Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2025-2026

36 764 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)

C **NOTA NAAR AANLEIDING VAN HET VERSLAG**
Ontvangen 17 juni 2026

Hierbij bied ik u de nota naar aanleiding van het verslag op het voorstel van wet 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, *Kamerstukken* 36764) aan.

Graag wil ik uw Kamer vragen om de behandeling van dit wetsvoorstel spoedig voort te zetten, omdat de implementatietermijn van de hiervoor genoemde richtlijn reeds geruime tijd is overschreden.

De Minister van Justitie en Veiligheid,

D.M. van Weel

NOTA NAAR AANLEIDING VAN HET VERSLAG

Met belangstelling heb ik kennisgenomen van het verslag van de vaste commissies voor Digitalisering en Justitie & Veiligheid op het wetsvoorstel voor de 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 commissies 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.

1. Inleiding

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van de Cyberbeveiligingswet. Deze leden onderschrijven het belang van een hoog niveau van cyberweerbaarheid, maar hebben nog enkele vragen.

Deze leden constateren dat voor de NIS2-richtlijn de omzettermijn 17 oktober 2024 is overschreden en ten aanzien van deze richtlijn inmiddels een inbreukprocedure is gestart door de Europese Commissie. Deze leden onderschrijven het belang van tijdige omzetting van Europese richtlijnen in nationale regelgeving en vragen de regering te reflecteren op het niet halen van de omzettermijnen en vragen de regering om dit nader toe te lichten.

De regering onderschrijft, met de leden van de CDA-fractie, het belang van tijdige omzetting van Europese richtlijnen in nationale regelgeving. Daarom is de regering ruim voor de formele vaststelling van de NIS2-richtlijn gestart met de voorbereidingen voor de benodigde implementatiewetgeving. Ook heeft de regering daarbij vastgehouden aan het principe van zuivere implementatie, wat inhoudt dat in de implementatieregelingen geen andere regels worden opgenomen dan voor implementatie noodzakelijk zijn, zodat implementatie zo spoedig mogelijk kan plaatsvinden. Bij het implementatieproces van de NIS2-richtlijn heeft de regering telkens bezien wanneer en in hoeverre een versnelling van dat proces mogelijk was. In dat licht heeft de regering de Afdeling advisering van de Raad van State gevraagd om met spoed te adviseren op het concept van het wetsvoorstel waarmee de NIS2-richtlijn wordt geïmplementeerd. Ook is in de Tweede Kamer het belang van een spoedige behandeling van het wetsvoorstel onder de aandacht gebracht. Hierbij onderkent de regering uiteraard dat het primaat van de parlementaire behandeling bij de Tweede Kamer en de Eerste Kamer zelf ligt.

De regering onderschrijft naast het belang van tijdige omzetting van de NIS2-richtlijn ook het belang van een zorgvuldige totstandkoming van de implementatiewetgeving, hetgeen tijd kost. Die zorgvuldigheid is nodig omdat de wet- en regelgeving waarmee de NIS2-richtlijn wordt geïmplementeerd, grote impact heeft op de vele bedrijven en organisaties die onder het toepassingsbereik daarvan komen te vallen, zowel in de private als in de publieke sector. De Cbw (waarmee de NIS2-richtlijn wordt geïmplementeerd) is van toepassing op circa 8.100 Nederlandse bedrijven en organisaties, uit maar liefst 18 sectoren. Deze duizenden Nederlandse bedrijven en organisaties zullen met de komst van de Cbw onder meer diverse verplichtingen opgelegd krijgen, waar op de naleving toezicht plaatsvindt. Vanwege de hiervoor benoemde grote impact op duizenden Nederlandse bedrijven en organisaties, is de totstandkoming van het wetsvoorstel voor de Cbw, evenals de onderliggende regelgeving, zorgvuldig aangepakt. Dat heeft de nodige tijd gekost. Zo is het bedrijfsleven actief betrokken geweest, bijvoorbeeld met interviews. Ook heeft de regering besloten om het wetsvoorstel en de ontwerpen van de onderliggende regelgeving open te stellen voor internetconsultatie, zodat een ieder daarop kon reageren. Internetconsultatie is bij implementatiewetgeving niet verplicht en kan omwille van de snelheid van de totstandkoming van implementatiewetgeving worden overgeslagen. Toch heeft de regering de afweging gemaakt om deze stap niet over te slaan, vanwege het belang dat bedrijven en organisaties de mogelijkheid zouden krijgen om te reageren op de concepten van het wetsvoorstel en de onderliggende regelgeving. De regering heeft alle ontvangen consultatiereacties bezien en overwogen of naar aanleiding van die reacties het wetsvoorstel of de bijbehorende toelichting op punten moeten worden aangepast. Dat laatste is ook gebeurd; de internetconsultatie heeft, tezamen met de formele consultatie, geleid tot vele nuttige reacties, die op hun beurt hebben geleid tot aanpassing van het wetsvoorstel of aanpassing, verscherping of verduidelijking in de bijbehorende memorie van toelichting. Het voorgaande geldt ook voor de onderliggende regelgeving.

[1] *PbEU* 2022, L 333.

Het voorgaande maakt dan ook dat de implementatietermijn van nog geen twee jaar voor de NIS2-richtlijn te kort is gebleken in het licht van de tijd die nodig was voor zorgvuldige totstandkoming van wetgeving, rekening houdend met de impact daarvan op bedrijven en organisaties en met het doorlopen van de verplichte (en belangrijke) wetgevingsstappen (advisering door de Afdeling advisering van de Raad van State en behandeling in de Tweede Kamer en Eerste Kamer). Het is Nederland ondanks alle inspanningen dan ook niet gelukt om de richtlijn tijdig te implementeren. Nederland is binnen de Europese Unie daar niet de enige in: naast Nederland hebben 22 andere lidstaten van de Europese Unie de NIS2-richtlijn niet tijdig geïmplementeerd. De regering benadrukt dat het benoemen van deze aantallen absoluut geen excuus is om zelf ook niet tijdig te implementeren, maar wijst erop dat deze grote aantallen wel een indicatie geven van de complexiteit en haalbaarheid om binnen de gegeven implementatietermijn de richtlijn te implementeren, wat dus ook het merendeel van de lidstaten niet is gelukt.

Tot slot merkt de regering op dat op het moment van schrijven nog geen inbreukprocedure door de Europese Commissie is gestart vanwege de te late implementatie van de NIS2-richtlijn. Dit is wel het geval ten aanzien van de CER-richtlijn, die wordt geïmplementeerd in de Wet weerbaarheid kritieke entiteiten (hierna: Wwke).[2]

Kan de regering aan de leden van de fractie van de VVD bevestigen dat inwerkingtreding in het tweede kwartaal van 2026 haalbaar is, gezien de ingebrekestelling door de Europese Commissie en de benodigde amvb's?

De leden van de VVD-fractie hebben terecht aandacht voor de inwerkingtreding van de implementatiewetgeving. De regering onderschrijft het belang dat de Cbw zo snel als mogelijk in werking treedt, vanwege het overschrijden van de implementatietermijn van de NIS2-richtlijn en het belang van deze wet voor de digitale veiligheid van Nederland. Inwerkingtreding in het tweede kwartaal van 2026 is helaas niet meer haalbaar. De regering acht echter de inwerkingtreding halverwege het derde kwartaal van 2026 haalbaar indien het voorliggend wetsvoorstel voor de start van het zomerreces van de Eerste Kamer tot stemming wordt gebracht en wordt aangenomen. In dat geval wordt voorzien dat de Cbw en onderliggende regelgeving in werking treden op 15 augustus 2026. Of het voorliggend wetsvoorstel voor de start van het zomerreces tot stemming wordt gebracht, is uiteraard een beslissing van uitsluitend de Eerste Kamer.

Hierbij wordt opgemerkt dat op het moment van schrijven nog geen inbreukprocedure door de Europese Commissie is gestart vanwege de te late implementatie van de NIS2-richtlijn. Dit is wel het geval ten aanzien van de CER-richtlijn.

Welke overgangstermijn hanteert de regering voor entiteiten die nieuw onder de werkingssfeer vallen en hoe wordt voorkomen dat met name MKB-entiteiten en gemeenten overvraagd worden?

De Cbw bevat geen overgangstermijn, omdat een dergelijk termijn tot gevolg heeft dat Nederland de NIS2-richtlijn gedurende die termijn nog steeds niet heeft geïmplementeerd. Bovendien vindt de regering het belangrijk dat de regels die voortvloeien uit de NIS2-richtlijn zo snel mogelijk van toepassing zijn op de bedrijven en organisaties die onder deze richtlijn vallen. Hierop geldt overigens een uitzondering voor hogeronderwijsinstellingen die op grond van artikel 11 Cbw worden aangewezen als essentiële entiteit of op grond van artikel 13 Cbw worden aangewezen als belangrijke entiteit. Artikel 97 Cbw bepaalt dat de zorgplicht ten aanzien van die instellingen van toepassing is vanaf 36 maanden na de hiervoor bedoelde aanwijzing. Deze specifieke regeling voor onderwijsinstellingen is mogelijk, omdat de in de artikelen 11 en 13 Cbw opgenomen bevoegdheid tot aanwijzing voortvloeit uit een mogelijkheid die artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn hiertoe biedt.

Er is bij het opstellen van deze wet- en regelgeving nadrukkelijk oog geweest voor de administratieve last en de regeldruk die organisaties zullen ervaren als gevolg daarvan. Er is gekozen voor een risicogebaseerde aanpak, zodat bedrijven en organisaties ruimte hebben om risicogebaseerd een eigen invulling te geven aan de verplichte maatregelen. Deze risicogebaseerde aanpak biedt ruimte om gezien de context van de organisatie tot de meest (kosten) effectieve oplossing te komen. Bij de beoordeling welke specifieke passende en evenredige maatregelen genomen moeten worden, kunnen zij gebruik maken van bestaande normenkaders, zoals ISO27001. Vanuit de rijksoverheid zijn voorts diverse tools en kennisproducten opgesteld die kunnen helpen bij het voldoen aan de zorgplicht uit de Cbw. Hieronder volgt een overzicht daarvan:

- Op de website van het Nationaal Cyber Security Centrum (hierna: NCSC) zijn meerdere infosheets te vinden over de zorgplicht uit de Cbw. Hierin wordt stap voor stap uitgelegd wat

[2] Richtlijn (EU) 2022/2557 van het Europees Parlement en de Raad van 14 december 2022 betreffende de weerbaarheid van kritieke entiteiten en tot intrekking van Richtlijn 2008/114/EG van de Raad (*PbEU* 2022, L 333).

een entiteit kan doen om invulling te geven aan die verplichting. Ook worden er met enige regelmaat Q&A's hierover op de website van het NCSC geplaatst.

- De Rijksinspectie Digitale Infrastructuur (hierna: RDI) heeft een quickscan ontwikkeld waarmee entiteiten aan de hand van 40 vragen kunnen beoordelen hoe het met hun cyberbeveiliging ervoor staat.[3]
- 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 onder andere hun aanpak voor het voldoen aan de zorgplicht uit de Cbw.

Het bedrijfsleven is in dit wetgevingstraject actief betrokken geweest, onder meer met interviews. Ook heeft de regering besloten om het wetsvoorstel en de ontwerpen van de onderliggende regelgeving open te stellen voor internetconsultatie, zodat een ieder daarop kon reageren.

Om de lasten voor medeoverheden te beperken, is ervoor gekozen om in de ministeriële regelingen onder de Cbw die voor entiteiten uit de sector overheid zullen gelden, zoveel mogelijk aan te sluiten bij reeds voor hen geldende verplichtingen en kaders. Zo wordt voor de nadere invulling van de zorgplicht, bedoeld in artikel 21 Cbw, bepaald dat zij, in aanvulling op de maatregelen zoals beschreven in het Cyberbeveiligingsbesluit (hierna: Cbb), meer specifiek moeten voldoen aan de Baseline Informatiebeveiliging Overheid versie 2.0 (hierna: BIO2). Dat is het bestaande normenkader voor informatiebeveiliging waaraan alle overheidslagen zich hebben gecommitteerd.[4] Ook voor het bepalen van de drempelwaarden in het kader van de meldplicht is zoveel mogelijk aangesloten bij bestaande uitgangspunten. Hiervoor worden criteria gebruikt op basis waarvan gemeenten reeds hun incidentmeldingen doen bij de Informatiebeveiligingsdienst (IBD).

De leden van de D66-fractie hebben met belangstelling kennisgenomen van het voorstel voor de Cyberveiligheidswet. Deze leden onderstrepen het belang van het beschermen en bevorderen van onze fysieke en digitale veiligheid. Dit geldt al helemaal in deze roerige tijden. Wel hebben deze leden nog enkele vragen over de uitvoering van deze wet.

De leden van de PVV-fractie hebben met interesse kennisgenomen van de Cyberbeveiligingswet en de daarbij horende stukken. Deze leden hebben buiten het voorstel tevens kennisgenomen van het feit dat de Europese Commissie Nederland voor het Hof van Justitie van de EU daagt vanwege het uitblijven van de volledige implementatie van de CER-richtlijn. Nederland loopt ver voorop waar het gaat om digitale veiligheid en cybersecurity. Deelt de regering de zorg van deze leden dat gezwinde spoed afbreuk doet aan een kwalitatief adequate implementatie en daarmee de digitale weerbaarheid en cyberveiligheid van Nederland en is zij voornemens deze houding stellig te veroordelen? Deze leden lezen graag een gedegen onderbouwing van de beantwoording.

Het is belangrijk dat de NIS2-richtlijn en de CER-richtlijn spoedig worden geïmplementeerd, maar het is óók belangrijk dat implementatiewetgeving zorgvuldig tot stand komt. Die zorgvuldigheid is nodig omdat de wet- en regelgeving waarmee de NIS2-richtlijn en de CER-richtlijn worden geïmplementeerd, grote impact hebben op de vele bedrijven en organisaties die onder het toepassingsbereik daarvan komen te vallen, zowel in de private als in de publieke sector. De Wwke (waarmee de CER-richtlijn wordt geïmplementeerd) is van toepassing op circa 500 Nederlandse bedrijven en organisaties, uit 11 sectoren. De Cbw (waarmee de NIS2-richtlijn wordt geïmplementeerd) is van toepassing op circa 8.100 Nederlandse bedrijven en organisaties, uit maar liefst 18 sectoren. Deze duizenden Nederlandse bedrijven en organisaties zullen met de komst van de Cbw en de Wwke onder meer diverse verplichtingen opgelegd krijgen, waar op de naleving toezicht plaatsvindt.

Vanwege de hiervoor benoemde grote impact op duizenden Nederlandse bedrijven en organisaties, is de totstandkoming van de wetsvoorstellen voor de Cbw en de Wwke, evenals de onderliggende regelgeving, zorgvuldig aangepakt. Dat heeft helaas de nodige tijd gekost. Zo is het bedrijfsleven actief betrokken geweest, bijvoorbeeld met interviews. Ook heeft de regering besloten om de wetsvoorstellen en de ontwerpen van de onderliggende regelgeving open te stellen voor internetconsultatie, zodat een ieder daarop kon reageren. Internetconsultatie is bij implementatiewetgeving niet verplicht en kan omwille van de snelheid van de totstandkoming van implementatiewetgeving worden overgeslagen. Toch heeft de regering de afweging gemaakt om deze stap niet over te slaan, vanwege het belang dat bedrijven en organisaties de mogelijkheid zouden krijgen om te reageren op de concepten van de wetsvoorstellen en onderliggende

[3] Deze quickscan is te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/.
[4] *Stcrt.* 2020, 7857.

regelgeving. De regering heeft alle ontvangen consultatiereacties bezien en overwogen of naar aanleiding van die reacties de wetsvoorstellen of de bijbehorende toelichtingen op punten moeten worden aangepast. Dat laatste is ook gebeurd; de internetconsultatie heeft, tezamen met de formele consultatie, geleid tot vele nuttige reacties, die op hun beurt hebben geleid tot aanpassing van de wetsvoorstellen of aanpassing, verscherping of verduidelijking in de bijbehorende memorie van toelichting. Het voorgaande geldt ook voor de onderliggende regelgeving.

Nederland zal de voorgaande aspecten benoemen in de procedure bij het Hof van Justitie van de Europese Unie.

Kan de regering aan de leden van de fractie van FVD toelichten waarom ervoor wordt gekozen om onder tijdsdruk van een lopende inbreukprocedure wetgeving versneld door het parlement te loodsen? Welke gevolgen heeft dit voor de kwaliteit van de parlementaire controle? Acht de regering het wenselijk dat wetgeving op dit terrein primair wordt ingegeven door dreigende EU-sancties in plaats van inhoudelijke nationale afwegingen?

De regering hecht aan spoedige omzetting van de NIS2-richtlijn en de CER-richtlijn. Dit is niet alleen omdat Nederland daartoe verplicht is vanwege de in die richtlijnen opgenomen (inmiddels door Nederland overschreden) implementatietermijn, maar ook in het kader van de weerbaarheid en digitale veiligheid van Nederland. De regering hecht echter ook aan een zorgvuldige totstandkoming van de implementatiewetgeving, hetgeen de nodige tijd heeft gekost en ook één van de redenen is dat Nederland de richtlijnen niet tijdig heeft weten te implementeren. Onderdeel van de zorgvuldige totstandkoming van de implementatiewetgeving is dat er een zorgvuldige parlementaire behandeling plaatsvindt van de implementatiewetsvoorstellen. De regering onderkent hierbij nadrukkelijk dat het primaat van de parlementaire behandeling bij de Tweede Kamer en Eerste Kamer zelf ligt. Het is dus uiteraard aan de Tweede Kamer en de Eerste Kamer elk afzonderlijk om zelf te bepalen over het vervolg van de parlementaire behandeling en de tijd die nodig is voor de zorgvuldige behandeling van de wetsvoorstellen.

Kan de regering voor de leden van de fractie van FVD uiteenzetten waarom Nederland ervoor heeft gekozen om de NIS2-richtlijn grotendeels één-op-één te implementeren, in plaats van kritisch te bezien welke onderdelen daadwerkelijk noodzakelijk zijn binnen de Nederlandse context? In hoeverre is hierbij nog sprake van nationale beleidsruimte, en waarom is die ruimte wel of niet benut?

De lidstaten van de Europese Unie kunnen bij de implementatie van een richtlijn alleen daar waar een richtlijn die ruimte biedt, nationale keuzes maken. Voor de onderdelen van richtlijnen waarin die ruimte niet wordt geboden, kunnen lidstaten er niet voor kiezen om de onderdelen niet of anders te implementeren. Lidstaten moeten bij de implementatie uiteraard wel bezien hoe die onderdelen moeten worden geïmplementeerd binnen de nationale context en het nationale recht.

De NIS2-richtlijn biedt lidstaten op onderdelen de ruimte om nationale keuzes te maken. Deze onderdelen zijn inzichtelijk gemaakt in de transponeringstabel die is opgenomen in hoofdstuk 11 van de memorie van toelichting. In de kolom “omschrijving beleidsruimte” in combinatie met de kolom “toelichting” is inzichtelijk gemaakt welke beleidsruimte de NIS2-richtlijn biedt voor lidstaten en welke keuzes Nederland daarin heeft gemaakt.

De leden van de Volt-fractie hebben met belangstelling kennis genomen van het voorliggende wetsvoorstel. Het geeft deze leden aanleiding tot het stellen van een aantal vragen.

2. Algemeen deel / hoofdlijnen wetsvoorstel / aanleiding

De leden van de fracties van GroenLinks-PvdA en PvdD hebben de volgende algemene vragen aan de regering.

1. *Welke bewindspersoon of instantie heeft tijdens een sectoroverstijgende cybercrisis de uiteindelijke doorzettingsmacht wanneer meerdere toezichthouders of ministeries betrokken zijn?*

   De Minister van Justitie en Veiligheid is in artikel 18 Cbw aangewezen als de cybercrisisbeheerautoriteit, bedoeld in artikel 9, eerste lid, NIS2-richtlijn, en is in die hoedanigheid verantwoordelijk voor het beheer van grootschalige cyberbeveiligingsincidenten en crisisrespons. De rol van cybercrisisbeheerautoriteit wordt in de praktijk vervuld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (hierna: NCTV) en het NCSC, organisatieonderdelen van het Ministerie van Justitie en Veiligheid.

