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) 2022/2557 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) (Wet weerbaarheid kritieke entiteiten, *Kamerstukken* 36765) 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 en de Europese Commissie inmiddels heeft besloten om bij het Europese Hof van Justitie een Hofprocedure te starten tegen Nederland wegens het te laat omzetten van deze richtlijn in nationale wetgeving.

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 Wet weerbaarheid kritieke entiteiten (hierna: Wwke). Dit wetsvoorstel strekt tot de uitvoering van de 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 (hierna: CER-richtlijn).[1] Ik dank de leden van de fracties voor de gestelde vragen, die ik in deze nota beantwoord. Ook dank ik de commissies voor het binnen een korte periode uitbrengen van het verslag, mede in het licht van het recentelijke besluit van de Europese Commissie om bij het Europese Hof van Justitie een Hofprocedure te starten tegen Nederland vanwege het te laat omzetten van de CER-richtlijn in nationale wetgeving.

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.

Het wetsvoorstel heeft de leden de fractie van GroenLinks-PvdA, mede namens de leden van de fractie van PvdD, en de leden van de fracties van de BBB, VVD, D66, CDA, PVV en FVD aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de CDA-fractie hebben met belangstelling kennisgenomen van de Wet weerbaarheid kritieke entiteiten. Deze leden onderschrijven het belang van het verhogen van de fysieke weerbaarheid van 'kritieke entiteiten', maar hebben nog enkele vragen.

Deze leden constateren dat voor de CER-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 CER-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, om ervoor te zorgen dat implementatie zo spoedig mogelijk kan plaatsvinden. Bij het implementatieproces van de CER-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 CER-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 CER-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 CER-richtlijn wordt geïmplementeerd, grote impact heeft op de 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. Deze Nederlandse bedrijven en organisaties zullen met de komst van de Wwke onder meer diverse verplichtingen opgelegd krijgen, waar op de naleving toezicht plaatsvindt. Vanwege de hiervoor benoemde grote impact op Nederlandse bedrijven en organisaties, is de totstandkoming

[1] *PbEU* 2022, L 333.

van het wetsvoorstel voor de Wwke, 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.

Het voorgaande maakt dan ook dat de implementatietermijn van nog geen twee jaar voor de CER-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 23 andere lidstaten van de Europese Unie de CER-richtlijn niet tijd 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.

De leden van de D66-fractie hebben met belangstelling kennisgenomen van het voorstel voor de Wet weerbaarheid kritieke entiteiten. 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 Wet weernaarheid kritieke entiteiten 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[2] 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 Cyberbeveiligingswet, hierna: 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

[2] 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).

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 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.

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

   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 Rijksinspectie Digitale Infrastructuur (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.[3] 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 Wwke 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 Wwke door kritieke entiteiten en houden daarbij rekening met de specifieke eigenschappen van een sector. Zij werken allemaal vanuit hetzelfde wettelijk kader, namelijk de Wwke 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.

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

3. *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 bij hen een incident zich

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

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 Nationaal Cyber Security Centrum (NCSC) voor meldingen onder beide wetten. Het uitgangspunt is dat het meldportaal op een lastenluwe manier wordt ingericht.

4. *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 kritieke 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.[4]

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

5. *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 (hierna: Wet vifo) kunnen verwervingsactiviteiten ten aanzien van onder meer vitale aanbieders (als doelonderneming) die binnen het toepassingsbereik vallen (conform artikel 7 Wet vifo) 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, in overeenstemming met de Minister van Justitie en Veiligheid, en – indien

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

van toepassing – de vakminister die het onderwerp betreft. Hierbij wordt opgemerkt dat kritieke entiteiten onder de Wwke niet automatisch onder de Wet vifo vallen.

Daarnaast bestaat er sectorspecifieke wetgeving om ongewenste zeggenschap in de telecommunicatiesector en de energiesector te voorkomen. De Wet ongewenste zeggenschap telecommunicatie en de specifieke investeringstoets uit de Energiewet zijn wettelijke mechanismen die de Nederlandse overheid inzet om de nationale veiligheid en leveringszekerheid te beschermen.

Verder wordt gewezen op de recent door het Europees Parlement goedgekeurde herziene FDI-screeningsverordening.[5] 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 vifo.

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

Bij het aanbesteden van kritieke (digitale) diensten die invloed kunnen hebben op de nationale veiligheid spelen geopolitieke criteria een rol in de eisen en wettelijke mogelijkheden van een aanbestedende dienst. Zodra er een vermoeden bestaat van risico's voor de nationale veiligheid, moet een aanbestedende dienst de Toolbox veilig inkopen gebruiken om risico's te signaleren en te bepalen of er maatregelen nodig zijn. Een quickscan over de aanbesteding is hier onderdeel van. De quickscan helpt aanbestedende diensten bij het signaleren van veiligheidsrisico's in aanbestedingen of bij een inkoopopdracht. Hierbij wordt onder andere beoordeeld of er toegang is tot informatie die de Nederlandse belangen schaadt. Indien de quickscan duidt op mogelijke risico's, volgt een uitgebreide risicoanalyse. De aanbestedende dienst is verantwoordelijk voor het beoordelen of bij een opdracht mogelijk sprake is van een nationaal veiligheidsbelang en welke wet van toepassing is: de Aanbestedingswet 2012 of de Aanbestedingswet op defensie- en veiligheidsgebied. De Aanbestedingswet 2012 verplicht aanbestedende diensten om alle bedrijven uit de Europese Unie en uit landen waarmee de Europese Unie een handelsovereenkomst heeft, op het gebied van aanbesteden (zowel multilateraal als bilateraal) gelijke toegang te geven. Bij inschrijvingen van bedrijven uit andere landen kan een aanbestedende dienst ervoor kiezen deze inschrijving terzijde te leggen. Uit recente uitspraken van het Hof van Justitie van de Europese Unie volgt dat deze keuze enkel bij de aanbestedende dienst ligt en nationaal beleid hierover niet is toegestaan.[6] Bij het gebruik van de Aanbestedingswet op defensie- en veiligheidsgebied kan een aanbestedende dienst bij alle inschrijvingen van bedrijven buiten de Europese Unie ervoor kiezen om deze terzijde te leggen. Daarnaast kunnen in de contractuele voorwaarden aanvullende eisen aan de toeleveringsketen worden opgelegd.

