of meldingen in het kader van artikel 33 op dezelfde manier verlopen als bij artikelen 25 t/m 29.

Er is geen sprake van hetzelfde verloop, vanwege het onderscheid tussen verplichte meldingen en meldingen op vrijwillige basis. De artikelen 25 tot en met 29 Cbw zien op de wettelijke verplichting voor essentiële entiteiten en belangrijke entiteiten om significante incidenten te melden en de handelingen die deze entiteiten in dat kader moeten verrichten. Artikel 33 Cbw ziet op de mogelijkheid om op vrijwillige basis bij een CSIRT melding te doen van (al dan niet significante) incidenten, bijna-incidenten en cyberdreigingen. Artikel 33 Cbw ziet dus op vrijwillige meldingen en bevat geenszins een verplichting om een dergelijke melding op een bepaalde manier te doen.

Het CSIRT verwerkt de vrijwillige meldingen wel overeenkomstig de wijze die is voorgeschreven voor verplicht gemelde significante incidenten (advies, aanvullende ondersteuning etc.), met dien verstande dat het CSIRT daarbij voorrang kan geven aan de verwerking van verplichte meldingen.

OVERIG

De leden van de VVD-fractie vinden het belangrijk dat er in de praktijk geen verdere versnippering plaatsvindt bij zelfstandige bestuursorganen zoals toezichthouders naar aanleiding van de implementatie van het wetsvoorstel. Welke maatregelen neemt de regering om in de praktijk overlapping en versnippering tussen taken en bevoegdheden van toezichthouders te voorkomen, en welke afspraken zijn er al gemaakt tussen toezichthouders in aanloop naar de indiening van het wetsvoorstel en welke afspraken worden er in de komende periode hierover nog gemaakt? Wie is verantwoordelijk voor het toezicht op de naleving van het maken van afspraken tussen toezichthouders onderling?

Voor de beantwoording van deze vraag wordt verwezen naar het antwoord op de vraag onder 5.6.3. De samenwerking en het maken van afspraken tussen de instanties waarvan de ambtenaren naar verwachting door de vakministers worden belast met het toezicht op de naleving van de verplichtingen uit de Cbw is van groot belang en heeft derhalve vanaf de start van het wetgevingstraject de aandacht van de betrokken departementen en zal dit voor de voorziene tijd behouden.

De leden van de NSC-fractie vragen de regering waarom in de toelichting bij het wetsvoorstel beperkt aandacht wordt besteed aan het grensoverschrijdende karakter van cyberdreigingen. Deze leden vragen welke wettelijke ruimte er is om dreigings- en incidentinformatie te delen met buitenlandse (niet-EU) CERT's, multilaterale partners zoals de NAVO, en private samenwerkingspartners.

Met het oog op het in overwegende mate grensoverschrijdende karakter van cyberdreigingen en -incidenten bevat de NIS2-richtlijn, en daarmee ook de Cbw, verschillende bepalingen die ertoe strekken dat binnen de Europese Unie uitwisseling van informatie daarover zal plaatsvinden. Zo dienen alle lidstaten van de Europese Unie een centraal contactpunt aan te wijzen, dat tot taak heeft te zorgen voor grensoverschrijdende samenwerking van de nationale autoriteiten met de relevante autoriteiten van andere lidstaten, de Europese Commissie en Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging) door middel van het vervullen van een verbindingsfunctie. In samenhang hiermee is in artikel 39 Cbw geregeld dat het centrale contactpunt meldingen van cyberdreigingen en -incidenten, die zijn ontvangen van een CSIRT, ter kennis brengt van centrale contactpunten van andere lidstaten en Enisa, indien die dreigingen of incidenten grensoverschrijdend zijn en kennisneming van meldingen daarom voor andere betrokken lidstaten relevantie hebben. Ook kan worden gewezen op verschillende in de NIS2-richtlijn geregelde gremia, zoals de samenwerkingsgroep, bedoeld in artikel 14 NIS2-richtlijn, en het CSIRT-netwerk, die tot doel hebben de samenwerking en informatie-uitwisseling tussen lidstaten te bevorderen. In samenhang hiermee is in artikel 52 Cbw geregeld dat een CSIRT voor de doeltreffende en doelmatige uitvoering van haar wettelijke taken met de CSIRT's van andere lidstaten samenwerkt en in het kader van die samenwerking alle daarvoor noodzakelijke gegevens, met inbegrip van persoonsgegevens, uitwisselt.