De wijze waarop bij sectoroverstijgende crises wordt gehandeld door de verschillende betrokkenen, waaronder de NCTV en het NCSC, is vastgelegd in het Landelijk Crisisplan Digitaal. Bij sectoroverstijgende cybercrises is er echter geen sprake van doorzettingsmacht. Ingeval van een situatie waarbij de nationale veiligheid in het geding is of kan zijn, of die anderszins een grote uitwerking op de maatschappij heeft of kan hebben, kan de nationale crisisstructuur worden geactiveerd en vindt de coördinatie en besluitvorming – met een spoedeisend karakter – plaats in de Ministeriële Commissie Crisisbeheersing. Die commissie wordt voorgezeten door de Minister van Justitie en Veiligheid of de minister-president.

2. *Hoe wordt voorkomen dat organisaties onder tegenstrijdige instructies van verschillende toezichthouders komen te staan?*

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. De vakministers zullen op grond van artikel 68, eerste lid, Cbw bij besluit de ambtenaren aanwijzen die zijn belast met het toezicht op de naleving van de verplichtingen uit de Cbw. Daarbij zal het gaan om de aanwijzing van ambtenaren van onder meer de Inspectie Leefomgeving en Transport (ILT), RDI en Inspectie Gezondheidszorg en Jeugd (IGJ). In alle gevallen geldt dat de toezichts- en handhavingstaken worden uitgeoefend onder gezag en verantwoordelijkheid van de bevoegde autoriteit (de vakminister). Voor de leesbaarheid van deze nota naar aanleiding van het verslag wordt, daar waar het gaat om de hiervoor bedoelde instanties waarvan de ambtenaren worden aangewezen, gesproken van “de toezichthouders” of “de toezichthoudende instanties”.

Sinds de inwerkingtreding van de Wet beveiliging netwerk- en informatiesystemen in 2019 werken de toezichthouders 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 in de vorm van een directeurenoverleg (DTDW). 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)

Deze instanties werken aan een werkplan met ambities op verschillende gebieden.[5] 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 omgegaan met entiteiten. Hierdoor ontstaat een consistente toezichtspraktijk en ontstaat er meer duidelijkheid over toezicht voor entiteiten die aan de Cbw moeten voldoen, in het bijzonder als zij te maken hebben met meerdere toezichthoudende instanties. De intensivering van de samenwerking staat daarbij overigens niet in de weg aan de sectorale aanpak van deze instanties.

De hiervoor genoemde instanties zijn overeengekomen om samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Hierin wordt onder meer vastgelegd welke informatie zij zullen uitwisselen binnen de daarvoor geldende wettelijke kaders en hoe wordt omgegaan met overlap in het toezicht waarbij een entiteit te maken heeft met meerdere toezichthoudende instanties. Op deze wijze wordt geborgd dat verschillen in sectorale context niet tot grote verschillen in de uitvoering van toezicht leiden, dat gelijkwaardig toezicht op alle entiteiten wordt geborgd en dat onnodige toezichtslasten zoveel mogelijk worden voorkomen.

De toezichthoudende instanties zien toe op de naleving van de verplichtingen uit de Cbw door entiteiten en houden daarbij rekening met de specifieke eigenschappen van een sector.

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

Zij werken allemaal vanuit hetzelfde wettelijk kader, namelijk de Cbw en onderliggende regelgeving, maar kunnen vanwege sectorspecifieke eigenschappen een andere invulling geven aan het toezicht. Zoals hiervoor aangegeven werken de toezichthoudende instanties 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 omgegaan met entiteiten. Ook zijn zij overeengekomen om samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Gelet op het voorgaande acht de regering het risico op tegenstrijdige instructies zeer gering.

3. *Kan de regering concreet uiteenzetten hoe de coördinatie tussen het Nationaal Cyber Security Centrum (NCSC), sectorale toezichthouders, veiligheidsregio's en crisisstructuren in de praktijk verloopt tijdens een grootschalige verstoring?*

De Minister van Justitie en Veiligheid is in artikel 18 Cbw aangewezen als de cybercrisisbeheerautoriteit, bedoeld in artikel 9, eerste lid, NIS2-richtlijn, en is in die hoedanigheid verantwoordelijk voor het beheer van grootschalige cyberbeveiligingsincidenten en crisisrespons. Deze rol wordt in de praktijk vervuld door de NCTV en het NCSC, organisatieonderdelen van het Ministerie van Justitie en Veiligheid. Beide organisatieonderdelen hebben een rol bij een grootschalige cybercrisis, zoals vastgelegd in het Landelijk Crisisplan Digitaal. Het beleggen van de taken en verantwoordelijkheid rondom het beheer van grootschalige cyberbeveiligingsincidenten en -crises bij de Minister van Justitie en Veiligheid in de Cbw sluit hierop aan en wordt hieronder nader (beknopt) toegelicht.

In het geval van een (dreigende) cybercrisis zijn getroffen entiteiten zelf primair verantwoordelijk voor het oplossen van de digitale verstoring binnen hun eigen organisaties. Een entiteit wordt door haar Computer security incident response team (hierna: CSIRT, meervoud: CSIRT's) ondersteund in geval van een incident bij het treffen van maatregelen om de continuïteit van de dienstverlening te waarborgen of te herstellen. Afhankelijk van de aard en omvang van een incident kan een CSIRT en/of het NCSC besluiten intern op te schalen. Bij een (dreigend) grootschalig digitaal incident adviseert het NCSC de NCTV over mogelijke inzet van de nationale crisisstructuur of onderdelen daarvan. Het opschalen van (onderdelen van) de nationale crisisstructuur gebeurt conform het Nationaal Handboek Crisisbeheersing.

Vanwege de (potentiële) impact van een digitaal incident kan ook sprake zijn van gevolgen voor de fysieke veiligheid en openbare orde. Het Nationaal Crisis Centrum (NCC) informeert bij grootschalige (dreigende) crises de betrokken veiligheidsregio('s) en/of lokaal bevoegd gezag over het incident met mogelijke cascade- en gevolgeffecten, indien hier aanleiding toe is. Daarnaast kunnen incidenten met gevolgen voor de fysieke veiligheid en openbare orde, direct gemeld worden bij de betrokken (hulp)diensten en/of regionale of lokale overheden, waaronder de veiligheidsregio. Informatie over een incident met (mogelijke) fysieke gevolgen binnen het regionaal of lokaal domein kan door de veiligheidsregio gecommuniceerd worden aan andere medeoverheden (gemeenten, provincies en waterschappen). Voor de fysieke gevolgbestrijding kan er door de veiligheidsregio worden opgeschaald vanuit bestaande en herkenbare structuren, bijvoorbeeld binnen de GRIP-structuur (Gecoördineerde Regionale Incidentbestrijdings Procedure) op regionaal niveau. Kortom, wanneer een digitaal incident de fysieke veiligheid raakt waardoor er bijvoorbeeld brandweerinzet noodzakelijk is, dan worden de veiligheidsregio's geïnformeerd, die in dat geval op basis van hun wettelijke taken deze incidenten oppakken.

4. *Waarom is niet gekozen voor één centrale cyberautoriteit met bindende coördinatiebevoegdheden?*

Voor zover de leden van de fracties van GroenLinks-PvdA en PvdD doelen op het CSIRT, is de reactie als volgt. In internationaal verband zijn het vaak CSIRT's die coördinerende taken vervullen en veel landen hebben die organisatie gedefinieerd als hun "nationale CSIRT". In de praktijk zal het NCSC in binnen- en buitenland, ook zonder formele aanwijzing, als "nationale CSIRT" opereren, ook gelet op de overige taken die het NCSC in de praktijk op grond van de Cbw vervult en de cruciale positie die het NCSC inneemt in het versterken van de digitale weerbaarheid. De coördinerende taken volgen uit de taken van de coördinator met het oog op een gecoördineerde bekendmaking van kwetsbaarheden (artikel 17 Cbw), het centrale contactpunt (artikel 14 Cbw) en de beheerder van het nationale register (artikel 43 Cbw).

Voor zover de leden van de fracties van GroenLinks-PvdA en PvdD doelen op het toezicht, is de reactie als volgt. In de Cbw worden de vakministers aangewezen als de bevoegde autoriteit voor de sectoren en subsectoren die onder hun beleidsverantwoordelijkheid vallen, zie artikel 15 Cbw. Er is niet gekozen voor één centrale bevoegde autoriteit, omdat door aanwijzing van de vakministers onder meer wordt geborgd dat de in de Cbw opgenomen taken van de bevoegde autoriteit, waaronder het toezicht op de naleving van de verplichtingen uit de Cbw, worden uitgevoerd met voldoende inzicht in sectorspecifieke eigenschappen en belangen.

5. *Kan de regering aangeven welke rol de Autoriteit Persoonsgegevens concreet krijgt bij toezicht op gegevensverwerking onder deze wet?*

De Autoriteit persoonsgegevens zal op grond van de Algemene verordening gegevens bescherming en de Uitvoeringswet Algemene verordening gegevensbescherming ten aanzien van de verwerkingen van persoonsgegevens op grond van de Cbw toezicht houden op de naleving van de voorschriften omtrent de verwerking van persoonsgegevens. Op de naleving van alle andere voorschriften op grond van de Cbw wordt, onder verantwoordelijkheid van de bevoegde autoriteit (de vakminister), toegezien door de eerdergenoemde toezichthoudende instanties.

6. *Hoe wordt voorkomen dat organisaties te maken krijgen met dubbele of overlappende rapportageverplichtingen onder de Cyberbeveiligswet en de Wet weerbaarheid kritieke entiteiten?*

Er zijn entiteiten die zowel onder het toepassingsbereik van de Cbw vallen, als onder het toepassingsbereik van de Wwke. Voor hen gelden dan zowel de meldplicht uit de Cbw als die uit de Wwke. Als zich een incident bij hen voordoet dat op grond van beide wetten meldplichtig is, dan moeten zij dat conform de in die wetten opgenomen voorschriften melden. Op dit moment wordt voorzien in de inrichting van één meldpunt bij het NCSC voor meldingen onder beide wetten.

7. *Hoe beoordeelt de regering de risico's van afhankelijkheid van Amerikaanse Cloud providers voor vitale infrastructuur?*

Het kabinet onderschrijft de noodzaak om ongewenste afhankelijkheden in het digitale domein af te bouwen. Tegelijkertijd is het kabinet terughoudend om verplichtingen of restricties ten aanzien van cloudgebruik die gelden voor de overheid generiek van toepassing te verklaren op de inrichting van alle organisaties die actief zijn in vitale processen. Zelfstandige organisaties die niet vallen onder het rijksbreed cloudbeleid zijn in beginsel vrij om clouddienstverlening naar eigen inzicht in te zetten. Wel adviseert het kabinet organisaties met klem om van geval tot geval, en op basis van proportionele en risicogebaseerde afwegingen, maatregelen nemen over de inrichting van hun cloudgebruik. Dit advies geldt uiteraard bij uitstek voor partijen die actief zijn in vitale processen.

Vakdepartementen en toezichthouders met bevoegdheden in specifieke vitale sectoren kunnen uiteraard een rol spelen in het bepalen van sectorspecifiek beleid ten aanzien van cloudgebruik. Zo heeft het Ministerie van Financiën in recente Kamervragen over digitale afhankelijkheden in de financiële sector aangegeven contact te hebben gelegd met toezichthouders en financiële instellingen om sectorspecifieke risico's in beeld te brengen.[6]

Welke gevolgen kan de Amerikaanse CLOUD Act in de optiek van de regering hebben voor Nederlandse vitale infrastructuur en overheidsdata? Deze leden lezen hier graag een analyse van.

De zogeheten CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*) biedt autoriteiten in de Verenigde Staten de mogelijkheid om onder voorwaarden toegang te krijgen tot de gegevens waarover een onderneming in de Verenigde Staten beschikt, óók wanneer de gegevens zich bevinden onder een dochtervennootschap en op servers buiten de Verenigde Staten.

De (potentiële) gevolgen hiervan voor de Nederlandse overheid en Nederlandse organisaties die betrokken zijn in vitale processen zijn volledig afhankelijk van de inrichting van hun IT-architectuur. Zoals onder de vorige vraag aangegeven adviseert het kabinet organisaties om

[6] *Kamerstukken II* 2025/26, aanhangsel bij 2025Z19476.

op basis van proportionele en risicogebaseerde afwegingen maatregelen te nemen over de inrichting van hun cloudgebruik.

8. *Welke mogelijkheden heeft de Nederlandse regering om buitenlandse overnames van vitale digitale infrastructuur tegen te houden? Deze leden lezen hier graag een analyse van en tevens een reactie op de vraag of de regering voornemens is hier, al dan niet in Europees verband, regelgeving voor in het leven te roepen.*

Op grond van de Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo) kunnen verwervingsactiviteiten ten aanzien van onder meer vitale aanbieders (als doelonderneming) worden getoetst op risico's voor de nationale veiligheid. Als wordt geoordeeld dat een verwervingsactiviteit leidt tot risico's voor de nationale veiligheid, kunnen eisen of voorschriften aan de activiteit worden verbonden om die risico's te voorkomen of tot een aanvaardbaar niveau te beperken. Als wordt geoordeeld dat een verwervingsactiviteit leidt tot een risico voor de nationale veiligheid, dat niet in voldoende mate beperkt kan worden door eisen of voorschriften, wordt deze activiteit verboden door de Minister van Economische Zaken en Klimaat. Hierbij wordt voorts gewezen op de recent door het Europees Parlement goedgekeurde herziene FDI-screeningsverordening.[7] Deze verordening verplicht de lidstaten van de Europese Unie onder meer een screeningsmechanisme in te voeren voor buitenlandse investeringen in doelondernemingen in onder meer de sector digitale infrastructuur, voor zover zij als kritiek worden beschouwd na een risicogebaseerde, gerichte beoordeling door de lidstaat waar zij zijn gevestigd. Genoemde verordening zal in Nederland worden uitgevoerd via onder meer een wijziging van de Wet veiligheidstoets investeringen, fusies en overnames (Wet vifo).

9. *Welke geopolitieke criteria worden betrokken bij aanbestedingen van vitale digitale diensten?*

Vanaf 1 januari 2026 gelden er nieuwe beveiligingseisen voor bedrijven die voor de overheid een opdracht uitvoeren met risico's voor de nationale veiligheid (bijzondere opdrachten). Dat zijn de Algemene Beveiligingseisen voor Rijksoverheidsopdrachten (hierna: ABRO). Met de ABRO gelden binnen de hele Rijksoverheid dezelfde eisen. De ABRO verkleint de risico's voor de nationale veiligheid, zoals cyberaanvallen en spionage.
Op grond van het Kaderbesluit ABRO Rijksdienst geldt onder meer het voorschrift dat de ministers zorgdragen dat bij de voorbereiding van een inkoopopdracht een quickscan wordt verricht, indien het vermoeden bestaat dat sprake kan zijn van risico's voor de nationale veiligheid. Indien de quickscan laat zien dat dergelijke risico's aan de orde kunnen zijn, moet in een risicoanalyse worden nagegaan of sprake is van een zogenoemde bijzondere opdracht. Bij toepassing van genoemde quickscan wordt onder meer in kaart gebracht of sprake is van toegang tot informatie die inzicht geeft in de Nederlandse positie of dat van bondgenoten op een thema dat interessant kan zijn voor statelijke actoren en of er gevoelige kennis, informatie of data wordt opgeslagen op buitenlandse servers of locaties. Bij toepassing van genoemde risicoanalyse wordt aanvullend en meer specifiek in kaart gebracht of sprake is van een strategische afhankelijkheid van partijen en landen met wie Nederland niet dezelfde geopolitieke belangen deelt.

10. *Hoe worden klimaatrisico's zoals overstromingen, droogte en hitte structureel meegenomen in de beoordeling van kritieke infrastructuur?*

De Wwke verplicht kritieke entiteiten om hun risico's systematisch in kaart te brengen. Dat gebeurt vanuit een brede *all hazard* benadering: alle mogelijke dreigingen en risico's worden meegewogen. Tegelijkertijd vraagt elk type dreiging om eigen kennis en methoden. Ook voor klimaatrisico's is specifieke expertise nodig om een goede analyse te kunnen maken. Dat is belangrijk omdat door de effecten van extreem weer in Nederland dit mogelijk snel tot maatschappelijke effecten kan leiden omdat vitale infrastructuur zo sterk met elkaar verweven is. Om hierbij te ondersteunen heeft Deltares, in opdracht van het Ministerie van Infrastructuur en Waterstaat, de Handreiking Klimaatbestendige Vitale Infrastructuur ontwikkeld.[8] Dit hulpmiddel ondersteunt kritieke entiteiten bij het bepalen van klimaatrisico's voor hun organisatie.

[7] FDI staat voor "Foreign Direct Investment". Zie ook het fiche van de werkgroep Beoordeling Nieuwe Commissievoorstellen (BNC) over de herziening van de FDI-screeningsverordening: *Kamerstukken II* 2023/24, 22112, nr. 3905.
[8] Deze handreiking is te raadplegen op https://www.rijksoverheid.nl/documenten/2025/10/15/handreiking-klimaatbestendige-vitale-infrastructuur-voor-het-bepalen-van-klimaatrisico-s.

11. *Hoe beoordeelt de regering de weerbaarheid van vitale infrastructuur tegen gecombineerde klimaat- en cyberdreigingen?*

In het Dreigingslandschap Vitale Infrastructuur (2025) concludeert de NCTV dat klimaatverandering versnelt en ernstiger wordt dan eerder werd gedacht.[9] Dit creëert nieuwe en versterkt bestaande dreigingen. Tegelijkertijd zijn de exacte gevolgen van klimaatverandering en de precieze impact daarvan op vitale processen moeilijk in te schatten. De toegenomen afhankelijkheid van burgers en bedrijven van onder andere ICT-netwerken maakt Nederland kwetsbaarder voor de gevolgen van klimaatverandering op dergelijke vitale infrastructuur. Daarbij geldt dat extreem weer meerdere vitale processen tegelijkertijd kan raken en dat een grotere kans op natuurlijke dreigingen ook betekent dat de kans op het samenvallen van verschillende dreigingen toeneemt. De weerbaarheid van vitale infrastructuur verschilt per soort infrastructuur en sector. Actoren kunnen gebruik maken van kritieke infrastructuur die al is verzwakt na bepaalde weersfenomenen. Door middel van ingebouwde redundantie en mitigerende maatregelen wordt rekening gehouden met dergelijke risico's.

Ten aanzien van de Cyberveiligheidswet lezen de leden van de D66-fractie dat voor de vitaalbeoordeling en de beslissing om een entiteit aan te wijzen de vakminister alleen verplicht is om te overleggen met de minister van J&V.[10] De leden van de D66-fractie vragen de regering of dit geen afbreuk doet aan het vermogen van de minister van J&V om coördinerend op te treden. Wat betekent dit voor mogelijke rechtsongelijkheid tussen verschillende sectoren, omdat verschillende vakministers verschillend zouden kunnen optreden?

De Cbw en het Cbb, dat is de algemene maatregel van bestuur onder de Cbw, bevatten diverse bepalingen met de bevoegdheid voor de vakministers om (nadere) regels of besluiten voor hun sectoren vast te stellen. Daarbij is een vorm van betrokkenheid van de Minister van Justitie en Veiligheid geregeld, waarbij is aangesloten bij de huidige verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid, waarbij elke minister beleidsmatig verantwoordelijk is voor de digitale weerbaarheid en de continuïteit van de entiteiten binnen zijn portefeuille. De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op cybersecurity en nationale veiligheid en zorgt vanuit die rol onder meer voor een goed functionerend cybersecuritystelsel.