Vanaf 1 januari 2026 gelden er bovendien nieuwe beveiligingseisen voor bedrijven die voor departementen, hun agentschappen en diensten, en de politie 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. Het Nationaal Bureau Industrieveiligheid (NBIV) controleert of een bedrijf aan de gestelde eisen voldoet voordat het een bijzondere opdracht mag uitvoeren.

Op grond van het Kaderbesluit ABRO Rijksdienst geldt onder meer het voorschrift dat de ministers zorgdragen dat bij de voorbereiding van een

[5] 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.
[6] HvJ EU 13 maart 2025, ECLI:EU:C:2025:178 en HvJ EU 22 oktober 2024, ECLI:EU:C:2024:910.

inkoopopdracht een quickscan wordt verricht, indien het vermoeden bestaat dat sprake kan zijn van risico's voor de nationale veiligheid.

7. *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.[7] Dit hulpmiddel ondersteunt kritieke entiteiten bij het bepalen van klimaatrisico's voor hun organisatie.

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

In het Dreigingslandschap Vitale Infrastructuur uit 2025[8] concludeert de NCTV dat klimaatverandering versnelt en ernstiger wordt dan eerder werd gedacht. 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.

9. *Welke concrete criteria worden gebruikt bij de aanwijzing van kritieke entiteiten onder de Wwke?*

Een entiteit wordt door de vakminister aangewezen als kritieke entiteit in de zin van de Wwke als:

- zij één of meer essentiële diensten verleent (een essentiële dienst is een dienst die van cruciaal belang is voor de instandhouding van vitale maatschappelijke functies, economische activiteiten, de volksgezondheid en openbare veiligheid of het milieu);
- zij actief is op het grondgebied van Nederland;
- haar kritieke infrastructuur zich bevindt op het grondgebied van Nederland; en
- een incident aanzienlijke verstorende effecten zou hebben op haar verlening van één of meer essentiële diensten, of aanzienlijke verstorende effecten zou hebben op haar verlening van andere essentiële diensten in de sectoren uit de bijlage van de Wwke of de sectoren die zijn aangewezen op grond van artikel 7, eerste lid, Wwke die afhankelijk zijn van die diensten.

[7] Deze handreiking is te raadplegen op https://www.rijksoverheid.nl/documenten/2025/10/15/handreiking-klimaatbestendige-vitale-infrastructuur-voor-het-bepalen-van-klimaatrisico-s.
[8] Het Dreigingslandschap Vitale Infrastructuur (2025) is te raadplegen op https://www.nctv.nl/documenten/2025/07/23/dreigingslandschap-vitale-infrastructuur.

Deze criteria zijn opgenomen in artikel 6, eerste lid, Wwke. Alleen de entiteiten die voldoen aan al deze criteria zullen worden aangewezen als kritieke entiteit.

10. *Hoe transparant wordt het aanwijzingsproces voor organisaties die mogelijk als kritieke entiteit worden aangewezen?*

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

11. *Hoe effectief is bezwaar en beroep mogelijk wanneer aanwijzingen gebaseerd zijn op vertrouwelijke risicoanalyses?*

De motivering van het besluit waarmee een entiteit op grond van artikel 6 Wwke wordt aangewezen als kritieke entiteit in de zin van de Wwke is onder meer gebaseerd op de risicobeoordeling van de vakminister. Die risicobeoordeling kan elementen bevatten die vertrouwelijk zijn en dus niet integraal gedeeld kunnen worden met de betrokken entiteit. Niettemin wordt de voor de betrokken entiteit relevante informatie uit die risicobeoordeling op grond van artikel 9, zesde lid, Wwke op passende wijze gedeeld met die entiteit. Met onder meer die informatie kan de entiteit de afweging van de vakminister volgen en betrekken bij de onderbouwing van haar bezwaar en beroep.

Kan de regering aan de leden van de fractie van de BBB aangeven of oorlogsvoering een risico is waartegen kritieke entiteiten zich onder deze wet ook moeten voorbereiden, of valt oorlogsvoering buiten deze wet? Is dit inclusief nucleaire oorlogsvoering en hierbij horende elektromagnetische pulsen? Valt 'cyber war' hier ook onder?

De verantwoordelijke vakminister voert op grond van artikel 9 Wwke een risicobeoordeling uit voor de sectoren waarvoor zij beleidsverantwoordelijk zijn. Hierbij worden alle relevante natuurlijke en door de mens veroorzaakte risico's die tot een incident zouden kunnen leiden in aanmerking genomen. De risicobeoordeling onder de Wwke is daarmee *all hazard* ingericht. Dat betekent dat alle potentiële relevante dreigingen, kwetsbaarheden en gevaren die tot een incident kunnen leiden in kaart gebracht en geanalyseerd worden. Het gaat daarbij expliciet ook om hybride en militaire dreigingen, zoals activering van artikel 5 uit het verdrag van de NAVO. In een dergelijke risicobeoordeling zit altijd een weging van de kans dat een scenario zich voordoet en de potentiële impact die het kan hebben.

Deze sectorale risicobeoordeling van de vakminister vormt vervolgens de basis voor de risicobeoordeling die de kritieke entiteit voor de eigen organisatie moet uitvoeren. De kritieke entiteit hanteert ook hierbij een *all hazard*-benadering. De kritieke entiteit neemt naar aanleiding van de in kaart gebrachte risico's passende en evenredige maatregelen in het kader van de zorgplicht.

Kan de regering aan deze leden toelichten of deze wet alleen bedoeld is voor betere beveiliging door kritieke entiteiten waarvandaan grote maatschappelijke schade kan ontstaan of is deze wet ook bedoeld voor private of publieke organisaties die juist als taak hebben om schade te beperken, dus om incidenten te bestrijden?