Ten aanzien van het kunnen verstrekken van informatie over dreigingen en incidenten met CERT's (*Computer Emergency Response Teams*) in landen buiten de Europese Unie wordt in artikel 54 Cbw geregeld dat een CSIRT een samenwerkingsrelatie tot stand kan brengen met een gelijkwaardig orgaan in een land buiten de Europese Unie. Binnen die samenwerkingsrelatie kan het CSIRT relevante informatie over cyberdreigingen en -incidenten, met inbegrip van persoonsgegevens, uitwisselen. Die informatie-uitwisseling door het CSIRT moet noodzakelijk zijn voor de doeltreffende en doelmatige uitvoering van haar taken uit hoofde van de Cbw. Daarbij valt bijvoorbeeld te denken aan de situatie dat het CSIRT informatie heeft over een server die door middel van malware gegevens uitwisselt met andere servers in landen binnen en buiten de Europese Unie én het noodzakelijk is om ook CERT's buiten de Europese Unie daarover te informeren, teneinde het bestaan van genoemde kwalijke infrastructuur duurzaam te bestrijden en daarmee de daaruit voortvloeiende risico's voor Nederlandse essentiële entiteiten en belangrijke entiteiten niet te laten voortbestaan.

Voor zover het bij bovengenoemde informatie-uitwisseling gaat om de verstrekking van persoonsgegevens geldt dat naast de met artikel 54 Cbw vervatte grondslag voor het kunnen verstrekken van die gegevens, en het moeten voldoen aan de overige voor alle verwerkingen van persoonsgegevens in de Avg gestelde vereisten, op grond van de Avg ook nog specifieke eisen voor verstrekkingen aan landen buiten de Europese Unie van toepassing zijn. Voor die verstrekkingen zal op basis hiervan sprake moeten zijn van een adequaatheidsbesluit van de Europese Commissie, waaruit blijkt dat het derde land een passend beschermingsniveau heeft, of van bijvoorbeeld een ander in artikel 46 Avg genoemd juridisch instrument (bijvoorbeeld een verdrag of anderszins afdwingbaar document) waaruit ten aanzien van het derde land blijkt van passende waarborgen. Mocht van beide geen sprake zijn, dan kan doorgifte plaatsvinden in enkele in artikel 49 Avg genoemde situaties, bijvoorbeeld als doorgifte noodzakelijk is wegens gewichtige redenen van algemeen belang.

Informatie-uitwisseling tussen een CSIRT en multilaterale partners zoals de NAVO vindt plaats voor zover noodzakelijk en mogelijk krachtens de daarvoor geldende internationale verdragen. Ook voor verstrekking op grond hiervan geldt, als het gaat om persoonsgegevens, dat hierbij aan de vereisten daaraan in de Avg moet worden voldaan. In geval van informatie over een cyberdreiging of -incident, met inbegrip van persoonsgegevens, die mogelijk relevantie heeft voor private partijen buiten Nederland, kan het CSIRT die informatie met inachtneming van bovengenoemde wettelijke bepalingen verstrekken aan het CSIRT van de betrokken lidstaat van de Europese Unie dan wel het CERT van het betrokken land buiten de Europese Unie. Daarmee kunnen zij (CSIRT van de betrokken lidstaat of CERT van het land buiten de Europese Unie) in het kader van de vervulling van hun respectievelijke taken die private partijen voor zover nodig informeren en adviseren. Ook kan daarmee worden bewerkstelligd dat informatie van die private partijen terugkomt doordat het CSIRT van de betrokken lidstaat of het CERT deze informatie (terug)verstrekt aan het Nederlandse CSIRT en het Nederlandse CSIRT op haar beurt deze informatie verstrekt aan de Nederlandse partijen waarvoor die informatie relevant is.

De leden van de NSC-fractie vragen de regering hoe wordt gewaarborgd dat Nederland bij internationale cyberincidenten snel en effectief kan schakelen met relevante partijen buiten de EU. Deze leden vragen tevens hoe de aansluiting wordt geborgd met niet-EU-certificeringsinstanties, internationale normenkaders en buitenlandse CERT's.