De betrokkenheid van de Minister van Justitie en Veiligheid komt in de Cbw en het Cbb in twee varianten tot uiting: ofwel is bepaald dat de vakministers regelingen of besluiten voor hun sectoren "in overeenstemming met" de Minister van Justitie en Veiligheid vaststellen, ofwel is bepaald dat de vakministers dit doen "na overleg met" de Minister van Justitie en Veiligheid.

De variant van "na overleg met" is gekozen bij de bepalingen in de Cbw en het Cbb waarbij de handelingen van de vakminister het integrale cybersecuritystelsel in mindere mate raken. In die gevallen is alleen overleg nodig tussen de vakminister en de Minister van Justitie en Veiligheid. Voor deze variant is onder meer, zoals de leden van de D66-fractie ook hebben aangegeven in de vraagstelling, gekozen in artikel 9 Cbw, op basis waarvan een vakminister een entiteit aanwijst als essentiële entiteit aan de hand van de in dat artikel opgenomen criteria. De regering is van mening dat deze variant geen afbreuk doet aan het vermogen van de Minister van Justitie en Veiligheid om coördinerend op te treden, omdat deze variant alleen is gekozen bij de bepalingen in de Cbw en het Cbb waarbij de handelingen van de vakminister het integrale cybersecuritystelsel in mindere mate raken en er bij deze variant onverkort overleg plaatsvindt tussen de vakminister en de Minister van Justitie en Veiligheid. Doordat er altijd overleg met de Minister van Justitie en Veiligheid plaatsvindt, wordt onder meer mogelijke rechtsongelijkheid tussen verschillende sectoren zoveel als mogelijk voorkomen.

De leden van de CDA-fractie constateren dat de regering kiest voor een stelsel waarin meerdere vakministers optreden als bevoegde autoriteit, terwijl de minister van J&V een coördinerende rol vervult. De Afdeling advisering van de Raad van State heeft gevraagd nader uiteen te zetten op welke wijze de minister van J&V daadwerkelijk "in positie" wordt gebracht als stelselverantwoordelijke.[11]

Voorts vragen deze leden waarom niet is gekozen voor een sterkere vorm van formele medebetrokkenheid van de minister van J&V bij sectorspecifieke regelgeving en besluiten die gevolgen kunnen hebben voor het functioneren van het integrale cybersecuritystelsel.

---

[9] Het Dreigingslandschap Vitale Infrastructuur (2025) is te raadplegen op https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur.
[10] *Kamerstukken II 2025/26, 36.764, nr. 8, pp. 18-19.*
[11] *Kamerstukken II 2025/26, 36.764, nr. 4.*

De regering is van mening dat de Cbw en het Cbb reeds voorzien in een afdoende sterke vorm van formele betrokkenheid van de Minister van Justitie en Veiligheid bij het vaststellen van sectorspecifieke regelgeving en besluiten die gevolgen kunnen hebben voor het functioneren van het integrale cybersecuritystelsel.

De Cbw en het Cbb bevatten diverse bepalingen met de bevoegdheid voor de vakministers om (nadere) regels of besluiten voor hun sectoren vast te stellen. Daarbij is een vorm van betrokkenheid van de Minister van Justitie en Veiligheid geregeld, waarbij is aangesloten bij de huidige verantwoordelijkheidsverdeling rondom het thema digitale weerbaarheid, waarbij elke minister beleidsmatig verantwoordelijk is voor de digitale weerbaarheid en de continuïteit van de entiteiten binnen zijn portefeuille. De Minister van Justitie en Veiligheid is coördinerend bewindspersoon op cybersecurity en nationale veiligheid en zorgt vanuit die rol onder meer voor een goed functionerend cybersecuritystelsel.

De betrokkenheid van de Minister van Justitie en Veiligheid komt in de Cbw en het Cbb in twee varianten tot uiting: ofwel is bepaald dat de vakministers regelingen of besluiten voor hun sectoren “in overeenstemming met” de Minister van Justitie en Veiligheid vaststellen, ofwel is bepaald dat de vakministers dit doen “na overleg met” de Minister van Justitie en Veiligheid.

De variant van “in overeenstemming met” is gekozen bij de bepalingen in de Cbw en het Cbb waarbij regelingen of besluiten van de vakminister het integrale cybersecuritystelsel raken, en dus van invloed zijn op de stelselverantwoordelijkheid van de Minister van Justitie en Veiligheid. Bij die bepalingen is voorgeschreven dat de vakministers de hiervoor bedoelde regels alleen kunnen vaststellen “in overeenstemming met” de Minister van Justitie en Veiligheid. De Minister van Justitie en Veiligheid zal dan toetsen en adviseren op onder meer sectoroverstijgende effecten, de druk op het cybersecuritystelsel en de bredere impact op de nationale veiligheid. Deze variant is onder meer opgenomen in artikel 21a Cbw, op basis waarvan een vakminister een entiteit de verplichting kan opleggen om een dienst of product van een specifieke leverancier te weren uit onderdelen van haar netwerk- en informatiesystemen. Deze verplichting kan worden opgelegd om risico’s voor de beveiliging van netwerk- en informatiesystemen die de nationale veiligheid raken te beheersen of om incidenten die de nationale veiligheid raken te voorkomen. Wanneer de vakminister gebruik maakt van deze bevoegdheid, is overeenstemming met de Minister van Justitie en Veiligheid nodig. Deze variant is ook onder meer gekozen in de artikelen 23, eerste lid, en 32, eerste lid, Cbw, op grond waarvan een vakminister een essentiële entiteit of belangrijke entiteit kan ontheffen van de zorgplicht en de meldplicht. Daarbij gaat het meer specifiek om in hoofdzaak entiteiten die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving.

De variant van “na overleg met” is gekozen bij de bepalingen in de Cbw en het Cbb waarbij de handelingen van de vakminister het integrale cybersecuritystelsel in mindere mate raken. In die gevallen is alleen overleg nodig tussen de vakminister en de Minister van Justitie en Veiligheid. Voor deze variant is onder meer gekozen in artikel 9 Cbw, op basis waarvan een vakminister een entiteit aanwijst als essentiële entiteit aan de hand van de in dat artikel opgenomen criteria.

Het verschil tussen “na overleg met” en “in overeenstemming met” is dat bij “na overleg met” eventueel verschil van inzicht kan worden besproken in de gangbare afstemmings- en overlegstructuren, maar de vakminister uiteindelijk de eindbeslissing neemt. Bij “in overeenstemming met” is instemming van de Minister van Justitie en Veiligheid met het te nemen besluit vereist.

Deze leden lezen verder dat bestaande sectorspecifieke toezichthouders, waaronder zelfstandige bestuursorganen, naast de bevoegde autoriteiten een rol blijven vervullen bij toezicht op veiligheid en cyberweerbaarheid.

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.[12] De vakministers wijzen bij besluit de ambtenaren aan die onder verantwoordelijkheid van de vakministers zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[13] Daarbij zal het gaan om de aanwijzing van ambtenaren van

[12] 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.

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

verschillende organisaties, afhankelijk van de sector. De hiervoor bedoelde aanwijzing voor het toezicht op de naleving van het bepaalde bij of krachtens de Cbw komt naast de taken die zij al reeds vervullen op grond van andere wettelijke kaders.

3. Rechtmatigheid / rechtsbeginselen / consistentie

De leden van de fracties van GroenLinks-PvdA en PvdD vragen de regering hoe zij garandeert dat deze wetgeving enerzijds voldoende flexibel blijft om cyberdreigingen het hoofd te bieden, maar anderzijds niet leidt tot structurele onzekerheid over de juridische verplichtingen van organisaties.

1. *Waarom heeft de regering ervoor gekozen essentiële normen grotendeels via lagere regelgeving uit te werken in plaats van in de wet zelf?*

   De regering gaat ervan uit dat deze leden doelen op de voorschriften met betrekking tot de maatregelen die in het kader van de zorgplicht moeten worden genomen. Deze zijn opgenomen in artikel 21, derde lid, Cbw, uitgewerkt in het Cbb en nader uitgewerkt in de onderliggende ministeriële regelingen van de vakministers.

   De zorgplicht is één van de hoofdelementen van de Cbw en is daarom geregeld op het niveau van een wet. Daarbij is op dit niveau ook voorgeschreven wat de in het kader van de zorgplicht te nemen maatregelen in elk geval moeten omvatten. De maatregelen die entiteiten in meer concrete zin 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. Dit is een gebruikelijk onderscheid bij de verdeling van regels tussen wetgeving en lagere regelgeving en 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 een zekere 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 iedere wijziging van een bestaande algemene maatregel van bestuur ter advies moet worden voorgelegd aan de Afdeling advisering van de Raad van State. Hierbij geldt ook dat de Eerste Kamer en de Tweede Kamer altijd in de gelegenheid zullen worden gesteld om voorafgaand aan de aanbieding aan de Afdeling advisering van de Raad van State te reageren op toekomstige wijzigingen van de uitwerking van de zorgplicht in het Cbb. Deze voorhangprocedure is geregeld in artikel 21, zesde lid, Cbw.

   De uitwerking van de zorgplicht in het Cbb wordt vervolgens nader uitgewerkt in onderliggende ministeriële regelingen van de vakministers. Deze regelingen voorzien in een sectorspecifieke uitwerking van de zorgplicht. De vakministers kunnen hiermee met nadere regels komen die nodig zijn voor de specifieke sectoren, subsectoren en soorten entiteiten waarvoor zij verantwoordelijk zijn.

2. *Op basis van welke concrete criteria kan een organisatie vooraf vaststellen dat zij voldoet aan de (zorgplicht) verplichting om “passende en evenredige maatregelen” te nemen? Kan de regering hierbij betrekken dat er geen sprake is van eenduidige wettelijke minimumnormen maar van uitwerking in lagere regelgeving?*

   De regering beantwoordt deze vraag samen met de volgende vraag. Zie het antwoord dat hierna volgt.

3. *Hoe wordt voorkomen dat pas achteraf, bij toezicht of handhaving of via jurisprudentie, duidelijk wordt of een organisatie aan haar wettelijke verplichtingen heeft voldaan? Aan de hand van welke concrete criteria wordt beoordeeld of een organisatie voldoet aan de zorgplicht? Is dit op voorhand voldoende kenbaar?*

   De criteria waaraan essentiële entiteiten en belangrijke entiteiten in het kader van de zorgplicht in ieder geval moeten voldoen staan in artikel 21 Cbw. Doordat hierin onder meer is voorgeschreven ten aanzien van welke onderwerpen in elk geval maatregelen moeten worden genomen, is er sprake van eenduidige wettelijke minimumnormen. De in het kader van de zorgplicht te nemen maatregelen worden vervolgens nader uitgewerkt en geconcretiseerd in lagere regelgeving, te weten het Cbb en ministeriële regelingen. Daarin is meer concreet uitgewerkt welke maatregelen entiteiten moeten treffen. Op welke wijze entiteiten in de praktijk specifiek invulling moeten geven aan die voorgeschreven zorgplichtmaatregelen is met name ook afhankelijk van de uitkomsten van de risicoanalyse

die elke entiteit afzonderlijk zal uitvoeren. Dit betekent dat een entiteit niet voorafgaand, maar na het uitvoeren van de risicoanalyse kan vaststellen welke specifieke invulling van de maatregelen voor haar passend en evenredig is. De uitkomsten van de risicoanalyse en daarmee de invulling van de te nemen maatregelen zullen daarom per entiteit verschillen. Bij het treffen van de maatregelen dient de entiteit onder meer rekening te houden met de stand van de techniek, zoals ook is voorgeschreven in artikel 21 Cbw, zodat de maatregelen effectief zijn om de actuele cyberdreigingen het hoofd te bieden.

Bij de beoordeling door de entiteit welke specifieke passende en evenredige maatregelen genomen moeten worden, kan de entiteit gebruik maken van bestaande normenkaders, zoals ISO27001. Vanuit de rijksoverheid zijn voorts diverse tools en kennisproducten opgesteld die kunnen helpen bij het voldoen aan de zorgplicht uit de Cbw. Hieronder volgt een overzicht daarvan:

- Op de website van het NCSC zijn meerdere infosheets te vinden over de zorgplicht uit de Cbw. Hierin wordt stap voor stap uitgelegd wat een entiteit kan doen om invulling te geven aan die verplichting. Ook worden er met enige regelmaat Q&A's hierover op de website van het NCSC geplaatst.

- De RDI heeft een quickscan ontwikkeld waarmee entiteiten aan de hand van 40 vragen kunnen beoordelen hoe het met hun cyberbeveiliging ervoor staat.[14]

- 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 onder andere hun aanpak voor het voldoen aan de zorgplicht uit de Cbw.

Het is vervolgens aan de toezichthouder om te beoordelen of de entiteit voldoende invulling heeft gegeven aan de zorgplichtmaatregelen en de toezichthouder zal daarbij risicogebaseerd te werk gaan, juist omdat de uitkomsten van de risicoanalyse en daarmee de invulling van de genomen maatregelen per entiteit zullen verschillen. De maatregelen die zijn omschreven in artikel 21 Cbw, de uitwerking daarvan in het Cbb en de nadere (sectorspecifieke) uitwerking daarvan in de onderliggende ministeriële regelingen bieden daarvoor een helder en kenbaar kader.

4. *Kan de regering exact aangeven welke minimale beveiligingseisen in de wet zelf zijn vastgelegd, los van lagere regelgeving?*

In artikel 21, derde lid, Cbw is bepaald dat de maatregelen die entiteiten moeten nemen in het kader van de zorgplicht moeten zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen. Deze wetsbepaling schrijft voor dat de maatregelen ten minste het volgende moeten omvatten:
a. beleid inzake risicoanalyse en beveiliging van informatiesystemen;
b. incidentenbehandeling;
c. bedrijfscontinuïteit, zoals back-upbeheer en herstelplannen, en crisisbeheer;
d. de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen de entiteit en haar rechtstreekse leveranciers of
dienstverleners;
e. beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
f. beleid en procedures om de effectiviteit van maatregelen voor het beheersen van cyberbeveiligingsrisico's te beoordelen;
g. basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
h. beleid en procedures over het gebruik van cryptografie en, in voorkomend geval, encryptie;
i. beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van assets; en
j. wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

[14] Deze quickscan is te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS2-Quickscan/.

Uiteraard moeten de criteria zoals die in de wet zelf zijn geformuleerd, worden gelezen in combinatie met de uitwerking daarvan in het Cbb en de daarop gebaseerde ministeriële regelingen.

5. *Hoe wordt parlementaire controle gegarandeerd op normen die feitelijk pas in lagere regelgeving en toezichtpraktijk worden ingevuld?*

De Eerste Kamer en de Tweede Kamer zullen altijd in de gelegenheid worden gesteld om te reageren op toekomstige wijzigingen van de uitwerking van de zorgplicht in het Cbb. Deze voorhangprocedure is geregeld in artikel 21, zesde lid, Cbw.

6. *Hoe voorkomt de regering dat verschillende sectorale toezichthouders de open normen verschillend interpreteren en daarmee ongelijkheid in handhaving ontstaat?*

Sinds de inwerkingtreding van de Wet beveiliging netwerk- en informatiesystemen in 2019 werken de toezichthouders 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 in de vorm van een directeurenoverleg (DTDW). 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)

Deze instanties werken aan een werkplan met ambities op verschillende gebieden.[15] 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 omgegaan met entiteiten. Hierdoor ontstaat een consistente toezichtspraktijk en ontstaat er meer duidelijkheid over toezicht voor entiteiten die aan de Cbw moeten voldoen, in het bijzonder als zij te maken hebben met meerdere toezichthoudende instanties. De intensivering van de samenwerking staat daarbij overigens niet in de weg aan een sectorale aanpak van deze instanties.

De hiervoor genoemde instanties zijn overeengekomen om samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Hierin wordt onder meer vastgelegd welke informatie zij zullen uitwisselen binnen de daarvoor geldende wettelijke kaders en hoe wordt omgegaan met overlap in het toezicht waarbij een entiteit te maken heeft met meerdere toezichthoudende instanties. Op deze wijze wordt geborgd dat verschillen in sectorale context niet tot grote verschillen in de uitvoering van toezicht leiden, dat gelijkwaardig toezicht op alle entiteiten wordt geborgd en dat onnodige toezichtslasten zoveel mogelijk worden voorkomen.

Door de hiervoor omschreven samenwerking en afspraken wordt zoveel als mogelijk voorkomen dat normen uit de Cbw en Wwke door de verschillende toezichthoudende instanties verschillend worden geïnterpreteerd met ongelijkheid in handhaving tot gevolg.

7. *Welke juridische grenzen zijn gesteld aan de normstellende rol van toezichthouders via richtsnoeren en handhavingspraktijk?*

Toezichthouders hebben meerdere instrumenten om op voorhand aan entiteiten duidelijk te maken op welke wijze zij wet- en regelgeving interpreteren en hoe zij daarop zullen toezien. Dit kan bijvoorbeeld in de vorm van richtsnoeren, verschillende vormen van toezichtsbeleid of beleidsregels. Bij het inzetten daarvan moeten toezichthouders uiteraard binnen de wettelijke kaders blijven en de algemene beginselen van behoorlijk bestuur in acht nemen.

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

Richtsnoeren, waarmee richting wordt gegeven aan de interpretatie van wet- en regelgeving, zijn in hun aard richtinggevend, waarbij de wet- en regelgeving, bijhorende toelichting en wat blijkt uit de parlementaire behandeling vanzelfsprekend altijd leidend blijft. Waar het gaat om toezichtsbeleid, waaronder bijvoorbeeld sanctiebeleid, dient de toezichthouder zich te houden aan de kaders en waarborgen die de Algemene wet bestuursrecht (hierna: Awb) daarvoor schept, zoals hoofdstukken 3 en 5 Awb, evenals eventuele wetspecifieke kaders, zoals artikel 69 Cbw. Ditzelfde geldt ook voor beleidsregels, waarvoor de regels voor het opstellen ervan zijn vastgelegd in titel 4.3 Awb.

Met hun normstellende rol kunnen toezichthouders derhalve richtinggevend zijn voor de partijen die onder de reikwijdte van de wetgeving vallen en kunnen zij daarmee de voorspelbaarheid vergroten, maar tegelijkertijd is deze rol van de toezichthouder in zichzelf ook juridisch begrensd.

8. *Hoe verhoudt deze open normstelling zich tot het rechtszekerheidsbeginsel en het vereiste van voorzienbare wetgeving onder het Europees Verdrag voor de Rechten van de Mens (EVRM)?*

In artikel 21, derde lid, Cbw is opgesomd wat de maatregelen, die entiteiten moeten nemen in het kader van de zorgplicht, tenminste moeten omvatten. De hiermee bedoelde maatregelen zijn, net als enkele andere maatregelen in het kader van de zorgplicht, uitgewerkt in het Cbb. Die uitwerking geldt in beginsel voor alle essentiële entiteiten en belangrijke entiteiten uit alle sectoren waarop de Cbw van toepassing is.[16] De uitwerking van de zorgplicht in het Cbb wordt vervolgens nader uitgewerkt in onderliggende ministeriële regelingen van de vakministers. Deze regelingen voorzien in een sectorspecifieke uitwerking van de zorgplicht. De vakministers kunnen hiermee met nadere regels komen die nodig zijn voor sectoren, subsectoren of soorten entiteiten waarvoor zij verantwoordelijk zijn. Door de opname van de normen in de Cbw, de uitwerking daarvan in het Cbb en sectorspecifieke uitwerking in ministeriële regelingen is sprake van voorzienbare wetgeving en voldoende rechtszekerheid voor de entiteiten waarop de zorgplicht van toepassing is.

Het vereiste van voorzienbare wetgeving onder het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (hierna: EVRM) betekent niet dat alleen naar de wet in formele zin moet worden gekeken. Het EVRM gaat uit van een materieel wetsbegrip. Daaronder vallen in de Nederlandse context ook algemene maatregelen van bestuur en ministeriële regelingen. Het gaat er dus om dat de Cbw, het Cbb en de daarop gebaseerde ministeriële regelingen in onderlinge samenhang bezien resulteren in voorzienbare wetgeving. Dat is naar het oordeel van de regering zonder meer het geval.