De wet ziet op het verhogen van de weerbaarheid en de continuïteit van essentiële diensten, die door kritieke entiteiten geleverd worden. De essentiële diensten worden in kaart gebracht door de bevoegde autoriteit. In artikel 6, eerste lid, Wwke zijn de criteria opgenomen op basis waarvan de vakminister beoordeelt of een entiteit kwalificeert als kritieke entiteit, waaronder het criterium dat een incident bij die entiteit aanzienlijke verstorende effecten zou hebben. Op basis van deze criteria zouden ook private of publieke organisaties aangewezen kunnen worden die als taak hebben om schade te beperken of incidenten te bestrijden. Daarbij moet wel in acht genomen worden dat in artikel 5, Wwke, is bepaald dat overheidsinstanties die in hoofdzaak activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving uitgezonderd zijn. Hieronder vallen ook de politie en veiligheidsregio's.

De leden van de D66-fractie merken op dat de minister van J&V een coördinerende rol heeft. De regering heeft aangegeven dat de vakminister 'in overeenstemming met' de minister van J&V nadere regels of besluiten voor sectoren kan vaststellen, in de gevallen dat de handelingen van de betrokken minister het integrale stelsel raken. Wanneer is dat het geval? In de andere gevallen behoeft de vakminister alleen te overleggen met de minister van J&V. Doet dat geen afbreuk aan het vermogen van deze minister om coördinerend op te treden? Heeft de regering zicht op hoe andere lidstaten invulling geven aan de coördinerende rol van de minister van J&V, specifiek ten aanzien van de vraag of in andere lidstaten de coördinerende minister wel in alle gevallen samen met de vakminister tot besluiten komt? Hoe kan worden gegarandeerd dat in dergelijke gevallen alle, voor de uitvoering van deze wet verantwoordelijke, vakministers de wetgeving op dezelfde manier interpreteren en daarmee de ene minister de ene sector niet strengere maatregelen oplegt dan de andere minister dat bij een andere sector doet?

De Wwke en het Besluit weerbaarheid kritieke entiteiten (hierna: Bwke), dat is de algemene maatregel van bestuur onder de Wwke, 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 vitale infrastructuur. De vakminister draagt de verantwoordelijkheid voor de eigen sector, en de sectoroverstijgende, coördinerende verantwoordelijkheid valt onder bevoegdheid van de Minister van Justitie en Veiligheid.

De betrokkenheid van de Minister van Justitie en Veiligheid komt in de Wwke en het Bwke 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 Wwke en het Bwke waarbij regelingen of besluiten van de vakminister het integrale stelsel van kritieke infrastructuur 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, intersectorale afhankelijkheden en effecten en de bredere impact op de nationale veiligheid. Van een besluit van de vakminister dat het integrale stelsel van kritieke infrastructuur raakt, is onder meer het geval bij gebruikmaking van de bevoegdheid uit artikel 15a Wwke. Op grond van dit artikel kan een vakminister een kritieke entiteit de verplichting opleggen om een dienst of product van een specifieke leverancier te weren uit onderdelen van haar kritieke infrastructuur. Deze verplichting kan worden opgelegd om incidenten bij een kritieke entiteit, die de nationale veiligheid raken, te voorkomen, te beperken of te beheersen. 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 artikel 24 Wwke, op grond waarvan een vakminister een kritieke entiteit kan ontheffen van onder meer de zorgplicht en de meldplicht. Daarbij gaat het in artikel 24, eerste lid, Wwke 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 Wwke en het Bwke waarbij de handelingen van de vakminister het integrale stelsel van kritieke infrastructuur 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 6 Wwke, op basis waarvan een vakminister een entiteit aanwijst als kritieke entiteit. Ook bij het aanwijzen van een sector, subsector of categorie van entiteiten (artikel 7 Wwke), het opstellen van de risicobeoordeling door de bevoegde autoriteit (artikel 9 Wwke) en het bieden van ondersteuning aan kritieke entiteiten (artikel 10 Wwke) prevaleren sectorale inzichten van de vakminister, maar wordt er wel overleg gepleegd met de Minister van Justitie en Veiligheid om de sectoroverstijgende aspecten en de toets op de nationale veiligheid te borgen. 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 Wwke en het Bwke waarbij de handelingen van de vakminister het integrale stelsel van kritieke infrastructuur 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.

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 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 15, eerste lid, Wwke, uitgewerkt in het Bwke en nader uitgewerkt in de onderliggende ministeriële regelingen van de vakministers.

   De zorgplicht is één van de hoofdelementen van de Wwke 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 Bwke. Deze voorhangprocedure is geregeld in artikel 47b Wwke.

   De uitwerking van de zorgplicht in het Bwke 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 categorieën van 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 kritieke entiteiten in het kader van de zorgplicht in ieder geval moeten voldoen staan in artikel 15 Wwke. 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 Bwke 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 risicobeoordeling die elke kritieke entiteit afzonderlijk zal uitvoeren. Dit betekent dat een kritieke entiteit niet voorafgaand, maar na het uitvoeren van de risicobeoordeling kan vaststellen welke specifieke invulling van de maatregelen voor haar passend en evenredig is. De uitkomsten van de risicobeoordeling en daarmee de invulling van de te nemen maatregelen zullen daarom per kritieke entiteit verschillen.