Zoals hierboven in het antwoord op de vorige vraag van de leden van de NSC-fractie is aangegeven, wordt in artikel 54 Cbw geregeld dat een CSIRT kan samenwerken met een gelijkwaardig orgaan, zoals een CERT, in een land buiten de Europese Unie en in het kader daarvan relevante informatie over onder meer internationale cyberincidenten kan uitwisselen. Daarbij geldt dat die informatie-uitwisseling mogelijk is indien dat noodzakelijk is voor de doeltreffende en doelmatige uitvoering van de taken van het CSIRT. Ook geldt dat bij de verstrekking van persoonsgegevens in het kader daarvan aan zowel de reguliere vereisten in de Avg als de specifiek voor verstrekkingen aan landen buiten de Europese Unie geldende vereisten moet worden voldaan. Met inachtneming hiervan kan het CSIRT een CERT in een land buiten de Europese Unie in de gelegenheid brengen om op basis van de ontvangen informatie private en publieke partijen in dat land over een cyberincident te informeren en te adviseren. Ook kan hiermee worden bewerkstelligd

dat informatie van die private en publieke partijen terugkomt doordat het CERT deze informatie (terug)verstrekt aan het Nederlandse CSIRT.

Voor niet EU-certificeringsinstanties geldt dat zij geen rol hebben in de afhandeling van internationale cyberincidenten en dat samenwerking met een CSIRT in die gevallen dus niet aangewezen is. Hoewel internationale normenkaders zoals ISO 27001 van belang zijn om te bepalen of de beveiliging van netwerk- en informatiesystemen van een partij op orde is, en zodoende ook kunnen bijdragen aan het waar nodig kunnen uitwisselen van informatie, zijn zij voor het afhandelen van een internationaal incident niet noodzakelijk.

De leden van de CDA-fractie hebben nog enkele vragen over het Cyberbeveiligingsbesluit en het Besluit weerbaarheid kritieke entiteiten. Deze leden vragen of de regering kan aangeven wat de reden is geweest om de interventiebevoegdheid van vakministers - om aan bedrijven de verplichting op te leggen om producten of diensten van specifieke leveranciers te weren dan wel te verwijderen - te introduceren in een AMvB.

Aanwijzing 2.19 van de Aanwijzingen voor de regelgeving schrijft voor dat bij de verdeling van de elementen van een regeling over de wet en algemeen verbindende voorschriften van lager niveau, de wet ten minste de hoofdelementen bevat van de regeling. De zorgplicht in het kader van de Cbw (artikel 21 Cbw) en de zorgplicht in het kader van de Wwke (artikel 15 Wwke) betreffen één van de hoofdelementen van de betreffende wet en zijn, ook rekening houdend met de hiervoor genoemde aanwijzing, daarom geregeld op het niveau van een wet. De bedoelde bevoegdheid van de vakminister betreft een uitwerking van de wettelijke zorgplicht en wordt daarom op het niveau van een algemene maatregel van bestuur geregeld.

De leden van de CDA-fractie vragen waarom de regering dit onderdeel heeft toegevoegd na de internetconsultatieronde, waardoor het bedrijfsleven hier geen zienswijze op heeft kunnen geven. Deze leden vragen op welke manier overleg en informatievoorziening tussen de vakministers en het bedrijfsleven geborgd is met de voorgestelde interventiebevoegdheid. Zij vragen wat het effect is op de eisen die zijn gesteld rondom het opmaken van een risicoanalyse. Verder vragen zij of de regering kan ingaan op de wijze waarop de interventiebevoegdheid kan worden ingezet en wat de eisen hiervoor zijn.

Nederland wordt steeds vaker geconfronteerd met cyberaanvallen op (al dan niet vitale) processen door statelijke en criminele actoren.[60] Naar verwachting zal de cyberdreiging de komende jaren aanhouden, omdat het relatief makkelijk is om een digitaal aanvalsprogramma op te zetten. Dergelijke aanvallen zijn ook steeds moeilijker herleidbaar tot de aanvaller. De inlichtingen- en veiligheidsdiensten identificeren in hun meest recente jaarverslagen een sterke toename van het aantal landen dat offensieve cyberprogramma's ontwikkelt en inzet bij het nastreven van hun politieke doelstellingen. In het licht van de hiervoor bedoelde ontwikkelingen, aanvallen en dreigingen voorziet artikel 18, eerste lid, Cbb in de bevoegdheid van de betrokken vakminister om, in overeenstemming met de Minister van Justitie en Veiligheid, een essentiële entiteit of belangrijke entiteit de verplichting op te leggen om in onderdelen van haar netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren en zo de risico's, die voortvloeien uit de hiervoor bedoelde offensieve cyberprogramma's, te beheersen.