Kan de regering aan de leden van de fractie van de VVD toelichten hoe de “essentiële entiteit” onder 36.764 zich tot de “kritieke entiteit” onder 36.765 verhoudt in gevallen waarin beide regimes van toepassing zijn?

Alle kritieke entiteiten in de zin van de Wwke zijn van rechtswege essentiële entiteit in de zin van de Cbw. Dit is geregeld in artikel 8, eerste lid, onderdeel i, Cbw. Andersom is dat niet het geval: een essentiële entiteit in de zin van de Cbw is niet van rechtswege ook kritieke entiteit in de zin van de Wwke. Wel kan een entiteit, die op grond van de Cbw van rechtswege al een essentiële entiteit of belangrijke entiteit is, ook als kritieke entiteit in de zin van de Wwke worden aangewezen. Als een entiteit zowel essentiële entiteit in de zin van de Cbw is, als kritieke entiteit in de zin van de Wwke, zijn beide wettelijke regimes elk afzonderlijk op de entiteit van toepassing.

Kan de regering toezeggen dat er één loket en één meldlijn komt?

[16] De uitwerking van de zorgplicht in het Cbb geldt niet voor 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, aanbieders van onlinezoekmachines, aanbieders van platforms voor socialenetwerkdiensten en verleners van vertrouwensdiensten. Dit is vastgelegd in artikel 4 Cbb en volgt uit de artikelen 1 en 2 van 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).

Op dit moment wordt voorzien in de inrichting van één meldpunt bij het NCSC voor meldingen onder de Cbw én de Wwke. Het uitgangspunt is dat het meldportaal op een lastenluwe manier wordt ingericht, waarin entiteiten die onder het toepassingsbereik van de Cbw vallen met één handeling een melding kunnen doen bij zowel hun CSIRT als hun bevoegde autoriteit.

De leden van de fractie van D66 constateren dat de regering hbo- en wo-instellingen als belangrijke of essentiële entiteit kwalificeert, waardoor deze instellingen onder de Cyberveiligheidswet komen te vallen. Zij geeft daarbij aan dat het geen onderscheid tussen individuele instellingen maakt, maar dat al deze instellingen als een dergelijke entiteit zullen worden aangemerkt. Deze leden vragen of dit niet kan leiden tot onwenselijke situaties. Kan de regering bijvoorbeeld uitleggen waarom wo- en hbo-instellingen belangrijkere of essentiëlere entiteiten zijn dan mbo-instellingen, zeker wanneer mbo-opleidingen duidelijke vitale functies raken, zoals ICT, transport of energie en dit bij bepaalde wo- en hbo-instellingen minder duidelijk kan zijn? Weegt in dergelijke gevallen de noodzaak van het vallen onder de Cyberveiligheidswet en daarmee het moeten voldoen aan de daaruit voortvloeiende eisen wel op tegen de daaruit voortvloeiende lasten?

Artikel 2, vijfde lid, onderdeel b, NIS2-richtlijn biedt de lidstaten van de Europese Unie de mogelijkheid om te bepalen dat de richtlijn ook van toepassing is op onderwijsinstellingen, met name wanneer zij kritieke onderzoeksactiviteiten verrichten. Deze mogelijkheid is geïmplementeerd in de artikelen 11 en 13 Cbw. Daarbij gaat het specifiek om de hbo- en wo-instellingen. De toenemende en permanente digitale dreiging maakt een brede en duurzame beheersing van cyberrisico’s in het hoger onderwijs, als rechtstreeks doelwit en onderdeel van het bredere digitale ecosysteem, noodzakelijk. Het verkrijgen van hoogwaardige kennis en technologie is een belangrijk doel van statelijke actoren en in dat kader kan onder meer digitale spionage op netwerken van kennisinstellingen schadelijk zijn voor de Nederlandse belangen. Bovendien is naast het beschermen van kritieke onderzoeksactiviteiten ook de bescherming van (privacygevoelige) gegevens van belang, aangezien deze voor de bekostigde instellingen en hun studenten en medewerkers cruciaal kunnen zijn voor het primaire proces.

Gezien de samenwerking en de sterke onderlinge afhankelijkheid tussen hbo- en wo-instellingen is het onwenselijk om de Cbw, met verplichtingen voor de entiteiten die onder die wet vallen, maar ook het recht op bijstand en advies van een CSIRT, van toepassing te laten zijn op een deel van de bekostigde hbo- en wo-instellingen. Ook gezien de complexiteit in uitvoerbaarheid en definieerbaarheid, is het maken van nader onderscheid tussen de bekostigde hbo- en wo-instellingen of binnen een instelling onwenselijk. De Cbw schrijft daarbij een risicogebaseerde aanpak voor, waarmee de instellingen de eigen risico’s dienen te identificeren en proportionaliteit in de te nemen maatregelen wordt geborgd. In de sectorspecifieke uitwerking van de aanwijzing van de bekostigde hogescholen en universiteiten is proportionaliteit ook het uitgangspunt en wordt waar mogelijk rekening gehouden met de uitvoeringslast.

De mbo-instellingen worden niet aangewezen onder de Cbw gezien de nadruk die in de NIS2-richtlijn wordt gelegd op de uitvoering van kritieke onderzoeksactiviteiten en de mbo-instellingen geen wettelijke taak hierin hebben. De versterking van de cyberweerbaarheid en bescherming van (privacy)gevoelige gegevens is tegelijkertijd ook in het mbo van belang. Daarom werkt de Minister van Onderwijs, Cultuur en Wetenschap momenteel aan hernieuwde bestuurlijke afspraken met de mbo-instellingen. Hierin worden ook afspraken gemaakt over de benodigde maatregelen en resultaten waarbij de zorgplicht uit de Cbw het uitgangspunt vormt. Zo wordt ervoor gezorgd dat voor het gehele vervolgonderwijs, ook in de samenwerking binnen SURF-verband, zo veel mogelijk dezelfde inzet wordt gekozen.[17]

De leden van de fractie van het CDA vragen de regering nader toe te lichten hoe in de praktijk wordt voorkomen dat verschillende bevoegde autoriteiten uiteenlopende normen, toezichtpraktijken en handhavingsstrategieën ontwikkelen. Deze leden vragen de regering daarnaast in hoeverre zij het risico aanwezig acht dat hierdoor rechtsongelijkheid ontstaat tussen sectoren of entiteiten.

Sinds de inwerkingtreding van de Wet beveiliging netwerk- en informatiesystemen in 2019 werken de toezichthouders 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 in de vorm van een directeurenoverleg (DTDW). 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)

[17] Coöperatie SURF is een coöperatieve vereniging van Nederlandse onderwijs- en onderzoeksinstellingen op het gebied van informatie- en communicatietechnologie.

− 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)

Deze instanties werken aan een werkplan met ambities op verschillende gebieden.[18] 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 omgegaan met entiteiten. Hierdoor ontstaat een consistente toezichtspraktijk en ontstaat er meer duidelijkheid over toezicht voor entiteiten die aan de Cbw moeten voldoen, in het bijzonder als zij te maken hebben met meerdere toezichthoudende instanties. De intensivering van de samenwerking staat daarbij overigens niet in de weg aan een sectorale aanpak van deze instanties.

De hiervoor genoemde instanties zijn overeengekomen om samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Hierin wordt onder meer vastgelegd welke informatie zij zullen uitwisselen binnen de daarvoor geldende wettelijke kaders en hoe wordt omgegaan met overlap in het toezicht waarbij een entiteit te maken heeft met meerdere toezichthoudende instanties. Op deze wijze wordt geborgd dat verschillen in sectorale context niet tot grote verschillen in de uitvoering van toezicht leiden, dat gelijkwaardig toezicht op alle entiteiten wordt geborgd en dat onnodige toezichtslasten zoveel mogelijk worden voorkomen.

Door de hiervoor omschreven samenwerking en afspraken wordt zoveel mogelijk voorkomen dat normen, toezichtpraktijken en handhavingsstrategieën uiteen lopen en wordt het risico op rechtsongelijkheid geminimaliseerd.

De regering geeft aan dat toezichthouders in voorkomende gevallen samenwerkingsafspraken zullen maken. Deze leden vragen waarom niet is gekozen voor een meer expliciete wettelijke afbakening van bevoegdheden en verantwoordelijkheden bij samenloop van toezicht. Daarnaast vragen deze leden hoe wordt voorkomen dat entiteiten geconfronteerd worden met overlappende toezichtslasten, tegenstrijdige aanwijzingen of onduidelijkheid over welke toezichthouder leidend is. Ook zijn deze leden benieuwd naar welke rol de minister van J&V speelt bij het coördineren van deze samenwerkingen.

De regering heeft niet gekozen voor het wettelijk afbakenen van bevoegdheden en verantwoordelijkheden bij samenloop van toezicht, omdat niet op voorhand is te bepalen welke toezichthouder in welke situatie het voortouw zou moeten nemen bij het toezicht. De entiteiten die onder het toepassingsbereik van de Cbw vallen, vallen doorgaans ook onder het toepassingsbereik van andere wet- en regelgeving en het daarbij behorende toezicht.

Sinds de inwerkingtreding van de Wet beveiliging netwerk- en informatiesystemen in 2019 werken de toezichthouders 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 in de vorm van een directeurenoverleg (DTDW). 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)

Deze instanties werken aan een werkplan met ambities op verschillende gebieden.[19] 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 omgegaan met entiteiten. Hierdoor ontstaat een consistente

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

toezichtspraktijk en ontstaat er meer duidelijkheid over toezicht voor entiteiten die aan de Cbw moeten voldoen, in het bijzonder als zij te maken hebben met meerdere toezichthoudende instanties. De intensivering van de samenwerking staat daarbij overigens niet in de weg aan een sectorale aanpak van deze instanties.

De hiervoor genoemde instanties zijn overeengekomen om samenwerkingsafspraken te formaliseren in een samenwerkingsprotocol. Hierin wordt onder meer vastgelegd welke informatie zij zullen uitwisselen binnen de daarvoor geldende wettelijke kaders en hoe wordt omgegaan met overlap in het toezicht waarbij een entiteit te maken heeft met meerdere toezichthoudende instanties. Op deze wijze wordt geborgd dat verschillen in sectorale context niet tot grote verschillen in de uitvoering van toezicht leiden, dat gelijkwaardig toezicht op alle entiteiten wordt geborgd en dat onnodige toezichtslasten zoveel mogelijk worden voorkomen.

Door de hiervoor omschreven samenwerking en afspraken worden overlappende toezichtslasten, tegenstrijdige aanwijzingen of onduidelijkheid over welke toezichthouder leidend is in specifieke gevallen waarin een entiteit onder het toezicht valt van meerdere instanties, zoveel mogelijk voorkomen.

Het Ministerie van Justitie en Veiligheid staat in nauw contact met het STDW en het DTDW. Daarmee geeft de Minister van Justitie en Veiligheid invulling aan het coördineren van dergelijke afspraken voor zover deze betrekking hebben op wetten in zijn portefeuille.

Deze leden hebben voorts vragen over het vereiste van operationeel onafhankelijk toezicht op overheidsinstanties als bedoeld in artikel 31, vierde lid, van de NIS2-richtlijn. De regering stelt dat de operationele onafhankelijkheid van het toezicht onder meer wordt gewaarborgd door organisatorische scheiding en de Aanwijzingen inzake de rijksinspecties. Deze leden vragen de regering nader te motiveren waarom deze organisatorische en bestuurlijke waarborgen voldoende worden geacht om te voldoen aan het vereiste van operationele onafhankelijkheid uit de richtlijn.

De verantwoordelijkheid voor het toezicht op de naleving van de verplichtingen uit de Cbw is belegd bij de bevoegde autoriteit. Dat is in alle gevallen de vakminister. Voor de sector overheid – met uitzondering van de waterschappen – is dit de Minister van Binnenlandse Zaken en Koninkrijksrelaties. Die minister zal op grond van artikel 68, eerste lid, Cbw ambtenaren van de RDI aanwijzen om toezicht te houden op de naleving van de verplichtingen uit de Cbw door entiteiten uit de sector overheid. De RDI is als rijksinspectie onderdeel van het Ministerie van Economische Zaken en Klimaat.

Het is van groot belang dat de RDI het hiervoor bedoeld toezicht operationeel onafhankelijk kan uitoefenen. Hier helpt het volgende bij. In de Aanwijzingen inzake de rijksinspecties staan waarborgen om de onafhankelijkheid van rijksinspecties te borgen. De beleidsinhoudelijk verantwoordelijke minister mag zijn bijzondere aanwijzingsbevoegdheid niet gebruiken om een rijksinspectie ervan te weerhouden een specifiek onderzoek te verrichten of af te ronden, noch om in te grijpen in de wijze waarop een rijksinspectie een specifiek onderzoek verricht, noch om invloed uit te oefenen op de bevindingen, oordelen en adviezen van een rijksinspectie. Indien in andere dan de hiervoor genoemde gevallen de bijzondere aanwijzingsbevoegdheid toch wordt ingezet door het ministerie aan de RDI, dan wordt de Staten-Generaal onverwijld geïnformeerd. Met de positionering van de toezichtstaken onder de secretaris-generaal wordt ervoor gezorgd dat de rijksinspecties niet hiërarchisch ondergeschikt zijn aan een ander onderdeel van het ministerie. Binnen het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is de beleidsverantwoordelijkheid voor de Cbw op de sector overheid belegd binnen het directoraat-generaal Digitalisering en Overheidsorganisatie (DGDOO) en daarmee ook de opdracht aan de RDI om toezicht te houden op de Cbw. De verantwoordelijkheid voor de implementatie van de Cbw bij het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in de eigen organisatie is belegd in de bedrijfsvoering van dat ministerie bij het CIO Office. Aanvullend op de organisatorische scheiding borgt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties dat er geen operationele bemoeienis met het toezicht is, zoals via openbaar kenbare relatiestatuten, regelingen of procedures.

Deze leden hebben eveneens een vraag over de voorgestelde uitzondering op de toepasselijkheid van de Wet open overheid (Woo). De regering motiveert deze uitzondering mede met het belang dat entiteiten erop moeten kunnen vertrouwen dat verstrekte informatie niet openbaar wordt gemaakt. Deze leden vragen de regering nader toe te lichten waarom de reeds bestaande uitzonderingsgronden binnen de Woo onvoldoende worden geacht om gevoelige bedrijfs- en veiligheidsinformatie te beschermen.

Artikel 66, eerste lid, Cbw biedt entiteiten die onder het toepassingsbereik van de Cbw vallen op voorhand de zekerheid dat vertrouwelijke gegevens die bij de CSIRT’s, de bevoegde autoriteiten en

het centrale contactpunt berusten niet openbaar kunnen worden gemaakt op grond van de Wet open overheid. De regering acht het noodzakelijk om die zekerheid op voorhand te bieden, om zo onder meer te voorkomen dat informatie niet meer door entiteiten met het CSIRT wordt gedeeld, waardoor de goede taakuitoefening door het CSIRT in het geding kan komen. Entiteiten kunnen terughoudend zijn met het delen van die informatie als zij niet op voorhand de zekerheid hebben dat deze niet op grond van de Wet open overheid openbaar kan worden gemaakt. Openbaarmaking daarvan kan immers leiden tot serieuze schade bij entiteiten, zoals reputatie-schade, toegenomen kwetsbaarheid voor aanvallen en benadeling van de concurrentiepositie.

4. Doeltreffendheid / doelmatigheid

Kan de regering aan de leden van de fractie van de VVD toelichten hoe de meldplicht "betekenisvol incident" geoperationaliseerd en voorkomen dat entiteiten uit voorzorg alles melden, met overbelasting van meldpunten tot gevolg?

Essentiële entiteiten en belangrijke entiteiten moeten op grond van artikel 25, eerste lid, Cbw ieder significant incident melden bij hun CSIRT en bevoegde autoriteit. 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. Op grond van artikel 25, derde lid, Cbw kunnen bij of krachtens algemene maatregel van bestuur de criteria worden vastgesteld op basis waarvan wordt bepaald of sprake is van een significant incident. Die criteria worden ook drempelwaarden genoemd. Aan de hand van een drempelwaarde kan worden bepaald of een incident bij een essentiële entiteit of belangrijke entiteit in de zin van de Cbw significant is en daarmee meldplichtig is op grond van de Cbw.

In het Cbb, de algemene maatregel van bestuur onder de Cbw, is geregeld dat die drempelwaarden bij ministeriële regeling kunnen worden vastgesteld door de vakministers voor de sectoren waarvoor zij beleidsverantwoordelijk zijn. De vakministers kunnen de drempelwaarden vaststellen aan de hand van de specifieke kennis die zij hebben over de sectoren en met consultatie van de betrokkenen binnen die sectoren. Door het overleg met de betrokken sector kan zoveel mogelijk maatwerk worden geleverd per sector, subsector, soort entiteit of entiteit. Indien relevant kan zodoende ook rekening worden gehouden met andere sectorale meldplichten en de daarvoor geldende drempelwaarden. Het vaststellen van de drempelwaarden per sector geeft entiteiten duidelijkheid over welke incidenten meldplichtig zijn. Daarbij wordt zoveel mogelijk voorkomen dat entiteiten uit voorzorg melden, al kan niet volledig worden uitgesloten dat dit soms toch gebeurt.

5. Uitvoerbaarheid / handhaafbaarheid

In juni 2024 heeft de Eerste Kamer motie-Fiers c.s. aangenomen met daarin een aantal voorwaarden voor de behandeling van digitaliseringswetgeving.[20] In deze motie wordt een drietal zaken gevraagd:

1. *bij de toekomstige wetsbehandeling van digitaliseringswetgeving (zowel nationale wetgeving als implementatiewetgeving van de Europese richtlijnen) inzicht te bieden in de samenhang van het voorliggende wetsvoorstel met bestaande en te verwachten digitaliseringswetten, zodat de Kamer een wetsvoorstel in de juridische context kan beoordelen;*

2. *bij toekomstige voorstellen voor digitaliseringswetgeving altijd vooraf een Uitvoeringstoets Decentrale Overheden (UDO) te laten uitvoeren, waarbij de samenhang met bestaande en te verwachten digitaliseringswetgeving wordt meegenomen en getoetst op uitvoerbaarheid, waarmee rekening wordt gehouden met juridische, organisatorische en technische implicaties, zodat de Kamer deze kan betrekken bij de beoordeling van voorstellen van digitaliseringswetgeving;*

3. *bij voorstellen voor toekomstige digitaliseringswetgeving een helder, met de medeoverheden afgestemd, implementatiepad aan te geven (onder andere AMvB's, KB's), met een haalbare implementatietermijn en met inschatting van de kosten voor invoering, zodat de Kamer dit kan betrekken bij de beoordeling om te komen tot zorgvuldige implementatie volgens de bedoeling van de wet.*

[20] *Kamerstukken I 2025/26, 36.382, D.*

Aan deze drie vereisten is niet voldaan. De leden van de fracties van GroenLinks-PvdA en PvdD verzoeken de regering om hier alsnog aan te voldoen.

De regering is van mening dat reeds is voldaan aan het drietal onderdelen waar in de motie van het lid Fiers c.s. naar wordt verwezen. Dit wordt hierna nader toegelicht.