Het is vervolgens aan de toezichthouder om te beoordelen of de kritieke entiteit voldoende invulling heeft gegeven aan de zorgplichtmaatregelen en de toezichthouder zal daarbij risicogebaseerd te werk gaan, juist omdat de uitkomsten van de risicobeoordeling en daarmee de invulling van de genomen maatregelen per kritieke entiteit zullen verschillen. De maatregelen die zijn omschreven in artikel 15 Wwke, de uitwerking daarvan in het Bwke 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 15, eerste lid, Wwke is bepaald dat kritieke entiteiten passende en evenredige technische, beveiligings- en organisatorische maatregelen moeten nemen om voor hun weerbaarheid te zorgen, met inbegrip van maatregelen die nodig zijn om:
a. te voorkomen dat zich incidenten voordoen, naar behoren rekening houdend met
maatregelen ter beperking van het risico op rampen en maatregelen voor aanpassing aan de klimaatverandering;
b. te zorgen voor adequate fysieke bescherming van haar gebouwen en de kritieke
infrastructuur, terdege rekening houdend met bijvoorbeeld het plaatsen van omheiningen, het oprichten van barrières, instrumenten en routines voor de bewaking van de omgeving,
detectieapparatuur en toegangscontroles;
c. de gevolgen van incidenten te bestrijden, te beperken en ertegen bestand te zijn, naar
behoren rekening houdend met de uitvoering van risico- en crisisbeheersingsprocedures en -protocollen en waarschuwingsroutines;
d. te herstellen van incidenten, naar behoren rekening houdend met bedrijfscontinuïteitsmaatregelen en de identificatie van alternatieve toeleveringsketens, om de verlening van de essentiële dienst te hervatten;
e. te zorgen voor adequaat beheer van personeelsbeveiliging, daarbij in ieder geval
rekening houdend met de volgende maatregelen:
1°. het vaststellen van categorieën personeelsleden die kritieke functies vervullen,
daarbij rekening houdend met het personeel van externe dienstverleners;
2°. het vaststellen van het recht van toegang tot gebouwen, kritieke infrastructuur en
gevoelige informatie;
3°. het instellen van procedures voor antecedentenonderzoek en het aanwijzen van
categorieën van personen die aan antecedentenonderzoek moeten worden onderworpen; en
4°. het vaststellen van passende opleidingsvoorschriften en kwalificaties; en
f. het relevante personeel bewust te maken van de maatregelen, genoemd in de

onderdelen a tot en met e, naar behoren rekening houdend met opleidingen, informatiemateriaal en oefeningen.

Artikel 15, tweede lid, Wwke schrijft voor dat zij die maatregelen moeten nemen op basis van de door de bevoegde autoriteit verstrekte relevante informatie over de sectorale risicobeoordeling en op basis van de resultaten van hun eigen risicobeoordeling.

Uiteraard moeten de criteria zoals die in de wet zelf zijn geformuleerd, worden gelezen in combinatie met de uitwerking daarvan in het Bwke 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 Bwke. Deze voorhangprocedure is geregeld in artikel 47b Wwke.

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 Rijksinspectie Digitale Infrastructuur (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.[9] 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 Wwke 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

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

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 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.

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. 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 15, eerste lid, Wwke 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 Bwke. Die uitwerking geldt voor alle kritieke entiteiten uit alle sectoren waarop de Wwke van toepassing is. De uitwerking van de zorgplicht in het Bwke 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 categorieën van entiteiten waarvoor zij verantwoordelijk zijn. Door de opname van de normen in de Wwke, de uitwerking daarvan in het Bwke 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 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 Wwke, het Bwke 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 BBB toelichten waarom in artikel 5 de genoemde overheidsorganisaties van de wet uitgezonderd zijn? Vallen alle in dit artikel niet genoemde overheidsorganisaties in principe wel onder de wet, ook organisaties die niet primair gericht zijn op ICT, maar wel ICT gebruiken? Deze

leden noemen hierbij enkele voorbeelden zoals beheerders van tunnels, dammen en eigenaren van laboratoria?

Artikel 5 Wwke strekt tot de implementatie van artikel 1, zesde lid, CER-richtlijn, waarin is bepaald dat de CER-richtlijn niet van toepassing is op overheidsinstanties die activiteiten uitvoeren op het gebied van nationale veiligheid, openbare veiligheid, defensie of rechtshandhaving, met inbegrip van het onderzoeken, opsporen en vervolgen van strafbare feiten. De regering heeft de CER-richtlijn zuiver geïmplementeerd, wat inhoudt dat in de Wwke geen andere regels worden opgenomen dan voor implementatie noodzakelijk zijn, om ervoor te zorgen dat implementatie zo spoedig mogelijk kan plaatsvinden. Alle niet in artikel 5 Wwke genoemde overheidsinstanties vallen dus onder toepassingsbereik van de wet, voor zover zij met toepassing van de criteria van artikel 6, eerste lid, Wwke zijn aangewezen als kritieke entiteit. De in artikel 5 Wwke genoemde overheidsinstanties kunnen niet worden aangewezen als kritieke entiteit.

Een deel van de kritieke entiteiten is afhankelijk van, of anderszins vervlochten met, andere kritieke entiteiten, zodat bijvoorbeeld cascade-effecten kunnen ontstaan. Deze leden vragen de regering of deze wet hen verplicht samen te werken om risico's af te dekken en maatregelen te nemen? Staat deze verplichting ook expliciet in de wet? Zo nee, waarom niet?

Sectoren, leveranciers en dienstverleners zijn steeds meer met elkaar verbonden en van elkaar afhankelijk. Daarom moeten kritieke entiteiten bij het uitvoeren van hun risicobeoordeling op grond van artikel 14, tweede lid, Wwke rekening houden met de mate waarin andere sectoren afhankelijk zijn van hun essentiële diensten, en de mate waarin zij zelf afhankelijk zijn van de essentiële diensten van andere entiteiten.

Cascade-effecten zijn een reëel risico. Het kan voorkomen dat er pas bij een incident ontdekt wordt dat een groter aantal organisaties binnen een sector diensten afneemt van één partij. Incidenten bij een dergelijke partij, ongeacht de aard of oorzaak, kunnen mogelijk grootschalige nationale of zelfs grensoverschrijdende gevolgen hebben. In het Bwke, de algemene maatregel van bestuur onder de Wwke, is dan ook in artikel 3 opgenomen dat kritieke entiteiten bij het uitvoeren van de risicobeoordeling rekening moeten houden met de mate waarin de dienstverlening van hun rechtstreekse leveranciers en dienstverleners risico's kan vormen voor hun essentiële dienstverlening. Ook wordt in de sectorale risicobeoordeling van de vakministers en in de nationale strategie aandacht besteed aan intersectorale en onderlinge afhankelijkheden.