Artikel 18 Cbb was ten tijde van de internetconsultatie nog niet gereed. Dit artikel is na de internetconsultatie, zodra het gereed was, toegevoegd aan het Cbb, waarna dat concept van het Cbb naar uw Kamer is gezonden. Diverse organisaties hebben daarop vernomen van de in artikel 18 Cbb geregelde bevoegdheid en hebben bij brief gereageerd op die bevoegdheid. De regering heeft die brieven bezien en indien nodig verwerkt in het concept van het Cbb.

Artikel 18, eerste lid, Cbb voorziet in de bevoegdheid van de betrokken vakminister om een essentiële entiteit of belangrijke entiteit de verplichting op te leggen om in onderdelen van haar netwerk- en informatiesystemen producten of diensten van specifieke leveranciers te weren. De regering beaamt dat de verplichting een zwaar middel betreft en benadrukt dan ook dat de verplichting alleen kan worden opgelegd als dit naar het oordeel van de vakminister noodzakelijk is om risico's voor de beveiliging van de

[60] *Kamerstukken II* 2022/23, 26643, nr. 1007.

netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen, of om incidenten die de nationale veiligheid raken te voorkomen.

Bij de inzet van de bevoegdheid zal het moeten gaan om leveranciers die ofwel zelf de intentie hebben om de beveiliging van de netwerk- en informatiesystemen van essentiële entiteiten of belangrijke entiteiten aan te tasten of incidenten bij die entiteiten te veroorzaken, dan wel leveranciers die nauwe banden hebben met of onder controle staan van een partij met een dergelijke intentie. Hierbij is het niet van belang of een partij in laatstbedoelde zin een statelijke actor is of een andere entiteit. Van nauwe banden of controle in bovenbedoelde zin kan in het eerste geval bijvoorbeeld sprake zijn indien de leverancier afkomstig is, of onder controle staat van een partij, uit een land met wetgeving die particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder staatsorganen die zijn belast met een inlichtingen- of militaire taak. Van de intentie in bovenbedoelde zin zal in datzelfde geval sprake kunnen zijn als het land, waaruit de leverancier zelf of de partij die controle heeft over die leverancier, een actief offensief programma heeft dat is gericht op Nederland en Nederlandse belangen of een gespannen relatie met Nederland heeft, die acties die Nederlandse belangen aantasten voorstelbaar maken.

Bij de beoordeling van risico's ten aanzien van onder meer spionage en sabotage door statelijke actoren bij digitale producten en diensten hanteert het kabinet de overwegingen die zijn vermeld in de brief van de Minister van Justitie en Veiligheid aan de Tweede Kamer over C2000.[61] De criteria die in artikel 18, eerste lid, Cbb zijn vermeld zijn in lijn met de overwegingen in genoemde Kamerbrief, met dien verstande dat in overweging 3A de term "vitale infrastructurele installaties of werken" is geactualiseerd naar "kritieke infrastructuur". Het gaat om de volgende overwegingen:

1. Is de partij die de dienst of het product levert afkomstig, of staat hij onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf?
2. Is de partij die de dienst of het product levert afkomstig uit een land met een actief offensief programma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn?

Indien het antwoord op de in bovenstaande overwegingen geformuleerde vragen positief is, zal er sprake zijn van een partij die nauwe banden heeft met of onder controle staat van een staat of entiteit die de intentie heeft om de beveiliging van de netwerk- of informatiesystemen van een essentiële entiteit of belangrijke entiteit aan te tasten of om incidenten bij die entiteit te veroorzaken, of waarvoor gronden zijn om dergelijke banden of controle te vermoeden. Dan komen de volgende overwegingen aan de orde:

3A. Krijgt de partij die de dienst of het product levert uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of de kritieke infrastructuur, waarbij misbruik een nationaal veiligheidsrisico kan vormen?
3B. Zijn er beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's die in het geding zijn voldoende beschermen?