In de eerste plaats verzoekt deze motie om inzicht te bieden in de samenhang van het voorliggende wetsvoorstel met bestaande en te verwachten digitaliseringsvoorstellen. In de memorie van toelichting op het wetsvoorstel voor de Cbw wordt de samenhang tussen de Cbw en de Wwke, en de samenhang tussen andere Europese richtlijnen en verordeningen, zoals de zogeheten *Digital Operational Resilience Act* (DORA)[21], nader toegelicht. In aanvulling daarop is in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties door de Vereniging voor Nederlandse Gemeenten (VNG) uitgewerkt wat de consequenties van onderdelen van de verschillende digitaliseringswetgeving zijn en hoe deze met elkaar samenhangen. In juni 2024 is de Uitvoeringsanalyse Digital Decade Regelgeving beveiliging netwerk- en informatiesystemen gepubliceerd.[22] Daarin zijn de gevolgen van de NIS2-richtlijn, de Cyberbeveiligingsverordening[23], de Cyberweerbaarheidsverordening[24] en de CER-richtlijn uitgewerkt, alsmede de onderlinge samenhang en de verhouding met andere digitaliseringswetten. Dit rapport laat onder meer zien dat bredere ontwikkelingen van invloed zijn op de uitvoeringscapaciteit van medeoverheden, meer specifiek de structurele financiële tekorten bij gemeenten en de krapte op de arbeidsmarkt binnen bepaalde expertisegebieden.

Ten tweede verzoekt deze motie de Uitvoerbaarheidstoets Decentrale Overheden (hierna: UDO) uit te voeren bij toekomstige voorstellen voor digitaliseringsvoorstellen. Zoals uitgewerkt in de Handleiding Uitvoerbaarheidstoets Decentrale Overheden behelst de UDO een gezamenlijk proces waarin het Rijk en de koepels komen tot beleid dat uitvoerbaar is en de gewenste doelen nastreeft.[25] In de eerdergenoemde Uitvoeringsanalyse Digital Decade Regelgeving beveiliging netwerk- en informatiesystemen komt naar voren dat een groot deel van de gevolgen voor decentrale overheden afhankelijk is van de nationale invulling die de implementatie van de NIS2-richtlijn met zich meebrengt. De Cbw behelst namelijk omzetting van bepalingen vanuit de NIS2-richtlijn in nationale wetgeving en kent een hoger abstractieniveau, omdat deze van toepassing is op alle entiteiten uit alle sectoren waarop de Cbw van toepassing is. Aangezien de gevolgen voor medeoverheden met name voortkomen uit nadere regelgeving onder de Cbw, zoals het Cbb en de ministeriële regelingen onder de Cbw die gelden voor overheidsorganisaties, is ervoor gekozen om de UDO vooral te richten op die nadere regelgeving. Ter uitvoering van de UDO hebben het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en het Ministerie van Infrastructuur en Waterstaat om die reden gedurende de afgelopen jaren veel overleggen gevoerd met respectievelijk gemeenten en provincies en de waterschappen. Als onderdeel hiervan is door de medeoverheden nader onderzocht wat de impact van nieuwe wetgeving (zoals de Cbw) is, onder meer in verhouding tot reeds geldende wet- en regelgeving voor medeoverheden. Een voorbeeld hiervan is de eerdergenoemde Uitvoeringsanalyse Digital Decade Regelgeving beveiliging netwerk- en informatiesystemen, een onderzoeksrapport van de Vereniging voor Nederlandse Gemeenten (VNG).[26] Inzichten daaruit dienen ter ondersteuning van het UDO-proces. In lijn met de hiervoor genoemde handleiding brengt de UDO niet noodzakelijk afzonderlijke rapportageverplichtingen met zich mee. De uitkomsten van het UDO-proces voor de Cbw worden verwerkt in onder meer de toelichtingen op de ministeriële regelingen onder de Cbw die gelden voor overheidsinstanties.

In de derde en laatste plaats verzoekt deze motie een helder implementatiepad te geven voor het voldoen aan verplichtingen. Hier geldt dat de verplichtingen voor alle entiteiten uit alle sectoren uit de Cbw gelden zodra de Cbw in werking treedt. Voor entiteiten die behoren tot de centrale overheid voorziet de NIS2-richtlijn niet in een overgangstermijn. Voor medeoverheden wordt hier vanuit de NIS2-richtlijn ruimte voor gelaten. Niettemin is ervoor gekozen om voor de gehele overheid een

---

[21] 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).

[22] Deze analyse is te raadplegen op https://vng.nl/sites/default/files/2024-07/rapport_uitvoeringsanalyse_regelgeving_beveiliging_netwerk-en_informatiesystemen_digital_decade.pdf.

[23] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening) (*PbEU* 2019, L 151).

[24] Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid) (*PbEU* 2024/2847).

[25] Deze handleiding is te raadplegen op https://zoek.officielebekendmakingen.nl/blg-1070574.pdf.

[26] Dit rapport is te raadplegen op https://vng.nl/artikelen/rapport-inzicht-in-gemeentelijke-kosten-en-aanpak-van-informatiebeveiliging.

gelijke inwerkingtredingsdatum te kiezen, gelijktijdig met wat geldt voor entiteiten uit de andere sectoren.[27]
Ten eerste omdat het voor overheidsorganisaties reeds lange tijd bekend is dat zij onder de reikwijdte van de Cbw komen te vallen. De medeoverheden zijn in aanloop naar de (aanstaande) inwerkingtreding van de Cbw vanaf november 2023 formeel per brief geïnformeerd over de verplichtingen uit de Cbw die eraan komen.[28] De aankondiging voor het wettelijk verplichten van informatiebeveiliging bij overheidsorganisaties dateert al van lang geleden. In 2018 is de noodzaak voor wetgeving bevestigd in een Kamerbrief[29] en reeds in 2021 is aangekondigd[30] dat de wettelijke verankering van informatieveiligheid wordt voorbereid. Ook is dit voornemen opgenomen in de tweede editie van de Werkagenda Waardengedreven Digitaliseren.[31] Naast dit algemene voornemen voor wetgeving op informatieveiligheid bij overheidsinstanties, is ook de invulling van deze verplichtingen langere tijd bij overheidsorganisaties bekend. In september 2025 is namelijk al overheidsbreed akkoord gegeven op de inhoud van de BIO2. Betrokken bestuurslagen hebben als onderdeel hiervan het advies gekregen de BIO2 onderdeel te maken van nadere regelgeving voor overheidsorganisaties onder de Cbw.
Ten tweede maken overheidsorganisaties deel uit van verschillende bestuurlijke ketens, zowel vanuit andere sectoren als met de centrale overheid, waar geen mogelijkheid bestaat tot het kiezen voor een andere implementatietermijn. Denk bijvoorbeeld aan de rol van gemeenten in het kader van afvalwater of interbestuurlijke ketens zoals de Basisregistratie Personen. Medeoverheden worden ook wanneer zij zelf een langere implementatietermijn krijgen, direct geconfronteerd met eisen op deze terreinen. Omwille van de duidelijkheid en rechtszekerheid geldt om die reden voor de gehele overheid hetzelfde moment van inwerkingtreding van de verplichtingen uit de Cbw. Dit is in lijn met de brede maatschappelijke functie die de gehele overheid heeft om met een verantwoorde manier om te gaan met de gegevens van burgers.

De Eerste Kamer heeft op 7 oktober 2025 per brief aan de regering te kennen gegeven dat uitvoerbaarheidstoetsen belangrijk zijn om de uitvoerbaarheid van wetgeving goed te kunnen beoordelen.[32] In deze Kamerbrief wordt vervolgens ook ingegaan op een aantal kwalitatieve eisen waaraan een uitvoerbaarheidstoets moet voldoen. Bij deze voorliggende wet zijn consultatiereacties van enkele belangrijke uitvoerende instanties en overheden gevoegd, maar deze consultatiereacties, op de concept-wetgeving, geven geen zicht op de uitvoerbaarheid van de uiteindelijke wet die voorligt. Daarom verzoeken de leden van de fracties van GroenLinks-PvdA en PvdD aan de regering om de Eerste Kamer alsnog te voorzien van uitvoerbaarheidstoetsen op de voorliggende, geamendeerde, wet van de betrokken organisaties/instanties.

Veel van de instanties die een consultatiereactie hebben gegeven op een eerder concept van het voorliggend wetsvoorstel, zijn ingegaan op de uitvoerbaarheid. De regering heeft bezien of die consultatiereacties, evenals alle andere consultatiereacties, aanleiding geven tot aanpassing van het wetsvoorstel of de bijbehorende memorie van toelichting. De consultatie heeft op punten geleid tot aanpassingen in het wetsvoorstel en de memorie van toelichting. De regering ziet echter geen aanleiding om het wetsvoorstel dat nu ter behandeling in de Eerste Kamer te voorzien van een uitvoerbaarheidstoets. Dat is in deze fase van het wetstraject niet gebruikelijk, maar in dit verband ook niet nodig. Ten opzichte van het concept van het wetsvoorstel dat in consultatie is gegaan, zijn er geen aanvullende verplichtingen opgenomen in het voorliggende wetsvoorstel.

Daarnaast vragen deze leden welke ondersteuning middelgrote organisaties krijgen die niet beschikken over eigen cybersecurityafdelingen?

Door diverse organisaties binnen de rijksoverheid tools, handreikingen 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.

[27] Uitzondering hierop is de sector onderwijs. Op grond van artikel 97 Cbw geldt de zorgplicht uit de Cbw voor hogeronderwijsinstellingen vanaf 36 maanden na de aanwijzing als essentiële entiteit of belangrijke entiteit.
[28] Deze brief is te raadplegen op https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2024/12/getekende-brief-NIS2-bij-de-overheid-met-link.pdf.
[29] *Kamerstukken II* 2018/19, 26643, nr. 574.
[30] *Kamerstukken II* 2020/21, 26643, nr. 749.
[31] *Kamerstukken II* 2022/23, 26643, nr. 940.
[32] *Kamerstukken I 2025/26, 31.731 / 29.362, X.*

- De RDI heeft twee tools gelanceerd om entiteiten te helpen in hun voorbereiding op de Cbw: een zelfevaluatietool[33] om te bezien of een entiteit onder de NIS2-richtlijn valt en een quickscan[34] 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 BIO2, en sectorale wet- en regelgeving zoals de zogeheten *Digital Operational Resilience Act* (DORA).[35]
- 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.

Hoe wordt voorkomen dat kleinere organisaties disproportioneel zwaar worden belast?

Bij het opstellen van deze wet- en regelgeving is nadrukkelijk oog geweest voor de administratieve last en de regeldruk die bedrijven zullen ervaren als gevolg daarvan. Er is gekozen voor een risicogebaseerde aanpak, zodat entiteiten ruimte hebben om risicogebaseerd een eigen invulling te geven aan de verplichte maatregelen. Deze risicogebaseerde aanpak biedt ruimte om gezien de context van de organisatie tot de meest (kosten)effectieve oplossing te komen en geeft de mogelijkheid om bijvoorbeeld verschillende wettelijke verplichtingen te combineren. Zo kan ervoor gekozen worden om een integrale risicobeoordeling uit te voeren voor de Wwke en de Cbw. Dit kan voor bedrijven een vermindering in de administratieve lasten betekenen en bij hen onnodige regeldruk voorkomen.

De proportionaliteit volgt in zichzelf uit het feit dat de maatregelen die essentiële entiteiten en belangrijke entiteiten op grond van de Cbw moeten nemen, passend en evenredig moeten zijn in relatie tot de specifieke risico's waarmee de entiteiten ten aanzien van de beveiliging van netwerk- en informatiesystemen kunnen worden geconfronteerd. Bij de beoordeling of een maatregel of combinatie van maatregelen passend is, wordt allereerst gekeken naar de effectiviteit van de maatregel om de betreffende risico's te beheersen. Hierbij gaat het er om dat de juiste maatregel op de juiste plek wordt ingezet. De effectiviteit van een maatregel kan onder andere worden afgeleid uit wat daarover beschreven staat in Europese en internationale standaarden, evenals de stand van de techniek en de door de entiteit uitgevoerde risicoanalyses. Europese of internationale standaarden kunnen een goede indicatie geven dat een maatregel passend is of zou kunnen zijn om een of meer van de genoemde doelen te bereiken. Dat geldt ook voor maatregelen die de actuele stand van de techniek benutten of toepassen. Daarnaast geldt het vereiste van evenredigheid. Dit betekent dat een maatregel of coherente set van maatregelen in verhouding dient te staan tot het te beheersen risico. De entiteit dient daarbij naar behoren rekening te houden met de mate waarin de entiteit aan risico's is blootgesteld, evenals de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen. Ook de omvang van de entiteit kan een rol spelen bij de vraag of maatregelenevenredig zijn. Wat ook een rol kan spelen bij de evenredigheid van maatregelen, zijn de nadelige effecten of risico's van die maatregelen, zoals de verstoring van de continuïteit van de kritieke processen van een entiteit. De omvang van een entiteit of de hoogte van uitvoeringskosten kan van invloed zijn op de keuze van de te nemen maatregelen. Een beperkte financiële capaciteit of een beperkte omvang van een entiteit kan een entiteit echter niet algeheel ontslaan van de verplichting om – kort gezegd – de weerbaarheid op orde te hebben. De evenredigheid houdt daarnaast in dat een maatregel of coherente set van maatregelen het minst belastend is voor de entiteit om het risico te beheersen.

Kan de regering de leden van de fractie van de VVD een totaaloverzicht geven van alle toezichthoudende instanties en hoe coördinatie (one-stop-shop) wordt geborgd?

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

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

[35] 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).

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.[36] De vakministers wijzen bij besluit de ambtenaren aan die onder verantwoordelijkheid van de vakministers zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Cbw, zie artikel 68, eerste lid, Cbw.[37] Daarbij zal het gaan om de aanwijzing van ambtenaren van verschillende organisaties, afhankelijk van de sector. Om welke organisaties het hierbij gaat, wordt hierna aangeduid als “toezichthoudende instantie”. Voor de beantwoording van de vraag van de leden van de VVD-fractie wordt hierna eerst de tabel in artikel 15, eerste lid, Cbw aangehaald.

Bevoegde autoriteit	**Sector**	**Subsector**	**Toezichthoudende instantie**
Minister van Binnenlandse Zaken en Koninkrijksrelaties	overheid	centrale overheden	RDI
		decentrale overheden, uitgezonderd de waterschappen	
Minister van Economische Zaken	digitale infrastructuur		RDI
	beheer van ICT-diensten (business-to-business)		
	ruimtevaart		
	post- en koeriersdiensten		
	vervaardiging	vervaardiging van informaticaproducten en van elektronische en optische producten	
		vervaardiging van elektrische apparatuur	
		vervaardiging van machines, apparaten en werktuigen, niet elders geclassificeerd	
		vervaardiging van motorvoertuigen, aanhangers en opleggers	
		vervaardiging van andere transportmiddelen	
	digitale aanbieders		
Minister van Financiën	bankwezen		De Nederlandsche Bank
	infrastructuur voor de financiële markt		Autoriteit Financiële Markten
Minister van Infrastructuur en Waterstaat	vervoer	lucht	Inspectie Leefomgeving en Transport
		spoor	
		water	
		weg	
	drinkwater (uitgezonderd verpakt drinkwater)		
	afvalwater		
	afvalstoffenbeheer		
	vervaardiging, productie en distributie van chemische stoffen		
	overheid	decentrale overheden, alleen voor wat betreft de waterschappen	
	drinkwater (verpakt drinkwater)		Nederlandse Voedsel- en Warenautoriteit
Minister van Klimaat en Groene Groei	energie	elektriciteit	RDI
		stadsverwarming en -koeling	
		aardolie	
		aardgas	
		waterstof	
Minister van Landbouw,	productie, verwerking en		Nederlandse Voedsel- en

[36] 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.

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

Visserij, Voedselzekerheid en Natuur	distributie van levensmiddelen		Warenautoriteit
Minister van Volksgezondheid, Welzijn en Sport	gezondheidszorg		Inspectie Gezondheidszorg en Jeugd
	vervaardiging	vervaardiging van medische hulpmiddelen en medische hulpmiddelen voor in-vitrodiagnostiek	

Aanvullend op bovenstaande tabel geldt het volgende.

De Minister van Economische Zaken (thans de Minister van Economische Zaken en Klimaat) is de bevoegde autoriteit voor de entiteiten die domeinnaamregistratiediensten verlenen. Ambtenaren van de RDI zullen worden aangewezen voor het toezicht op de naleving van de verplichtingen die voor deze entiteiten gelden.[38]

De Minister van Onderwijs, Cultuur en Wetenschap is de bevoegde autoriteit voor de hogeronderwijsinstellingen die op grond van artikel 11 Cbw als essentiële entiteit of op grond van artikel 13 Cbw als belangrijke entiteit kunnen worden aangewezen. De Minister van Onderwijs, Cultuur en Wetenschap heeft in een brief aan de Tweede Kamer aangegeven voornemens te zijn te besluiten om ambtenaren van de Inspectie van het Onderwijs te belasten met het toezicht op de naleving van de verplichtingen die voor deze entiteiten bij aanwijzing gaan gelden.[39]

Voor de sector onderzoek is de bevoegde autoriteit de minister die reeds is aangewezen als bevoegde autoriteit voor de sector of subsector waarin die onderzoeksorganisatie haar onderzoeksactiviteiten verricht. Voor bijvoorbeeld een onderzoeksorganisatie die onderzoek doet in de sector levensmiddelen is de Minister van Landbouw, Visserij, Voedselzekerheid en Natuur de bevoegde autoriteit en voor een onderzoeksorganisatie die onderzoek doet naar ruimtevaart de Minister van Economische Zaken (thans de Minister van Economische Zaken en Klimaat). Voor onderzoeksorganisaties die onderzoek doen in een sector waarvoor op grond van de Cbw nog geen bevoegde autoriteit is aangewezen, is de bevoegde autoriteit de Minister die het aangaat. Dat betekent bijvoorbeeld dat voor een onderzoeksorganisatie die onderzoek doet op onderwerpen die onder de beleidsverantwoordelijkheid van het Ministerie van Defensie vallen, de Minister van Defensie de bevoegde autoriteit is.

De coördinatie tussen de hiervoor genoemde instanties wordt geborgd dankzij samenwerkingsafspraken, die zij formaliseren in een samenwerkingsprotocol. Hierin wordt onder meer vastgelegd hoe wordt omgegaan met overlap in het toezicht waarbij een entiteit te maken heeft met meerdere toezichthoudende instanties.

Kan de regering deze leden toelichten hoe de persoonlijke aansprakelijkheid van bestuurders zich verhoudt tot bestaande privaat- en bestuursrechtelijke aansprakelijkheidsregimes? Bestaat het risico op over-compliance en defensief bestuur?

Als een bestuurslid van een essentiële entiteit of een belangrijke entiteit de in artikel 24, tweede tot en met zesde lid, Cbw opgenomen opleidingsverplichting niet naleeft, kan dat op grond van artikel 93 Cbw bestuursrechtelijk worden gesanctioneerd met een bestuurlijke boete van maximaal € 25.000,–. De Cbw bevat in artikel 92 ook de mogelijkheid om een last onder dwangsom op te leggen aan het bestuurslid. Deze bevoegdheden zien specifiek op de hiervoor genoemde opleidingsverplichting. De Cbw voorziet verder niet in nieuwe regels over de aansprakelijkheid van leden van het bestuur voor de naleving van de verplichtingen uit de Cbw. Het bestaande aansprakelijkheidsregime (zowel bestuurs- als civielrechtelijk) is dan ook onverkort en ongewijzigd van toepassing.

In antwoord op de vraag over de verhouding tot het bestaand bestuursrechtelijk aansprakelijkheidsregime licht de regering het volgende toe. In artikel 5:1, eerste lid, Awb is bepaald dat in de Awb wordt verstaan onder een overtreding: een gedraging die in strijd is met het bepaalde bij of krachtens enig wettelijk voorschrift. In artikel 5:1, tweede lid, Awb is bepaald dat onder overtreder wordt verstaan: degene die de overtreding pleegt of medepleegt.