De Wwke is risicogebaseerd ingericht, en de manier waarop een kritieke entiteit maatregelen neemt om deze risico's af te dekken is daarom aan de entiteit zelf. Samenwerking tussen partijen uit verschillende sectoren wordt echter aangemoedigd, bijvoorbeeld door platformbijeenkomsten die door de verantwoordelijke bevoegde autoriteiten georganiseerd worden en een cross-sectorale publiek-private netwerkdag.

Deze leden vragen de regering of zij vindt dat het voor invoering van deze wet nodig is om wet- en regelgeving over screening en veiligheidsonderzoeken van medewerkers van kritieke entiteiten en hun dienstverleners te herzien? Zijn hier al plannen voor?

De betrouwbaarheid van de personen die met de kritieke infrastructuur werken is uiteraard cruciaal voor de weerbaarheid van de kritieke entiteit. Artikel 15, eerste lid, onderdeel e, subonderdeel 3, Wwke bepaalt dat kritieke entiteiten in het kader van de zorgplicht procedures moeten instellen voor antecedentenonderzoek en categorieën van personen die aan antecedentenonderzoek moeten worden onderworpen, moeten aanwijzen. Ter uitwerking van dit voorschrift is in artikel 10 Bwke opgenomen dat kritieke entiteiten beleid vaststellen over de rollen, bevoegdheden en verantwoordelijkheden van hun personeel dat aan de weerbaarheid of beheer van de kritieke infrastructuur werkt. Onderdeel hiervan is in ieder geval het identificeren van categorieën van personeelsleden die kritieke functies vervullen.

Afhankelijk van de resultaten uit de uitgevoerde risicobeoordelingen kunnen door de verantwoordelijke vakminister vertrouwensfuncties worden aangewezen bij kritieke entiteiten en kan er voor bepaalde functionarissen een screening plaatsvinden op basis van de Wet veiligheidsonderzoeken. Hierbij kan worden gedacht aan personeelsleden met uitgebreide rechten of toegang tot kritieke infrastructuur of

omgevingen. Een andere mogelijkheid is het door de kritieke entiteit verplicht stellen van een Verklaring Omtrent het Gedrag (VOG) voor specifieke rollen. De regering acht de bestaande wet- en regelgeving hiervoor toereikend.

Deze leden vragen of eigenaren van kritieke entiteiten met deze wet ook aansprakelijk gemaakt worden voor het niet nakomen van de wet, zodat burgers en bedrijven schadevergoeding kunnen eisen? Of is deze aansprakelijkheid al in andere wetgeving vastgelegd? Is aansprakelijkheid voldoende in de wet vastgelegd?

Dit wetsvoorstel voorziet niet in nieuwe regels over aansprakelijkheid. Het bestaande aansprakelijkheidsregime (zowel bestuurs- als civielrechtelijk) is dan ook onverkort en ongewijzigd van toepassing.

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?

Op dit moment wordt voorzien in de inrichting van een meldpunt bij het Nationaal Cyber Security Centrum (NCSC) voor meldingen onder de Cbw én 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 Computer security incident response team (CSIRT) als hun bevoegde autoriteit.

Ten aanzien van de Wet weerbaarheid kritieke entiteiten heeft de regering allereerst aangegeven dat de zorgplicht van kritieke entiteiten mogelijk kleur kan worden gegeven door sectorspecifieke voorschriften in een EU-rechtshandeling. De leden van de D66-fractie vragen de regering of zij zelf al ideeën heeft over die sectorspecifieke voorschriften in EU-verband en of zij daarom met een duidelijke inzet ten aanzien van de beoogde voorschriften naar Europa afreist.

Op dit moment heeft de regering de in de vraagstelling bedoelde ideeën nog niet. Nadat de Wwke in werking is getreden, kan uit de ervaringen in de praktijk met die wet blijken dat bepaalde sectorspecifieke voorschriften in breder Europees verband nuttig zouden kunnen zijn. Als dat geval zich voordoet, zal de regering overwegen om daarvoor de aandacht te vragen in overleggen in Europees verband.

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 34, eerste lid, Wwke biedt entiteiten die onder het toepassingsbereik van de Wwke vallen op voorhand de zekerheid dat vertrouwelijke gegevens die bij de bevoegde autoriteiten, het centrale contactpunt en de Minister van Justitie en Veiligheid 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 de hiervoor genoemde partijen wordt gedeeld, waardoor de goede taakuitoefening van die partijen in het geding kan komen. Kritieke 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 reputatieschade, 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?

Kritieke entiteiten moeten op grond van artikel 17, eerste lid, Wwke incidenten die de verlening van hun essentiële dienst aanzienlijk verstoren of kunnen verstoren melden bij de bevoegde autoriteit. In artikel 17, derde lid, Wwke is bepaald dat bij het bepalen of een verstoring aanzienlijk is, in aanmerking wordt genomen: het aantal door de verstoring getroffen gebruikers en hun aandeel daarin, de duur van de verstoring, het door de verstoring getroffen geografische gebied, rekening houdend met de vraag of het gebied geografisch geïsoleerd is en de bij of krachtens algemene maatregel van bestuur vastgestelde aanvullende parameters. Op grond van artikel 17, vijfde lid, Wwke kunnen bij of krachtens algemene maatregel van bestuur de criteria worden vastgesteld op basis waarvan wordt bepaald of een verstoring aanzienlijk is als hiervoor bedoeld. Die criteria worden ook drempelwaarden genoemd. Aan de hand van een drempelwaarde kan worden bepaald of sprake is van een aanzienlijke verstoring bij een kritieke entiteit en daarmee meldplichtig is op grond van de Wwke.

In het Bwke, de algemene maatregel van bestuur onder de Wwke, 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 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, categorie van 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 kritieke entiteiten duidelijkheid over welke incidenten meldplichtig zijn. Er kan echter niet worden voorkomen dat kritieke entiteiten uit voorzorg melden.

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.[10] 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.*

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.

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

De genoemde motie ziet op digitaliseringswetgeving, terwijl de Wwke niet op netwerk- en informatiesystemen ziet. Deze vraag wordt daarom beantwoord langs de lijnen van de Cbw.