De reikwijdte van de op te leggen verplichting is beperkt tot die onderdelen die in de beschikking worden aangewezen. Bij de afweging welke onderdelen in de beschikking worden aangewezen, komen bovenstaande overwegingen als volgt aan bod. Eerst worden de kritieke onderdelen van de entiteit in kaart gebracht. Dit zijn de onderdelen waarvoor geldt dat de leverancier uitgebreide toegang tot gevoelige locaties, gevoelige ICT-systemen of de kritieke infrastructuur krijgt, waarbij misbruik een nationaal veiligheidsrisico kan vormen (overweging 3A). Vervolgens wordt beoordeeld of het opleggen van de verplichting in relatie tot die onderdelen noodzakelijk is om risico's die de nationale veiligheid raken: dit houdt in dat er geen andere maatregelen mogelijk en realiseerbaar zijn om deze risico's voldoende te beheersen (overweging 3B). Hiertoe wordt met name de toereikendheid van de maatregelen die de essentiële entiteit of belangrijke entiteit in het kader van de wettelijke zorgplicht reeds heeft genomen of nog geacht wordt te moeten nemen in ogenschouw genomen. De kritieke onderdelen waarvoor geldt dat er geen andere beheersmaatregelen zijn om het risico voldoende te beheersen worden vervolgens

[61] *Kamerstukken II* 2018/19, 25124, nr. 96.

aangewezen in de beschikking, waarmee de reikwijdte van de verplichting om uitsluitend gebruik te maken van vertrouwde leveranciers tot die aangewezen onderdelen is beperkt.

De volgende procesmatige stappen worden in het kader van de beoordeling in elk geval doorlopen: 1. het bepalen van het risico; 2. het plan van aanpak voor het (technisch) onderzoek; 3. het vaststellen van de kritieke onderdelen; en 4. het identificeren van de reeds getroffen en aanvullend mogelijke beveiligingsmaatregelen. De betrokken entiteit wordt hierbij zo veel als mogelijk betrokken en in de gelegenheid gesteld een zienswijze hierop te geven.

Het hiervoor geschetste beoordelingskader is ook opgenomen in de nota van toelichting op het Cbb, meer specifiek in de artikelsgewijze toelichting op artikel 18 Cbb.

De in artikel 18, eerste lid, Cbb opgenomen bevoegdheid voor de vakministers heeft geen effect op de verplichting voor essentiële entiteiten en belangrijke entiteiten tot het opstellen van een risicoanalyse die onderdeel is van de zorgplicht van artikel 21 Cbw.

De leden van de CDA-fractie vragen of het in lijn is met de wettelijke waarborgen om de interventiebevoegdheid onder te brengen in een AMvB, in plaats van in het wetsvoorstel zelf. Deze leden vragen of de regering in dat licht ook kan reflecteren op artikel 21 van de Cyberbeveiligingswet en artikel 15 van de Wwke.

Aanwijzing 2.19 van de Aanwijzingen voor de regelgeving schrijft voor dat bij de verdeling van de elementen van een regeling over de wet en algemeen verbindende voorschriften van lager niveau, de wet ten minste de hoofdelementen bevat van de regeling. De zorgplicht in het kader van de Cbw (artikel 21 Cbw) en de zorgplicht in het kader van de Wwke (artikel 15 Wwke) betreffen één van de hoofdelementen van de betreffende wet en zijn, ook rekening houdend met de hiervoor genoemde aanwijzing, daarom geregeld op het niveau van een wet. De maatregelen die entiteiten moeten nemen in het kader van de wettelijke zorgplicht en de in de vraagstelling bedoelde bevoegdheid van de vakminister betreffen uitwerkingen van de zorgplicht. Daarom zijn de regels daarover opgenomen op het niveau van een algemene maatregel van bestuur. Deze verdeling van elementen tussen de wet en algemene maatregel van bestuur botst niet met de hiervoor genoemde aanwijzing. Hierbij wordt overigens ook opgemerkt dat de opname van de bevoegdheid in een algemene maatregel van bestuur, ter uitwerking van de wettelijke zorgplicht, uiteraard geen onderwerp betreft waarvoor een grondwettelijk delegatieverbod geldt.

De Minister van Justitie en Veiligheid,