[38] Op deze entiteiten is een aantal verplichtingen uit de Cbw, waaronder de zorgplicht en de meldplicht, niet van toepassing, voor zover zij niet tevens een essentiële entiteit of belangrijke entiteit in de zin van de Cbw zijn. In dat geval gelden voor hen uitsluitend andere specifieke verplichtingen, zoals die over het verzamelen van domeinnaamregistratiegegevens in een database (artikel 49 Cbw). Voor deze entiteiten gelden deze specifieke verplichtingen, vanwege hun belang voor de beveiliging, weerbaarheid en stabiliteit van het domeinnaamsysteem. Indien een aanbieder van domeinnaamregistratiediensten tevens een belangrijke entiteit of essentiële entiteit is, gelden de bijhorende verplichtingen, zoals de zorgplicht en de meldplicht, uiteraard wel.

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

Artikel 5:1, derde lid, Awb bepaalt dat overtredingen kunnen worden begaan door natuurlijke personen en rechtspersonen en dat artikel 51,tweede en derde lid, Wetboek van Strafrecht van overeenkomstige toepassing is. Artikel 51, tweede lid, Wetboek van Strafrecht bepaalt dat indien een strafbaar feit wordt begaan door een rechtspersoon, de strafvervolging kan worden ingesteld en de in de wet voorziene straffen en maatregelen kunnen worden uitgesproken tegen die rechtspersoon, dan wel tegen de opdrachtgever of feitelijk leidinggevende, dan wel tegen de hiervoor genoemden tezamen. In artikel 51, derde lid, Wetboek van Strafrecht wordt voor de toepassing van het tweede lid met de rechtspersonen gelijkgesteld: de vennootschap zonder rechtspersoonlijkheid, de maatschap, de rederij en het doelvermogen.

Door de schakelbepaling in artikel 5:1, derde lid, Awb is het mogelijk om in het geval dat een overtreding is gepleegd of medegepleegd door een rechtspersoon, een bestuurlijke boete of een last onder bestuursdwang of dwangsom op te leggen aan degenen die tot de door de rechtspersoon begane overtreding opdracht hebben gegeven of daaraan feitelijk leiding hebben gegeven. De bevoegde autoriteit kan bij een overtreding van een verplichting uit de Cbw dus 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. Meer specifiek kan het in het eerste geval gaan om een bestuurder van een entiteit. Bij het laatste geval kan bijvoorbeeld gedacht worden aan een moedermaatschappij die als feitelijke leidinggevende of opdrachtgever kwalificeert van een overtreding bij een dochteronderneming.

In antwoord op de vraag over de verhouding tot het bestaand privaatrechtelijk aansprakelijkheidsregime wordt gewezen op artikel 2:9 Burgerlijk Wetboek. In dit artikel is onder meer bepaald dat elke bestuurder tegenover de rechtspersoon gehouden is tot een behoorlijke vervulling van zijn taak (eerste lid), dat elke bestuurder de verantwoordelijkheid voor de algemene gang van zaken draagt en dat een bestuurder voor het geheel aansprakelijk is voor onbehoorlijk bestuur, tenzij – kort gezegd – hem geen verwijt kan worden gemaakt en hij niet nalatig is geweest (tweede lid).

De regering ziet niet het risico van over-compliance en defensief bestuur. Voor bestuursleden van essentiële entiteiten en belangrijke entiteiten geldt dat zij moeten voldoen aan de in artikel 24, tweede tot en met zesde lid, Cbw opgenomen opleidingsverplichting. Zoals hiervoor reeds aangegeven voorziet de Cbw verder niet in nieuwe regels over de aansprakelijkheid van leden van het bestuur voor de naleving van de verplichtingen uit de Cbw. Het bestaande aansprakelijkheidsregime (zowel bestuurs- als civielrechtelijk) is dan ook onverkort en ongewijzigd van toepassing.

De leden van de fractie van D66 lezen dat de regering aangeeft dat afhankelijkheid van bepaalde leveranciers een te groot risico kan vormen ten aanzien van de beveiliging van digitale systemen. Dit zou kunnen volgen uit de risicobeoordelingen die belangrijke en essentiële entiteiten moeten doen. Het afbouwen van dergelijke afhankelijkheid zou de Nederlandse strategische autonomie ten goede kunnen komen. Kan de regering voorbeelden noemen van gevallen waarin de afhankelijkheid als zodanig groot kan worden gezien, dat het wenselijk is om te stoppen met bepaalde leveranciers? Moet er een concrete aanleiding zijn, zoals een incident ten aanzien van de entiteit zelf, waardoor entiteiten kunnen waarnemen dat de afhankelijkheid te groot is, of kan de macht van een leverancier op zichzelf al reden genoeg zijn?

De NIS2-richtlijn erkent in overweging 90 met betrekking tot artikel 21, tweede lid, NIS2-richtlijn dat afhankelijkheden en andere niet-technische risicofactoren een risico kunnen vormen voor de beveiliging en de weerbaarheid van netwerk- en informatiesystemen. Voorbeelden van die risico’s zijn ongepaste beïnvloeding door derde landen, technologische lock-ins of verborgen kwetsbaarheden.

De regering ziet het in kaart brengen van en het bepalen van de omgang met dergelijke afhankelijkheden als een belangrijk onderdeel van de maatregelen die essentiële entiteiten en belangrijke entiteiten met betrekking tot de beveiliging van de toeleveringsketen moeten nemen. In artikel 10, eerste lid, van het concept van het Cbb, de algemene maatregel van bestuur onder de Cbw, 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.

Uit de in artikel 21 Cbw voorgeschreven risicoanalyse zou kunnen 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 leveranciers van 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.

Omdat de netwerk- en informatiesystemen en de leverancierskеten van iedere entiteit er anders uitzien, is het niet mogelijk om op voorhand al specifieke voorbeelden te geven van leveranciers waarmee gestopt dient te worden. Dit dient namelijk te blijken uit de risicobeoordeling van entiteiten zelf.

Entiteiten zijn zelf verantwoordelijk voor het uitvoeren van een risicoanalyse. Dit begint met het in kaart brengen van de zogenaamde “kroonjuwelen” van de organisatie: de meest kritieke processen en middelen. Vervolgens worden de risico’s voor deze kroonjuwelen geïdentificeerd. Op basis van de kans en de mogelijke gevolgen van deze risico’s kan de entiteit besluiten nemen over te treffen maatregelen. Er zijn verschillende methoden om risico’s te identificeren. Zo kan er worden gekeken worden naar incidenten die al eens hebben plaatsgevonden, zoals het verliezen van bestanden of een stroomstoring.

Voor het constateren dat een afhankelijkheid te groot is, hoeft zich dus niet noodzakelijk eerst een incident bij de entiteit zelf te hebben voorgedaan. De macht van een leverancier kan op zichzelf al voldoende reden zijn om de afhankelijkheid af te bouwen, mits dit als een zodanig risico naar voren komt uit de risicobeoordeling die de entiteit uitvoert. In die beoordeling wordt de afhankelijkheid steeds gewogen in samenhang met de kans en de gevolgen voor de kroonjuwelen van de entiteit. Een concrete aanleiding zoals een incident kan dit risico zichtbaar maken, maar is daarvoor geen voorwaarde.

Daarnaast heeft de regering in de nota naar aanleiding van het verslag aangegeven dat er geen verkenning heeft plaatsgevonden ten aanzien van de vraag of er genoeg materiaal en genoeg cursussen beschikbaar zijn om bestuursleden op te leiden over cyberveiligheid.[40] Daarbij heeft de regering te kennen gegeven dat dit niet is gebeurd, omdat bekend zou zijn dat er voldoende aanbieders van cursussen zijn. Waar baseert de regering dit op, wanneer er geen verkenning heeft plaatsgevonden? Deze leden merken op dat genoeg aanbieders niet noodzakelijkerwijs betekent dat de kwaliteit van de cursussen goed is. Ook is onduidelijk wat voor soort materiaal er beschikbaar is. Is de regering voornemens om hier een verkenning naar uit te voeren? Zo nee, waarom niet?

De regering ziet geen aanleiding om de in de vraagstelling bedoelde verkenningen uit te voeren. De regering ziet dat op dit moment veel partijen, waaronder opleidingsinstituten en adviesbureaus, trainingen aanbieden op het gebied van ICT en informatiebeveiliging. Het materiaal dat daarvoor beschikbaar wordt gesteld zal verschillend zijn. Om te voldoen aan de in artikel 24, tweede lid jo. vijfde lid, Cbw opgenomen trainingsverplichting en verplichting om een certificaat te bezitten waaruit deelname blijkt van die training, kan – in plaats van een training bij een externe partij – ook een interne training worden gevolgd, verzorgd door de functionarissen die daartoe de expertise hebben. Op basis van het voorgaande is de regering van mening dat er voor bestuursleden voldoende mogelijkheden zijn om aan de hiervoor genoemde verplichtingen te voldoen en ziet geen aanleiding voor nadere verkenningen.

De regering maakt melding van een verwacht aantal meldingen per jaar.[41] Ten aanzien van de Computer Security Incident Response Teams geeft zij aan dat deze teams op dit moment voorbereidingen treffen om hier in de toekomst mee om te kunnen gaan. Kan de regering aan deze leden toelichten om wat voor voorbereidingen het hier gaat?

De beoogde CSIRT’s bereiden zich voor op meldingen in het kader van de Cbw door uitbreiding van het personeel, door de onderlinge samenwerking te intensiveren en door hun systemen verder te beveiligen.

Daarnaast laat de regering weten dat het cyberlandschap snel verandert. Voorziet de regering steeds meer meldingen? Wat betekent het aantal meldingen en een mogelijke stijging van het aantal meldingen over tijd voor de werklast en operationele capaciteit van de teams?

Een snel veranderend cyberlandschap betekent volgens de regering niet noodzakelijkerwijs meer meldingen in het kader van de Cbw. De regering wijst er in dit verband op dat voor essentiële entiteiten en belangrijke entiteiten in de zin van de Cbw de zorgplicht uit artikel 21 Cbw geldt. Zij moeten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico’s voor de beveiliging van de netwerk- en informatiesystemen, die zij voor hun

[40] *Kamerstukken II 2025/26, 36.764, nr. 8.*
[41] *Kamerstukken II 2025/26, 36.764, nr. 8.*

werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheersen. Ook moeten zij deze maatregelen nemen om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken. Artikel 21, tweede lid, Cbw schrijft voor dat die maatregelen zorgen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de hiervoor bedoelde risico's. De hiervoor bedoelde maatregelen kunnen incidenten voorkomen, wat ook tot gevolg heeft dat er juist minder meldingen worden gedaan.

Hierbij benadrukt de regering tevens de grote waarde van meldingen. De entiteit krijgt na een melding bijstand van haar CSIRT waarmee in potentie de schade van een significant incident beperkt wordt (en de bijbehorende tijdsinvestering die daarmee gepaard gaat). De melding levert ook informatie op voor andere partijen of inzet in de toekomst. Dit draagt daarmee ook bij aan het voorkomen van incidenten in de toekomst en het mitigeren van de impact van die incidenten.

De regering gaat er van uit dat in de vraagstelling wordt gedoeld op de werklast en operationele capaciteit van de CSIRT's. De beoogde CSIRT's hebben vooruitlopend op de inwerkingtreding van de Cbw hun teams en expertise uitgebreid.

Daarnaast hebben deze leden nog een vraag ten aanzien van de samenstelling van de teams. Hoeveel technische medewerkers zullen ongeveer nodig zijn om alle teams van de wenselijke operationele capaciteit te voorzien? Hoe is de regering van plan om een mogelijk grote hoeveelheid aan vacatures in te vullen, gelet op het grote tekort in Nederland aan beschikbaar personeel in deze sector?

CSIRT's bereiden zich ieder afzonderlijk voor op de inwerkingtreding van de Cbw door hun teams en expertises verder uit te breiden. De Cbw betekent voor het grootste CSIRT, het NCSC, een forse uitbreiding van de doelgroep, waardoor het NCSC straks meer bedrijven en organisaties moet voorzien van informatie en advies. Dit vraagt wat van de operationele capaciteit van het NCSC. Het is echter niet op voorhand in te schatten hoeveel operationele capaciteit nodig is.

De afgelopen periode is fors geïnvesteerd in de versterking van het NCSC om de slagkracht en schaalbaarheid van het NCSC te vergroten. Om de groei van de doelgroep het hoofd te kunnen bieden werkt het NCSC aan een datagedreven aanpak om wendbare en schaalbare dienstverlening mogelijk te maken. Data-analyse zorgt voor beter zicht op dreigingen, patronen en kwetsbaarheden. Hierdoor kunnen risico's effectiever worden ingeschat en kan de capaciteit van het NCSC efficiënt worden ingezet. Ook bevordert deze aanpak informatie-uitwisseling tussen (internationale) publieke en private partners, zodat gezamenlijk een actueel dreigingsbeeld kan worden gevormd en passende maatregelen kunnen worden getroffen. De verwachting is dat ook de komende jaren het NCSC nog verder zal groeien om de nodige dienstverlening te kunnen leveren.

Om te kunnen voldoen aan de wervingsbehoefte binnen een schaarse arbeidsmarkt worden gerichte middelen ingezet. Hierbij ligt de focus op arbeidsmarktcommunicatie en een sterke *employer branding*. Daarnaast wordt geïnvesteerd in samenwerkingen met onderwijsinstellingen, efficiënte recruitmentprocessen en het proactief op zoek gaan naar kandidaten tijdens wervingsprocessen via onder meer LinkedIn en andere online kanalen.

Deze leden lezen dat er duidelijke inschattingen zijn over het aantal organisaties dat aan de verplichtingen in de wet moet voldoen. Tegelijkertijd geeft de regering aan dat in de meeste gevallen de organisaties zelf moeten nagaan of ze een entiteit zijn in de zin van de wet en daarom aan de verplichtingen moeten voldoen. Waarom heeft de regering er niet voor gekozen om organisaties ervan op de hoogte te stellen dat ze onder de wet zouden kunnen gaan vallen, zeker gelet op dat er al wel onderzocht is om welke organisaties het zou gaan?

Er is inderdaad een schatting gemaakt van het aantal organisaties waarop naar verwachting de Cbw van toepassing zal zijn. Pas zodra organisaties die kwalificeren als essentiële entiteit of belangrijke entiteit in de zin van de Cbw zich op grond van artikel 44 Cbw geregistreerd hebben, zal echter duidelijk zijn hoeveel entiteiten er precies onder het toepassingsbereik van de Cbw vallen.

Het merendeel van die entiteiten valt van rechtswege onder het toepassingsbereik van de Cbw. Dit betekent dat zij zelf moeten beoordelen of zij voldoen aan de daarvoor geldende wettelijke criteria, omdat zij bij uitstek degenen zijn die die beoordeling kunnen doen. Voor veel entiteiten geldt dat voor het antwoord op de vraag of zij onder de Cbw vallen dat niet alleen afhangt van de vraag of zij behoren tot een soort entiteit, genoemd in één van de bijlagen bij de Cbw, maar ook of zij gelet op het aantal werknemers, de jaaromzet en het jaarlijkse balanstotaal van een bepaalde omvang zijn. De kennis over die laatstgenoemde aspecten berust uiteraard bij de entiteiten zelf. Ook zijn zij degenen die zicht hebben op een eventuele wijziging in de dienstverlening of de bedrijfsactiviteiten, waardoor zij gaan behoren of juist niet meer behoren tot een soort entiteit, genoemd in één van de

bijlagen bij de Cbw, en zij daardoor onder het toepassingsbereik van de Cbw komen te vallen of juist niet meer onder dat toepassingsbereik vallen.

De RDI heeft een zelfevaluatietool ontwikkeld waarmee entiteiten kunnen toetsen of zij onder het toepassingsbereik van de NIS2-richtlijn vallen.[42]

De leden van de fractie van het CDA constateren dat de Vereniging Nederlandse Gemeenten (VNG) en de Unie van Waterschappen zorgen hebben geuit over de uitvoerbaarheid van de Cyberbeveiligingswet voor decentrale overheden. Daarbij wordt onder andere gewezen op financiële en organisatorische consequenties die uitvoering van de Cyberbeveiligingswet met zich brengt. Deze leden vragen de regering toe te lichten hoe deze zorgen worden ondervangen.

Om de zorgen van medeoverheden voor de consequenties van de Cbw voor de uitvoering zoveel mogelijk te ondervangen, is ervoor gekozen om in de ministeriële regelingen die voor entiteiten uit de sector overheid zullen gelden, zoveel mogelijk aan te sluiten bij reeds voor hen geldende verplichtingen en kaders.

Zo wordt in de ministeriële regelingen in het kader van de nadere invulling van de zorgplicht, bedoeld in artikel 21 Cbw, voor overheidsinstanties bepaald dat zij, in aanvulling op de maatregelen zoals beschreven in het Cbb, meer specifiek moeten voldoen aan de BIO2. Dat is het bestaande normenkader voor informatiebeveiliging waaraan alle overheidslagen zich hebben gecommitteerd.[43] De totstandkoming van de BIO2 heeft bovendien plaatsgevonden onder coördinatie van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in samenwerking met alle bestuurslagen.

Ook voor het bepalen van de drempelwaarden in het kader van de meldplicht is zoveel mogelijk aangesloten bij bestaande uitgangspunten. Hiervoor worden criteria gebruikt op basis waarvan gemeenten reeds hun incidentmeldingen doen bij de Informatiebeveiligingsdienst. Ook waterschappen zijn, via de Unie van Waterschappen, actief betrokken bij het wetgevingsproces. Zo is voor de Cybersecurityregeling IenW uitvoerig gesproken over de uitvoerbaarheid van de drempelwaarden in het kader van de meldplicht.

Voor de registratieplicht, bedoeld in artikel 44 Cbw, geldt dat een deel van de gegevens die entiteiten op grond van dat artikel moeten aanleveren, reeds beschikbaar is of al op grond van andere verplichtingen wordt aangeleverd. Hierbij kan worden gedacht aan domeinnamen die in het kader van digi-toegankelijkheid reeds zijn geregistreerd in het Dashboard DigiToegankelijkheid en algemene gegevens uit het Register van Overheidsorganisaties. Daarnaast zal voor toezicht en verantwoording zoveel mogelijk gebruik worden gemaakt van bestaande verantwoording van medeoverheden, zoals de Eenduidige Normatiek Single Information Audit (ENSIA) die door gemeenten wordt gebruikt.

Buiten deze verplichtingen die dus zoveel mogelijk aansluiten bij bestaande instrumenten of verplichtingen, kent de Cbw voor medeoverheden slechts beperkt aanvullende verplichtingen. Voor medeoverheden zal de trainingsverplichting voor bestuurders, bedoeld in artikel 24, tweede en vijfde lid, Cbw geheel nieuw zijn. Hiervoor geldt dat de invulling van deze verplichting samen met de overheidsorganisaties wordt uitgewerkt. Het doel is om te komen tot een opleiding die overheidsorganisaties zelf kunnen geven, zodat zij niet afhankelijk zijn van het inkopen van deze training bij marktpartijen. Op grond van artikel 24, derde lid, Cbw moet binnen twee jaar na de inwerkingtreding van de Cbw zijn voldaan aan de trainingsverplichting. De meldplicht is als expliciete verplichting nieuw. Tegelijkertijd zijn overheidsorganisaties al wel gewend om meldingen van incidenten te doen bij partijen als het NCSC, de Informatiebeveiligingsdienst en de Autoriteit persoonsgegevens. Daardoor zijn er veelal al processen ingericht om de meldingen te doen en op te volgen.

Gedurende het gehele wetgevingsproces voor het wetsvoorstel voor de Cbw is uitgebreid contact geweest met medeoverheden om zorgen in een vroeg stadium mee te nemen en waar nodig conceptregelgeving dusdanig aan te passen zodat deze zorgen ondervangen kunnen worden. Dat is in lijn met het proces van de UDO.