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)[11], 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.[12] Daarin zijn de gevolgen van de NIS2-richtlijn, de Cyberbeveiligingsverordening[13], de Cyberweerbaarheidsverordening[14] 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.[15] 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).[16] Inzichten daaruit dienen ter ondersteuning van het UDO-proces. In

---

[11] 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).

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

[13] 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).

[14] 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).

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

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

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 gelijke inwerkingtredingsdatum te kiezen, gelijktijdig met wat geldt voor entiteiten uit de andere sectoren.[17]
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.[18] 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[19] en reeds in 2021 is aangekondigd[20] dat de wettelijke verankering van informatieveiligheid wordt voorbereid. Ook is dit voornemen opgenomen in de tweede editie van de Werkagenda Waardengedreven Digitaliseren.[21] 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 Baseline Informatiebeveiliging Overheid versie 2.0 (hierna: 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.[22] 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

---

[17] 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.
[18] 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.
[19] *Kamerstukken II* 2018/19, 26643, nr. 574.
[20] *Kamerstukken II* 2020/21, 26643, nr. 749.
[21] *Kamerstukken II* 2022/23, 26643, nr. 940.
[22] *Kamerstukken I 2025/26, 31.731 / 29.362, X.*

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.

De leden van de fractie van de BBB vragen of de kritieke entiteiten zich op de vrije markt kunnen verzekeren voor de risico's en maatrelen waar deze wet zich op richt of zijn deze risico's (deels) onverzekerbaar?

De markt mag in principe zelf bepalen welke verzekeringen worden aangeboden. Die contractsvrijheid is echter niet onbeperkt: 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 de risico's en maatregelen waar de Wwke zich op richt 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.

Deze leden vragen of de regering verwacht dat kritieke entiteiten door deze wet, om risico's te verkleinen, sommige uitbestede werkzaamheden weer zelf, 'binnenshuis', zullen moeten gaan uitvoeren? Zijn de kritieke entiteiten hier goed toe in staat?

De verantwoordelijkheid voor het nemen van maatregelen in het kader van de zorgplicht onder de Wwke ligt bij kritieke entiteiten zelf. Voor de concrete invulling van die maatregelen is ruimte voor een eigen afweging van kritieke entiteiten om te bepalen welke precieze maatregelen zij redelijkerwijs moeten nemen, onder meer op basis van de eigen risicobeoordeling en de afweging van de mate waarin een maatregel passend en evenredig is. Of entiteiten hiervoor bepaalde kennis en kunde in huis hebben, dit willen opbouwen of dit gaan uitbesteden is een afweging die entiteiten zelf kunnen maken onder het risicogebaseerde raamwerk van de Wwke.

Deze leden vragen of de organisatie die toezicht moet houden op de kritieke entiteiten voor de uitvoering van de wet hiervoor voldoende wettelijke bevoegdheden heeft, maar ook kwantitatief en kwalitatief voldoende capaciteit. Zijn hier extra inspanningen van de regering voor nodig?

In de Wwke wordt het toezicht vormgegeven langs de lijnen van de ministeriële verantwoordelijkheden voor de sectoren. De regering heeft deze keuze gemaakt in het verlengde van de keuze om de risicobeoordeling van de bevoegde autoriteit door de verantwoordelijke vakminister uit te laten voeren. Sectorspecifieke kennis is namelijk een belangrijk onderdeel van de benodigde kwalitatieve capaciteiten om te kunnen beoordelen of een kritieke entiteit weerbaar is. Daarnaast kan het aansluiten op reeds bestaande toezichtrelaties gunstig zijn voor de (administratieve) lasten en regeldruk voor de betreffende kritieke entiteiten. Kritieke entiteiten staan doorgaans al in contact met hun sectorale toezichthouder, en zijn daardoor bekend met de instantie en werkwijze.

De toezichthoudende instanties werken momenteel aan het gereed stellen van hun organisaties voor de nieuwe toezichtstaken onder deze Wwke. Overleg tussen de toezichthoudende instanties vindt plaats in het overlegorgaan Samenwerkend Toezicht (Digitale) Weerbaarheid (STDW). In dit overlegorgaan maken deze instanties afspraken over noodzakelijke afstemming, informatie-uitwisseling en contact richting entiteiten, en wordt kennis uitgewisseld. Door bovengenoemde inspanningen hebben de aangewezen toezichthouders voldoende kwantitatieve en kwalitatieve capaciteiten om deze taken goed uit te voeren.

Deze leden vragen of de regering voldoende zicht heeft op de risico's van het gebruik van oude of verouderde ICT-systemen, ook wel 'legacy systems' genoemd, door kritieke entiteiten? Worden hier door de overheid en/of bedrijven voldoende maatregelen tegen genomen?

De Wwke kent een risicogebaseerde aanpak. Een *legacy system* is onderdeel van de risicoanalyse. Wanneer uit de risicoanalyse blijkt dat de beveiliging niet op orde is, dan zullen er compenserende maatregelen genomen moeten worden. Hierbij kan gedacht worden aan netwerksegmentatie, monitoring en beperkte toegang. Mochten

eventuele compenserende maatregelen ook niet leiden tot het gewenste beveiligingsniveau, dan zal het *legacy system* uitgefaseerd moeten worden.

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?

In artikel 8, eerste en tweede lid, Wwke zijn de vakministers aangewezen als de bevoegde autoriteit voor kritieke entiteiten. Op grond van artikel 8, derde lid, onderdeel a, Wwke heeft de bevoegde autoriteit, en dus de vakminister, de taak om te zorgen voor de bestuursrechtelijke handhaving van het bepaalde bij of krachtens de Wwke.[23] 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 Wwke, zie artikel 36, eerste lid, Wwke.[24] 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 8, eerste lid, Wwke aangehaald.