Een veelgehoorde zorg bij de Cyberbeveiligingswet ziet toe op de regeldruk. De leden van de PVV-fractie vinden dit een terechte zorg en vrezen dat er vanuit de EU bij de totstandkoming van de Cyberbeveiligingswet onvoldoende aandacht is geweest voor de reeds aanwezige controlemechanieken en protocollen die in het kader van de ketenafhankelijkheid al reeds sinds jaar en dag toezien op, onder meer, cyberveiligheid. Te denken valt aan de Corporate Sustainability Reporting Directive (CSRD) die bedrijven verplicht om duidelijk te laten zien wat de impact is van

[42] Te raadplegen op https://regelhulpenvoorbedrijven.nl/NIS-2-NL/.
[43] *Stcrt*. 2020, 7857.

hun bedrijfsactiviteiten, waarbij het gaat om effecten op mens, milieu en klimaat over de hele waardeketen en die moet voldoen aan de European Sustainability Reporting Standards (ESRS). Vele bedrijven zijn aangesloten bij platforms en beoordelingsbureaus die gespecialiseerd zijn in zogenaamde Environmental, Social en Governance (ESG)-ratings en het controleren van duurzaamheid in wereldwijde toeleveringsketens. De ketenpartners van deze bedrijven worden overstelpt met verplichte questionnaires die onderbouwd moeten worden met bewijslast, zoals certificaten, rapportages, diploma's, verklaringen, et cetera. Voor ieder platform en beoordelingsbureau dient dit nét anders te worden onderbouwd. Kleinere ketenpartners lopen steeds verder uit de pas vanwege onvoldoende beschikbare capaciteit. Deze leden zien graag een inventarisatie van de regering van de beschikbare platforms en beoordelingsbureaus en hun aangeboden pakketten die reeds voldoen aan de Cyberbeveiligingswet. Tevens willen deze leden van de regering weten wat zij concreet gaat doen om dergelijke repetitieve handelingen terug te dringen en te voorkomen dat de uitvoering van de Cyberbeveiligingswet er ook een wordt?

Uit een recent artikel van Het Financieele Dagblad blijkt dat grote bedrijven per jaar tot circa 6700 arbeidsuren en middelgrote bedrijven circa 3500 uur verwachten te moeten investeren in de voorbereidingen op de implementatie van de Cyberbeveiligingswet.[44] Kan de regering aan de leden van de fractie van JA21 inzichtelijk maken wat de verwachte arbeidsdruk voor het implementeren en naleven van de wet voor kleine bedrijven is? Kan de regering daarnaast aangeven in hoeverre zij het realistisch acht dat kleine, middelgrote en grote bedrijven tijdig aan de verplichtingen uit de Cyberbeveiligingswet kunnen voldoen?

In de nota van toelichting op het Cbb zijn de regeldrukkosten die bedrijven verwachten om te voldoen aan de Cbw en het Cbb beschreven en uitgesplitst voor essentiële entiteiten en belangrijke entiteiten. De verwachte kosten zijn primair het gevolg van de voorbereidingen die bedrijven moeten treffen om aan de zorgplicht te kunnen voldoen, zowel eenmalig als structureel. 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. 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. Voor middelgrote- en kleine bedrijven (hierna: mkb) is een (kwalitatieve) mkb-toets uitgevoerd. Tijdens deze toets is gesproken met een panel van mkb-ondernemers in een open en vertrouwelijk gesprek. Zij konden meedenken over de regelgeving en 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. De Cbw is echter, 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.

De regering acht het realistisch dat een groot deel van bedrijven die onder het toepassingsbereik van de Cbw vallen, tijdig aan de verplichtingen uit de Cbw kunnen voldoen. Een deel van de entiteiten zal reeds in meer of mindere mate investeringen hebben gedaan op het gebied van beveiliging van hun systemen om zodoende incidenten en – als gevolg daarvan – mogelijk grote schadeposten zoveel mogelijk proberen te voorkomen. In dit verband merkt de regering op dat de rijksoverheid bedrijven en organisaties via diverse communicatiekanalen heeft opgeroepen om zich voor te bereiden op de komst van de Cbw en om de inwerkingtreding van de Cbw niet af te wachten.

Door de verwevenheid en complexiteit van beide wetsvoorstellen bestaat het risico dat kleine en middelgrote bedrijven in de praktijk vaak beschikken over onvoldoende capaciteit om te voldoen aan de uitgebreide administratieve verplichtingen. Kan de regering aan deze leden toelichten op welke wijze wordt voorkomen dat de administratieve en bureaucratische druk voor deze bedrijven onevenredig zwaar wordt?

Voor zowel het wetsvoorstel voor de Cbw als het wetsvoorstel voor de Wwke is een regeldruktoets uitgevoerd. Een onderdeel van die toets was een mkb-toets om de verwachte regeldruk voor het midden- en kleinbedrijf in kaart te brengen. Hieruit kwam vanuit het midden- en kleinbedrijf steun voor de risicogebaseerde systematiek van de wetten naar voren. Deze systematiek geeft bedrijven immers de ruimte voor maatwerk, en biedt hen ook de mogelijkheid om bijvoorbeeld verplichtingen uit verschillende wettelijke kaders te combineren. Een voorbeeld hiervan is dat bedrijven zelf kunnen kiezen welke methode of systematiek gebruiken bij het in kaart brengen van hun risico's. Ook kunnen bedrijven bijvoorbeeld het uitvoeren van de risicobeoordeling in het kader van de Cbw en de Wwke combineren om administratieve lasten te verminderen.

[44] *Cyberbeveiligingswet komt eraan, maar bedrijven lopen mijlenver achter, Het Financieele Dagblad, 7 mei 2026.*

Deze leden constateren dat op grond van artikel 24 van de Cyberbeveiligingswet ieder lid van het bestuur van een essentiële of belangrijke entiteit verplicht behoort te beschikken over aantoonbare kennis en vaardigheden op het gebied van cyberbeveiliging, inclusief certificering en het actueel houden daarvan. Artikel 93 voorziet daarnaast in de mogelijkheid om individuele bestuurders bestuurlijk te sanctioneren indien niet aan deze verplichtingen wordt voldaan.

1. *Hoe voorkomt de regering dat persoonlijke sancties moeilijk of niet verzekerbaar blijken voor bestuurders van essentiële en belangrijke entiteiten?*

   De (on)verzekerbaarheid van boetes is een breder vraagstuk dat ook in de vakliteratuur en in de wetenschap is behandeld.[45] Daaruit komt naar voren dat er op de Nederlandse markt verzekeringen zijn die dekking bieden voor bestuurlijke boetes, waarbij veelal de beperking wordt aangebracht dat bestuursrechtelijke boetes onder de dekking vallen “voor zover verzekering van deze boetes door de rechter of wetgever zijn toegestaan”, “voor zover dit wettelijk is toegestaan” of “voor zover wettelijk verzekerbaar”. Zoals ook in de vakliteratuur en in de wetenschap aan de orde is gekomen, is het op dit moment niet duidelijk of het juridisch is toegestaan om bestuurlijke boetes te verzekeren. En indien dat is toegestaan, is evenmin duidelijk in welke gevallen dat is toegestaan. In artikel 3:40, eerste lid, Burgerlijk Wetboek is bepaald dat een rechtshandeling die door inhoud of strekking in strijd is met de goede zeden of de openbare orde nietig is. Of een verzekeringsovereenkomst tot dekking van bestuurlijke boetes naar inhoud of strekking in strijd is met de goede zeden of de openbare orde, dient te worden beoordeeld naar de specifieke omstandigheden van het geval. Het uiteindelijke oordeel daarover is aan de rechter. Hierbij wordt voorts gewezen op artikel 7:952 Burgerlijk Wetboek, waarin is bepaald dat schade die door opzet van de verzekerde is ontstaan, niet kan worden verzekerd.

2. *Kan de regering nader toelichten op welke categorieën van private organisaties en bestuursorganen deze verplichtingen van toepassing zijn? Geldt dit bijvoorbeeld voor bestuurders van veiligheidsregio’s, provincies, gemeenten, waterschappen?*

   De in artikel 24, tweede lid jo. vijfde lid, Cbw opgenomen trainingsverplichting en verplichting om een certificaat te bezitten waaruit deelname blijkt van die training, geldt voor elk lid van het bestuur van een essentiële entiteit en belangrijke entiteit. Dit betekent dat alle leden van het bestuur van private organisaties en bestuursorganen die essentiële entiteit of belangrijke entiteit in de zin van de Cbw zijn, aan die verplichtingen moeten voldoen. Welke organisaties essentiële entiteit en belangrijke entiteit in de zin van de Cbw zijn, wordt geregeld in hoofdstuk 4 van de Cbw. Tot die essentiële entiteiten en belangrijke entiteiten behoren, naast verschillende soorten privaatrechtelijke organisaties die worden genoemd in bijlage 1 en 2 bij de Cbw, ook overheidsinstanties als ministeries, provincies, gemeenten en waterschappen. De regering verwijst hierbij naar artikel 8, eerste lid, onderdelen g en h, Cbw. Artikel 24, zevende tot en met twaalfde lid, Cbw regelt vervolgens onder meer voor de hiervoor genoemde overheidsinstanties welke functionarissen voor de toepassing van artikel 24 Cbw als leden van het bestuur van een essentiële entiteit of belangrijke entiteit worden aangemerkt. Zo volgt uit artikel 24, twaalfde lid, Cbw dat de hiervoor genoemde verplichtingen ten aanzien van ministeries gelden voor de minister, ten aanzien van provincies gelden voor de gedeputeerde staten, ten aanzien van gemeenten voor het college van burgemeester en wethouders en ten aanzien van waterschappen voor het dagelijks bestuur. Als deze functionarissen de hiervoor bedoelde verplichtingen niet naleven, kan op grond van artikel 92 Cbw daarvoor een last onder dwangsom worden opgelegd en op grond van artikel 93 Cbw een bestuurlijke boete. Voor bestuurders van veiligheidsregio’s geldt het voorgaande daarentegen niet, omdat de veiligheidsregio’s op grond van artikel 5 Cbw zijn uitgezonderd van de toepasselijkheid van de Cbw.

3. *Kan de regering daarnaast toelichten in hoeverre voldoende trainings- en certificeringscapaciteit beschikbaar is om deze bestuurders binnen de gestelde termijn aan deze verplichtingen te laten voldoen? In hoeverre zijn er uitzonderingsmogelijkheden gewaarborgd?*

   De regering ziet dat op dit moment veel partijen, waaronder opleidingsinstituten en adviesbureaus, trainingen aanbieden op het gebied van ICT en informatiebeveiliging. Om te voldoen aan de in artikel 24, tweede lid jo. vijfde lid, Cbw opgenomen trainingsverplichting en verplichting om een certificaat te bezitten waaruit deelname blijkt van die training, kan – in plaats van een training bij een externe partij – ook een interne training worden gevolgd,

[45] Zie J.K. Stam en W.C.T. Weterings, “(On)verzekerbaarheid van boetes”, *AV&S* 2022/33. Zie ook N.M. Brouwer, “De cyberverzekering vanuit civielrechtelijk perspectief”, *Onderneming en recht* nr. 129, Deventer: Wolters Kluwer 2021.

verzorgd door de functionarissen die daartoe de expertise hebben. Op basis van het voorgaande is de regering van mening dat er voor bestuursleden voldoende mogelijkheden zijn om aan de hiervoor genoemde verplichtingen te voldoen.

De Cbw bevat geen uitzonderingsmogelijkheden op de trainingsverplichting.

4. *Hoe beoordeelt de regering de proportionaliteit van het opleggen van persoonlijke sancties aan politieke en publieke ambtsdragers wegens het niet voldoen aan verplichtingen die uit de functie voortvloeien?*

In het algemeen rusten de in de Cbw neergelegde verplichtingen op essentiële of belangrijke entiteiten. De in artikel 24, tweede tot en met vijfde lid, Cbw neergelegde verplichting om te beschikken over kennis en vaardigheden met betrekking tot cyberbeveiliging vormt een uitzondering daarop. Deze verplichting rust namelijk op ieder lid van het bestuur van een essentiële of belangrijke entiteit. Om te voldoen aan deze verplichting dient ieder lid van het bestuur in elk geval te beschikken over een certificaat waaruit blijkt dat diegene een training heeft gevolgd over cyberbeveiliging.

Artikel 31, tweede lid, NIS2-richtlijn verplicht ertoe om effectief toezicht te houden op en de noodzakelijke maatregelen te nemen om te zorgen voor de naleving van de NIS2-richtlijn. De bepalingen over het beschikken over kennis en vaardigheden en het volgen van een training zijn hiervan niet uitgezonderd. Er dient daarom een mogelijkheid te zijn om handhavend op te treden bij het niet nakomen van deze verplichtingen. Om die reden is in artikel 92 en 93 Cbw bepaald dat de bevoegde autoriteit aan een lid van het bestuur van een essentiële of belangrijke entiteit een last onder dwangsom of een bestuurlijke boete kan opleggen indien deze persoon het bepaalde bij of krachtens artikel 24, tweede tot en met zesde lid, Cbw overtreedt. Dat voor het niet nakomen van de genoemde verplichting handhavend kan worden opgetreden jegens een individuele bestuurder, is omdat de verplichting ook op die individuele bestuurder rust.

Voor de proportionaliteit is van belang dat een bestuurder na inwerkingtreding van de Cbw twee jaar de tijd heeft om de training te volgen. Ook een bestuurder die pas na inwerkingtreding van de Cbw wordt benoemd, heeft twee jaar de tijd om de training te volgen. Daar komt bij dat het tijdsbeslag van de training beperkt zal zijn. Verder is van belang dat een last onder dwangsom is gericht op het alsnog nakomen van de verplichting. Indien een bestuurder binnen de in de last bepaalde tijd alsnog de training volgt, is hij de dwangsom dus niet verschuldigd. Voor de bestuurlijke boete is van belang dat de maximale hoogte daarvan € 25.000,– is. Dat is vele malen lager dan het maximale boetebedrag van € 1.000.000,– dat voor veel andere overtredingen geldt. Bij het bepalen van maximum van € 25.000,– is gekeken naar de kosten van trainingen over cyberbeveiliging die nu worden aangeboden, waarbij ook een punitief element is meegenomen. Verder is meegewogen wat een individuele bestuurder zou moeten kunnen dragen.

Hierbij wordt ook opgemerkt dat de in artikel 78 opgenomen bevoegdheid van de bevoegde autoriteit om de burgerlijke rechter te verzoeken om een bestuurslid te schorsen, niet van toepassing is op overheidsinstanties. Dit is geregeld in artikel 79 Cbw.

5. *Herkent de regering het risico dat het opleggen van dergelijke persoonlijke sancties een negatieve invloed kan hebben op de bereidheid om bestuurlijke functies binnen decentrale overheden te vervullen en ertoe kan leiden dat zowel publieke als private bestuursfuncties langdurig vacant blijven?*

Gelet op de grote gevolgen die cyberincidenten kunnen hebben voor de dienstverlening van entiteiten, mag worden aangenomen dat bestuurders cyberbeveiliging heel serieus willen nemen. Zo bezien is het slechts een geringe inspanning om gedurende hooguit enkele dagdelen een training te volgen. Deze verplichting kan een bestuurder gemakkelijk nakomen. In dat licht bezien is er geen aanleiding om aan te nemen dat de mogelijkheid van handhaving van de trainingsverplichting, waaraan kan worden gedaan zonder bovenmatige inspanningen, personen ervan zal weerhouden om een bestuurlijke functie op zich te nemen.

6. *Is de regering van mening dat het persoonlijk sanctioneren van openbare bestuurders een ongewenst precedent kan scheppen?*

De verplichting voor ieder lid van het bestuur van een essentiële of belangrijke entiteit om een training te volgen, volgt uit de NIS2-richtlijn. Hetzelfde geldt voor de bevoegdheid om handhavend op te treden bij het niet nakomen van die verplichting. Voor andere verplichtingen in andere wetgeving zal een eigenstandige afweging moeten worden gemaakt.

7. *Kan de regering nader toelichten hoe artikel 24, lid 3 wordt toegepast op bestuurders die bijvoorbeeld slechts voor één tot twee jaar bestuurder zijn geweest van een essentiële of belangrijke entiteit? Geldt die verplichting ook voor hen en zouden zij in aanmerking kunnen komen voor een persoonlijke sanctie indien zij binnen die periode de benodigde training niet hebben volbracht?*

   De in artikel 24, tweede lid jo. vijfde lid, Cbw opgenomen trainingsverplichting geldt voor elk lid van het bestuur van een essentiële entiteit en belangrijke entiteit. Artikel 24, derde lid, Cbw bepaalt dat bestuursleden aan die verplichting moeten voldoen binnen twee jaar na de inwerkingtreding van de Cbw.[46] Als een bestuurslid wordt benoemd na de inwerkingtreding van de Cbw, dan moet dat bestuurslid de training hebben afgerond binnen twee jaar na de benoeming. Voor bestuursleden die voor een kortere periode dan twee jaar worden benoemd is het aangewezen dat zij zo snel mogelijk de training volgen en afronden, maar als zij dat niet binnen hun benoemingstermijn van korter dan twee jaar doen, kan dat niet worden gesanctioneerd met een bestuurlijke boete.

De invoering van de wet heeft gevolgen voor provincies en gemeenten, in het bijzonder gemeenten die grote infrastructurele projecten beheren zoals havens en luchthavens. Kan de regering aan de leden van de fractie van Volt toelichten welk overleg zij met de mede-overheden hierover gevoerd heeft? Op welke wijze worden de mede-overheden ondersteund? Op welke wijze wordt gewerkt aan gezamenlijke maatregelen ter uitvoering van de richtlijn? Hoe zit dit met grensoverstijgende samenwerking, bijvoorbeeld tussen de havens van Rotterdam en Antwerpen?

Voor de Wwke, waar deze vraag naar verwachting op ziet, geldt dat beheerders van (grote) infrastructurele projecten onder het toepassingsbereik van de Wwke gebracht kunnen worden. In het merendeel van de gevallen zijn dat niet de provincie of gemeente, maar de rechtspersoon die het beheer uitvoert. Dat geldt ook voor alle beheerders van havens en luchthavens waarvan het voornemen is hen aan te wijzen als kritieke entiteit in de zin van de Wwke. Dat een deel van de aandeelhouders in de rechtspersoon die de haven of luchthaven beheert medeoverheid is, betekent niet dat deze medeoverheden daardoor ook een kritieke entiteit in de zin van de Wwke zouden moeten worden. Gemeenten en provincies worden niet rechtstreeks geraakt door de aanwijzing van beheerders van havens en luchthavens. Voor de havens en luchthavens wordt, om die reden, geen overleg met gemeenten en provincies gevoerd.

Overigens zijn er gemeenten die wel rechtstreeks zee- en binnenhavens beheren. Deze gemeenten vallen reeds van rechtswege onder de Cbw, mede vanwege hun verantwoordelijkheden als beheerder van de zee- en binnenhaven, maar voor deze gemeenten bestaat niet het voornemen om hen om die reden aan te wijzen als kritieke entiteit onder de Wwke.
Gemeenten en provincies zijn voorts beheerders van het wegennet. Op basis van een sectorale risicobeoordeling van de Minister van Infrastructuur en Waterstaat voor de subsector weg, die nog niet volledig is afgerond, vindt er reeds overleg plaats met enkele gemeenten en provincies die voorzien zijn als kritieke entiteit voor een klein deel van hun wegennet. Die aanwijzing zou betekenen dat voor een specifiek deel van de wegen door betreffende gemeenten en provincies een risicobeoordeling gemaakt zou moeten worden. Daaruit kan blijken welke maatregelen voor de weerbaarheid nog getroffen moeten worden. In de individuele overleggen komt aanleiding van de voorgenomen aanwijzing als kritieke entiteit, de werking van de Wwke en de behoefte aan ondersteuning aan de orde.