Bevoegde autoriteit	**Sector**	**Subsector**	**Toezichthoudende instantie**
Minister van Binnenlandse Zaken en Koninkrijksrelaties	overheid		Beveiligingsautoriteit Rijk
Minister van Economische Zaken	digitale infrastructuur		*
	ruimtevaart		Rijksinspectie Digitale Infrastructuur
Minister van Financiën	bankwezen		*
	infrastructuur voor de financiële markt		
Minister van Infrastructuur en Waterstaat	vervoer	lucht	Inspectie Leefomgeving en Transport
		spoor	
		water	
		weg	
		openbaar vervoer	
	drinkwater (uitgezonderd verpakt water)		
	afvalwater		
	drinkwater (verpakt water)		Nederlandse Voedsel- en Warenautoriteit
Minister van Klimaat en Groene Groei	energie	elektriciteit	Rijksinspectie Digitale Infrastructuur
		stadsverwarming en -koeling	
		olie	
		gas	
		waterstof	
Minister van Landbouw, Visserij, Voedselzekerheid en Natuur	productie, verwerking en distributie van levensmiddelen		Nederlandse Voedsel- en Warenautoriteit
Minister van Volksgezondheid, Welzijn en Sport	gezondheidszorg		Inspectie Gezondheidszorg en Jeugd

De bovenstaande tabel biedt geen uitputtende lijst van sectoren en toezichthoudende instanties. Na de inwerkingtreding van de Wwke kunnen de bevoegde autoriteiten (vakministers) namelijk ervoor kiezen om aanvullende sectoren aan te wijzen, conform artikel 7 Wwke. De vakministers zullen dan ook voor die aanvullende sectoren bij besluit de ambtenaren aanwijzen die zijn belast met het toezicht op de naleving van het bepaalde bij of krachtens de Wwke. De Minister van Infrastructuur en Waterstaat is voornemens om onder gebruikmaking van de hiervoor genoemde mogelijkheid in

[23] Dit geldt ook voor de bestuursrechtelijke handhaving van het bepaalde in de op grond van artikel 13, zesde lid, CER-richtlijn vastgestelde uitvoeringshandelingen, voor zover in die uitvoeringshandelingen is bepaald dat deze verbindend zijn en rechtstreeks toepasselijk zijn in elke lidstaat van de Europese Unie. Zie artikel 8, derde lid, onderdeel b, Wwke.
[24] Artikel 5:11 Awb spreekt in deze context over “toezichthouder”.

artikel 7 Wwke de aanvullende sectoren keren en beheren, meteorologie, chemie en nucleair aan te wijzen. De beoogde toezichthoudende instanties – zoals hiervoor bedoeld – zijn de Inspectie Leefomgeving en Transport voor kritieke entiteiten uit de sectoren keren en beheren, meteorologie en chemie, en de Autoriteit Nucleaire Veiligheid en Stralingsbescherming voor kritieke entiteiten uit de sector nucleair.

* Kritieke entiteiten in de sectoren digitale infrastructuur, bankwezen en infrastructuur voor de financiële markt zijn uitgezonderd van de verplichting tot het uitvoeren van een risicobeoordeling, de zorgplicht, de meldplicht, de verplichting tot het aanwijzen van een verbindingsfunctionaris, de verplichting uit artikel 20 Wwke (over de kennisgeving over de verlening van essentiële diensten aan of in zes of meer lidstaten van de Europese Unie) en de verplichting die is neergelegd in artikel 22 Wwke (over kritieke entiteiten van bijzonder Europees belang). Dit is geregeld in artikel 23 Wwke.

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?

Dit wetsvoorstel voorziet niet in nieuwe regels over aansprakelijkheid. 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.

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 Wwke 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 kritieke 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. Zoals hiervoor reeds aangegeven voorziet de Wwke niet in nieuwe regels over

aansprakelijkheid. Het bestaande aansprakelijkheidsregime, zowel bestuurs- als civielrechtelijk, is onverkort en ongewijzigd van toepassing.

De leden van de fractie van D66 constateren dat de regering aangeeft dat toezichthouders onderling afspraken moeten maken om overlap van het uitoefenen van bevoegdheden op dezelfde terreinen te voorkomen. Vindt de regering dat hier ook een taak voor de minister van J&V is weggelegd, vanuit de coördinerende rol van deze minister, om het overzicht goed te bewaren en te achterhalen welke afspraken worden gemaakt en of toezichthouders erin slagen om deze overlap in de praktijk te voorkomen?

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 Rijksinspectie Digitale Infrastructuur (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. De Minister van Justitie en Veiligheid heeft formeel geen zitting in het STDW en DTDW. Dit is van belang om de operationele onafhankelijkheid van de toezichthouders te borgen. Wel wordt de Minister van Justitie en Veiligheid, vertegenwoordigd door de NCTV, als stelselverantwoordelijke voor zowel cyberveiligheid als kritieke infrastructuur, regelmatig geïnformeerd over de ontwikkelingen in deze samenwerkingsgremia. Hierdoor wordt zowel de onafhankelijkheid van toezicht geborgd, en heeft de Minister van Justitie en Veiligheid voldoende informatiepositie om zijn sectoroverstijgende en coördinerende rol uit te oefenen. Toezicht valt echter primair onder verantwoordelijkheid van de betrokken vakministers.

In het hierboven genoemde overleg komen de toezichthouders samen om de overlap tussen de verschillende wet- en regelgeving die de weerbaarheid raken in kaart te brengen en daar afspraken over te maken. De afspraken die worden gemaakt tussen de toezichthouders zullen worden gepubliceerd. 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 heeft op wetten in zijn portefeuille. Daarmee is de regering het met de leden van de fractie van D66 eens dat de Minister van Justitie en Veiligheid hier een coördinerende rol in heeft, voor zover het gaat over de uitvoering van wetten die in zijn portefeuille zitten.

De regering maakt zelf vooral melding van de noodzaak van afspraken tussen ambtenaren in dit kader. Nu het om essentiële verdelingen van taken en bevoegdheden gaat, vragen deze leden of het niet meer voor de hand ligt dat vakministers en topfunctionarissen van zbo's hier ook onderling het gesprek over aangaan.