Gelet op het bovenstaande is er slechts zeer beperkt sprake van de gezamenlijke uitvoering door medeoverheden van de CER-richtlijn die in de Wwke wordt omgezet. Er zijn wel initiatieven ontplooid om de samenwerking en gezamenlijke uitvoering van de Cbw door medeoverheden vorm te geven, waaronder de eerste stappen richting de ontwikkeling van een cybersecuritystandaard voor operationele technologie. De gezamenlijke uitvoering van de Cbw wordt ook bevorderd door de CSIRT's. Hiervoor wordt verwezen naar artikel 16, vijfde en zesde lid, Cbw. Deze samenwerking kan onder meer vorm krijgen in een *Information Sharing and Analysis Center* (hierna: ISAC). Een ISAC biedt deelnemers toegang tot waardevolle informatie over cyberdreigingen die specifiek zijn voor de eigen sector. Het delen van dreigingsinformatie helpt organisaties om sneller te reageren op

[46] De voorschriften in artikel 24, derde lid, Cbw zijn verbonden aan de inwerkingtreding van artikel 24, tweede lid, Cbw. Voor de leesbaarheid van deze passage wordt gesproken over de inwerkingtreding van de Cbw, ook omdat de regering niet voornemens is om te voorzien in gefaseerde inwerkingtreding van de Cbw.

incidenten en proactieve maatregelen te nemen. Daarnaast kunnen deelnemende organisaties van elkaar leren. Voor de Rotterdamse haven is een dergelijke ISAC opgezet. Dit geldt ook voor het Noordzeekanaalgebied.

Voor de grensoverstijgende samenwerking tussen havens ligt het initiatief in eerste instantie bij de havenbedrijven zelf. De havens van Antwerpen-Brugge en Rotterdam werken samen op thema's waar gezamenlijke inzet duidelijke meerwaarde heeft, terwijl zij op commerciële dossiers blijven concurreren. De samenwerking past binnen het Europees mededingingsrecht en is gericht op het versterken van de havens en de Europese industrie. Op het terrein van weerbaarheid werken beide havens samen om hun kritieke functies beter te beschermen tegen geopolitieke, criminele, fysieke en digitale dreigingen. Deze samenwerking sluit aan bij de nieuwe Europese en nationale weerbaarheidsverplichtingen. Voor de havens betekent dit dat samenwerking steeds belangrijker wordt voor de continuïteit van essentiële diensten. Denk aan gezamenlijke risicoanalyses, crisis- en continuïteitsplanning, uitwisseling van dreigingsinformatie, gezamenlijke oefeningen, versterking van digitale havensystemen en afstemming rond Host Nation Support en kritieke logistieke corridors.

6. Kostenaspect

Kan de regering aan de leden van de fractie van de VVD uiteenzetten wat de geactualiseerde raming van de structurele lasten voor bedrijfsleven is en overheid en welke compensatie is voorzien voor gemeenten?

De kosten voor de overheid worden geraamd op een structureel bedrag oplopend tot circa € 83 miljoen. De budgettaire gevolgen per departement, zoals weergegeven in de memorie van toelichting op het wetsvoorstel, zijn in de onderstaande tabel uitgesplitst.[47]

(in mln. €)	2024	2025	2026	2027	2028	Structureel
Economische Zaken en Klimaat	7,30					
Economische Zaken		9,30	12,33	12,39	12,91	12,91
Klimaat en Groene Groei		7,02	9,84	9,78	9,26	9,26
Infrastructuur en Waterstaat	0,00	11,90	13,40	15,00	16,50	18,00
Volksgezondheid, Welzijn en Sport	5,07	8,11	8,11	8,04	8,04	8,04
Binnenlandse Zaken en Koninkrijksrelaties	2,54	7,06	7,26	7,46	7,56	7,56
Onderwijs, Cultuur en Wetenschap	2,14	2,3	4,09	4,09	4,09	3,59
Landbouw, Visserij, Voedselzekerheid en Natuur	0,70	5,10	5,80	6,80	6,80	6,80
Justitie en Veiligheid	3,64	6,37	9,00	10,68	13,92	15,17
Financiën	0,00	1,20	1,30	1,40	1,50	1,50
Totaal	**21,39**	**58,36**	**71,13**	**75,64**	**80,58**	**82,83**

Naargelang de implementatie van de Cbw vordert kan een meer betrouwbare raming worden gemaakt en kan bijstelling nodig blijken te zijn.

Ten aanzien van het bedrijfsleven zijn de eenmalige kosten primair het gevolg van de voorbereidingen die bedrijven moeten treffen om de maatregelen in het kader van de zorgplicht uit te voeren, en de eenmalige meerkosten voor 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 bedrijven 614 uur aan eenmalige extra tijdsbesteding per bedrijf nodig te hebben voor de voorbereiding en implementatie van de te nemen maatregelen ten aanzien van de zorgplicht. Voor grote bedrijven ligt dit getal aanzienlijk hoger, namelijk op gemiddeld 6.708 uur aan eenmalige extra tijdsbesteding per bedrijf. Naast tijdbesteding zullen bedrijven ook out-of-pocket-investeringen moeten doen. Middelgrote bedrijven verwachten gemiddeld lagere kosten te moeten maken dan grote bedrijven: € 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. De structurele

[47] In 2026 is Klimaat en Groene Groei onderdeel geworden van het Ministerie van Economische Zaken en Klimaat, maar voor de overzichtelijkheid van deze tabel zijn Economische Zaken en Klimaat en Groene Groei nog gescheiden gehouden.

meerkosten voor bedrijven volgen dan ook primair uit verplichtingen uit de Cbw die meer diepgang of een bredere 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. 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 om te voldoen aan de zorgplicht. Bij grote bedrijven 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 bedrijven liggen niet ver uit elkaar, deze bedragen gemiddeld € 30.000,– respectievelijk € 32.800,– per jaar.

Er is geen sprake van algemene (financiële) compensatie van medeoverheden voor de implementatie van de Cbw. Dit geldt tevens voor alle bedrijven en organisaties die onder deze wet komen te vallen. Dat is bijvoorbeeld destijds ook niet gebeurd bij onder meer de Algemene verordening gegevensbescherming.

De Cbw bevat voor essentiële entiteiten en belangrijke entiteiten – kort gezegd – de verplichting om passende en evenredige 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 gebruikt, te beheersen. Het verschilt per (decentrale) overheidsinstantie welke passende en evenredige maatregelen genomen moeten worden. De ene organisatie zal vanwege zijn aard meer en/of andere maatregelen moeten treffen dan een andere organisatie. Afhankelijk van het te beschermen belang en de dreiging wordt een risicoafweging gemaakt door de entiteit welke maatregelen noodzakelijk zijn. De gevolgen kunnen dus sterk verschillen tussen organisaties. Overigens geldt voor overheidsorganisaties dat zij reeds op grond van verschillende bestaande wet- en regelgeving in bepaalde mate gebonden zijn aan het nemen van maatregelen ten behoeve van informatiebeveiliging. Zo moeten op grond van de Algemene verordening gegevensbescherming risico’s met betrekking tot de verwerking van persoonsgegevens in kaart worden gebracht en maatregelen worden genomen om onderkende risico’s te mitigeren. De mate waarin reeds wordt voldaan aan deze bestaande informatiebeveiligingseisen kan ook verschillen tussen overheidsorganisaties.

Om de gevolgen van deze wetgeving voor medeoverheden te beperken, is bij de nadere uitwerking van de zorgplicht en de meldplicht in de ministeriële regelingen voor entiteiten uit de sector overheid zoveel mogelijk aangesloten bij reeds voor hen geldende verplichtingen en kaders. Dit blijkt tevens uit de uitwerking van de impact voor overheidsinstanties, bijvoorbeeld bij gemeenten. Daarin komt naar voren dat een groot deel van de kosten zijn oorsprong kent in het voldoen aan bestaande wet- en regelgeving.

Buiten deze verplichtingen die dus zoveel mogelijk aansluiten bij bestaande instrumenten of verplichtingen, kent de Cbw voor medeoverheden slechts beperkt aanvullende verplichtingen. Voor medeoverheden zal de trainingsverplichting voor bestuurders, bedoeld in artikel 24, tweede en vijfde lid, Cbw geheel nieuw zijn. Hiervoor geldt dat de invulling van deze verplichting samen met de overheidsorganisaties wordt uitgewerkt. Het doel is om te komen tot een opleiding die overheidsorganisaties zelf kunnen geven, zodat zij niet afhankelijk zijn van het inkopen van deze training bij marktpartijen. De meldplicht is als expliciete verplichting nieuw. Tegelijkertijd zijn overheidsorganisaties al wel gewend om meldingen van incidenten te doen bij partijen als het NCSC, de Informatiebeveiligingsdienst (IBD) en de Autoriteit persoonsgegevens. Daardoor zijn er veelal al processen ingericht om de meldingen te doen en op te volgen.

Van belang is ook dat uit de Uitvoeringsanalyse Digital Decade Regelgeving beveiliging netwerk- en informatiesystemen volgt dat er twee factoren in het bijzonder van invloed zijn op de uitvoeringscapaciteiten: structurele tekorten bij gemeenten en de krapte op de arbeidsmarkt voor specialistische kennis. Een generieke compensatie draagt niet bij aan het oplossen van deze bredere vraagstukken, ook omdat in het volledige cybersecuritydomein de beschikbare kennis en expertise schaars is. In plaats van een generieke compensatie zet de regering daarom in op het versterken van onderlinge samenwerking en het gebruik van elkaars beschikbare kennis en expertise. Ondersteuning vanuit de Rijksoverheid gebeurt om die reden bij voorkeur via centrale ondersteuningsproducten, waar individuele overheidsorganisaties gebruik van kunnen maken ten behoeve van hun eigen organisaties.

Een voorbeeld van het voorgaande is het lopende ondersteuningsprogramma van de BIO2 waar organisaties gebruik kunnen maken van een veelheid aan kennisproducten, informatiesessies en tools. Met deze producten wordt bijgedragen aan de opbouw van expertise en de consequente en

consistente uitvoering van de maatregelen uit de BIO2 en breder op het terrein van informatiebeveiliging. Daarnaast is recent gestart met een initiatief van de Informatiebeveiligingsdienst (IBD), waarbij een centrale groep van experts gemeenten helpt met het goed opzetten van een managementsysteem voor informatiebeveiliging. Daarmee wordt bijgedragen aan een gemeenschappelijk hoog niveau van informatiebeveiliging. Dit initiatief wordt als pilot bekostigd door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Afhankelijk van de bevindingen uit deze pilot kan worden bezien of het wenselijk is dit uit te breiden voor meer overheidsorganisaties. Gezamenlijk met de bestuurslagen wordt voortdurend de behoefte aan ondersteuning van medeoverheden op het gebied van informatiebeveiliging verkend, ontwikkeld en bijgesteld, zodat zij in staat zijn een zo hoog mogelijk niveau van informatiebeveiliging te waarborgen.

Op welke wijze wordt voorkomen dat decentrale overheden – die geen keuze hebben om niet onder de wet te vallen – worden geconfronteerd met onevenredige lasten?

Er is bij het opstellen van deze wet- en regelgeving nadrukkelijk oog geweest voor de administratieve last en de regeldruk die organisaties zullen ervaren als gevolg daarvan. Er is gekozen voor een risicogebaseerde aanpak, zodat essentiële entiteiten en belangrijke entiteiten in de zin van de Cbw ruimte hebben om risicogebaseerd een eigen invulling te geven aan de verplichte maatregelen. Deze risicogebaseerde aanpak biedt ruimte om gezien de context van de organisatie tot de meest (kosten) effectieve oplossing te komen.

In aanvulling daarop is, om de lasten voor medeoverheden te beperken, ervoor gekozen om in de ministeriële regelingen onder de Cbw die voor entiteiten uit de sector overheid zullen gelden, zoveel mogelijk aan te sluiten bij reeds voor hen geldende verplichtingen en kaders. Zo wordt voor de nadere invulling van de zorgplicht, bedoeld in artikel 21 Cbw, bepaald dat entiteiten, in aanvulling op de maatregelen zoals beschreven in het Cbb, meer specifiek moeten voldoen aan de BIO2. Dat is het bestaande normenkader voor informatiebeveiliging waaraan alle overheidslagen zich hebben gecommitteerd.[48] De totstandkoming van de BIO2 heeft bovendien plaatsgevonden onder coördinatie van Ministerie van Binnenlandse Zaken en Koninkrijksrelaties in samenwerking met alle bestuurslagen.

Ook voor het bepalen van de drempelwaarden in het kader van de meldplicht is zoveel mogelijk aangesloten bij bestaande uitgangspunten. Hiervoor worden criteria gebruikt op basis waarvan gemeenten reeds hun incidentmeldingen doen bij de Informatiebeveiligingsdienst (IBD). Ook waterschappen zijn, via de Unie van Waterschappen, actief betrokken (geweest) bij het wetgevingsproces. Met name bij de lagere regelgeving, zoals de Cybersecurityregeling IenW, waar uitvoerig is gesproken over de uitvoerbaarheid van de drempelwaarden in het kader van de meldplicht uit de Cbw.

Voor de registratieplicht, bedoeld in artikel 44 Cbw, geldt dat een deel van de gegevens die entiteiten op grond van dat artikel moeten aanleveren, reeds beschikbaar zijn of al op grond van andere verplichtingen worden aangeleverd. Hierbij kan worden gedacht aan domeinnamen die in het kader van digi-toegankelijkheid reeds zijn geregistreerd in het Dashboard DigiToegankelijkheid en algemene gegevens uit het Register van Overheidsorganisaties (ROO). Daarnaast zal voor toezicht en verantwoording zoveel mogelijk gebruik worden gemaakt van bestaande verantwoording van medeoverheden, zoals de Eenduidige Normatiek Single Information Audit (ENSIA) die door gemeenten wordt gebruikt.

Buiten deze verplichtingen die op grond van bestaande instrumenten zijn ingevuld, of reeds volgden uit bestaande verplichtingen, kent de Cbw voor medeoverheden slechts beperkt aanvullende verplichtingen. Voor medeoverheden zal de trainingsverplichting voor bestuurders, bedoeld in artikel 24, tweede en vijfde lid, Cbw geheel nieuw zijn. Hiervoor geldt dat de invulling van deze verplichting samen met de overheidsorganisaties wordt uitgewerkt. Het doel is om te komen tot een opleiding die overheidsorganisaties zelf kunnen geven, zodat zij niet afhankelijk zijn van het inkopen van deze training bij marktpartijen. De meldplicht is als expliciete verplichting nieuw. Tegelijkertijd zijn overheidsorganisaties al wel gewend om meldingen te doen bij partijen als het NCSC, de Informatiebeveiligingsdienst (IBD) en de Autoriteit persoonsgegevens. Daardoor zijn er veelal al processen ingericht om de meldingen te doen en op te volgen.

Over knelpunten die mogelijk ontstaan ondanks deze initiatieven, wordt op reguliere basis met de medeoverheden gesproken. Dat gebeurt onder meer via de werkgroepen voor de Baseline Informatiebeveiliging Overheid. Ook worden overheidsorganisaties op frequente basis door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, het NCSC en de NCTV geïnformeerd over de komst van de Cbw. Bovendien hebben zij onder meer via het Centrum voor Informatiebeveiliging

[48] *Stcrt*. 2020, 7857.

en Privacy (CIP) en de websites bio-overheid.nl en digitaleoverheid.nl ondersteunende producten en tools tot hun beschikking. Bovendien is in samenwerking met de Vereniging Nederlandse Gemeenten gestart met regioaanjagers bij gemeenten om hen te helpen met het implementeren van maatregelen voor hun informatiebeveiliging.

Kan de regering aan de leden van de fractie van FVD toelichten hoe wordt geborgd dat de nieuwe verplichtingen voor kritieke entiteiten niet leiden tot onevenredige administratieve lasten en kostenstijgingen voor essentiële sectoren zoals zorg, energie en drinkwatervoorziening? Kan de regering concreet onderbouwen dat de proportionaliteit van de maatregelen systematisch is getoetst? Zo ja, op basis van welke criteria?

De regering gaat er van uit dat deze vraag ziet op de Wwke, vanwege de vermelding van kritieke entiteiten in de vraagstelling.

Er is bij het opstellen van deze wet- en regelgeving nadrukkelijk oog geweest voor de administratieve last en de regeldruk die bedrijven zullen ervaren als gevolg daarvan. Er is gekozen voor een risicogebaseerde aanpak, zodat kritieke entiteiten in de zin van de Wwke ruimte hebben om risicogebaseerd een eigen invulling te geven aan de verplichte maatregelen. Deze risicogebaseerde aanpak biedt ruimte om gezien de context van de organisatie tot de meest (kosten)effectieve oplossing te komen en geeft de mogelijkheid om bijvoorbeeld verschillende wettelijke verplichtingen te combineren. Zo kan ervoor gekozen worden om een integrale risicobeoordeling uit te voeren voor de Wwke en de Cbw. Dit kan voor bedrijven een vermindering in de administratieve lasten betekenen en bij hen onnodige regeldruk voorkomen. Bij het opstellen van de verplichtingen in de Wwke heeft de regering los van de regeldruktoets geen aparte systematische toets op de proportionaliteit van de maatregelen uitgevoerd.

De proportionaliteit volgt echter in zichzelf uit het feit dat kritieke entiteiten op grond van artikel 15 Wwke passende en evenredige maatregelen dienen te treffen om voor hun weerbaarheid te zorgen. De maatregelen die kritieke entiteiten op grond van de Wwke moeten nemen, moeten passend en evenredig zijn in relatie tot de risico’s die zij hebben vastgesteld op basis van de eigen risicobeoordeling en tegen het licht van de door de vakminister uitgevoerde risicobeoordeling. Bij de beoordeling of een maatregel of een combinatie van maatregelen passend is, wordt allereerst gekeken naar de effectiviteit. De maatregelen moeten één of meer van de volgende effecten bewerkstelligen: een incident voorkomen en als een incident zich toch voordoet, de gevolgen beperken door het incident te beheersen, zich aan te passen aan een incident of daarvan zo spoedig mogelijk te herstellen. In artikel 1 Wwke is een incident gedefinieerd als elke gebeurtenis die het verlenen van een essentiële dienst aanzienlijk verstoort of kan verstoren. De maatregelen moeten zijn afgestemd op de risico’s in relatie tot de entiteit en de specifieke context. Een passende maatregel kan dus per entiteit verschillen, onder meer door de specifieke kenmerken van de entiteit, de aard van de dienstverlening en de sector waarin de entiteit de dienst verleent. Daarnaast geldt het vereiste van evenredigheid. Dit betekent dat een maatregel of coherente set van maatregelen in verhouding dient te staan tot het te beheersen risico en dat de entiteit kan kiezen voor de maatregelen die het minst belastend zijn voor de entiteit om het risico te beheersen. Als gevolg van de afweging of een maatregel passend en evenredig is, is er een bepaald niveau van risico dat aanvaardbaar is. Het volledig uitsluiten van risico’s en het creëren van volledige bescherming is niet mogelijk. Kritieke entiteiten worden daarom geacht maatregelen te nemen om risico’s te beheersen en de mogelijke gevolgen van restrisico’s zoveel mogelijk tot een minimum te beperken. Het is in eerste instantie aan kritieke entiteiten zelf om vast te stellen welke maatregelen passend en evenredig zijn om de risico’s, waarmee zij geconfronteerd worden, te kunnen beheersen. Entiteiten hebben immers zelf – mede op basis van onder meer de door de vakminister uitgevoerde risicobeoordeling en de eigen risicobeoordeling – inzicht in risico’s die hun dienstverlening kunnen raken en hebben de meeste kennis van hun eigen systemen en processen. Hoe risicogebaseerd maatregelen te treffen kan onder andere worden afgeleid uit wat daarover beschreven staat in Europese en internationale standaarden of normen, evenals door gebruik te maken van de laatste stand van de techniek voor het treffen van technische maatregelen. Europese en internationale standaarden en normen kunnen een goede indicatie geven van hoe technische en organisatorische veiligheids- en beveiligingsmaatregelen te treffen.

Tot slot worden alleen de bedrijven en organisaties als kritieke entiteit in de zin van de Wwke aangewezen die een dergelijke cruciale rol in de continuïteit van de Nederlandse samenleving spelen, dat de regering de ervaren regeldruk en administratieve lasten als proportioneel beschouwt, gezien de gevolgen die incidenten bij deze bedrijven en organisaties kunnen hebben voor Nederland.

De Minister van Justitie en Veiligheid,