Omdat de uitvoering van het toezicht bij (de ambtenaren van) toezichthoudende instanties is belegd, ligt het naar de mening van de regering meer voor de hand dat daar het gesprek wordt gevoerd. Dat gebeurt in de praktijk al in het Samenwerkend Toezicht Digitale Weerbaarheid (STDW), waarin de volgende instanties samenwerken:
- 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)

Hoe denkt de regering over een register om de verschillende taken vanuit verschillende wetten van de verschillende toezichthouders op het gebied van veiligheid in kaart te brengen, zodat overlap voorkomen kan worden? Hoe denkt de regering daarnaast over het openbaar maken van een dergelijk register, zodat ook kritieke entiteiten zelf duidelijk en op een toegankelijke wijze kunnen achterhalen met wie ze van doen hebben?

De regering herkent dat vanuit verschillende wetten verschillende toezichthouders actief zijn die raken aan het thema veiligheid. Tegelijkertijd regelen deze verschillende wetten in het veiligheidsdomein verschillende aspecten van veiligheid, geredeneerd vanuit wettelijk verschillende gedefinieerde belangen en geldend voor verschillende groepen van entiteiten. Een eerdere inventarisatie daarvan, specifiek gericht op cybersecurity, is eerder aan de Tweede Kamer aangeboden.[25] Een overzicht van alle nationale, Europeesrechtelijke en internationaalrechtelijke wettelijke bepalingen ten aanzien van veiligheid in zijn vele verschijningsvormen (van mijnbouw, omgang met gevaarlijke stoffen, nucleaire veiligheid, milieuveiligheid, kunstmatige intelligentie tot sectorale wetten ten aanzien van bijvoorbeeld drinkwater of transport), gekoppeld aan de precieze entiteiten waarvoor specifieke bepalingen gelden en gekoppeld aan de bijhorende toezichthouders ziet de regering als niet-uitvoerbaar. Waar het gaat om kritieke entiteiten onder de Wwke betreft het bovendien een beperkte groep van entiteiten waarvoor de aanvullende weerbaarheidsvereisten vanuit die wet gaan gelden, waardoor de regering geen aanleiding ziet om naar aanleiding hiervan in een alomvattend overzicht te voorzien.

Verder constateren deze leden dat de regering heeft aangegeven dat zij verwacht in het eerste kwartaal van 2026 duidelijk te hebben hoe een toezichthouder op de sector overheid onafhankelijk kan optreden. Zijn deze inzichten inmiddels beschikbaar? Wanneer dit het geval is, zouden deze gegevens gedeeld kunnen worden?

Op dit moment wordt nog gewerkt aan een brief aan de Tweede Kamer die deze onafhankelijkheid nader onderbouwt. Ook wordt de Tweede Kamer binnen afzienbare tijd geïnformeerd over de uitwerking van het toezicht door de Beveiligingsautoriteit Rijk.

Daarnaast geeft de regering aan dat de vakministers momenteel bezig zijn met de risicobeoordelingen, maar dat het nog even kan duren voordat duidelijk zal zijn op welke entiteiten de Wet weerbaarheid kritieke entiteiten specifiek toe gaat zien. Kan de regering voor deze leden een inschatting maken hoelang dit zal duren? Kan dit sterk per sector verschillen? Zo ja, wat zijn de belangrijkste factoren die voor dit verschil in tempo zorgen?

Op grond van artikel 9, eerste lid, Wwke moet elke vakminister een risicobeoordeling uitvoeren voor de sectoren waarvoor zij in de Wwke zijn aangewezen als bevoegde autoriteit. Die risicobeoordelingen worden ook wel aangeduid als sectorale risicobeoordelingen. Het doel van de sectorale risicobeoordelingen is om in kaart te brengen waar risico’s bestaan of kunnen bestaan die negatieve gevolgen kunnen hebben voor de verlening van essentiële diensten. Kritieke entiteiten moeten vervolgens, zodra zij als zodanig zijn aangewezen, op grond van artikel 14, eerste lid, Wwke rekening houden met deze sectorale risicobeoordelingen bij het uitvoeren van hun eigen risicobeoordelingen.

Niet iedere vakminister is op hetzelfde moment gestart met het uitvoeren van de sectorale risicobeoordeling. De vakministers streven ernaar om vóór de inwerkingtreding van de Wwke de sectorale risicobeoordelingen af te ronden. Uiterlijk één maand na de inwerkingtreding van de Wwke moeten de sectorale risicobeoordelingen zijn uitgevoerd en entiteiten – die voldoen aan de criteria uit artikel 6 Wwke – zijn aangewezen als kritieke entiteit in de zin van de Wwke.[26]

De regering maakt duidelijk dat zij van plan is om bedrijven te ondersteunen bij de verplichtingen die voortvloeien uit de wet. Verschillende manieren waarop de overheid kritieke entiteiten hierbij kan helpen, volgen ook uit de wet zelf. Kan de regering aan deze leden toelichten hoe zij kijkt naar het opzetten van een netwerk van kritieke entiteiten, zodat kritieke entiteiten (vooral in dezelfde sectoren) ook onderling informatie over het uitvoeren van de wettelijke verplichtingen kunnen uitwisselen? Is de regering voornemens om ook publieke kritieke entiteiten te ondersteunen? Zo ja, doet zij dat op dezelfde manier?

---

[25] *Kamerstukken II* 2020/21, 26643, nr. 738.

[26] Dit volgt uit de artikelen 43 en 44 Wwke. De voorschriften in deze artikelen zijn verbonden aan de inwerkingtreding van die artikelen. Voor de leesbaarheid van deze passage wordt gesproken over de inwerkingtreding van de Wwke, ook omdat de regering niet voornemens is om te voorzien in gefaseerde inwerkingtreding van de Wwke.

Het kabinet werkt actief aan de ondersteuning van kritieke entiteiten, onder andere door informatie-uitwisseling te bevorderen. Zo zet het kabinet in op het ontwikkelen van netwerken zoals sectortafels, waarbij kritieke entiteiten en andere relevante partijen onderling informatie kunnen uitwisselen. De ondersteuning van kritieke entiteiten in zowel de publieke sector als de private sector loopt via de vakministers. Zij geven onder meer advies en zorgen voor de uitwisseling van informatie.

Verder vragen deze leden in hoeverre de werklast binnen overheidsinstanties toeneemt vanwege de risicobeoordelingen en in hoeverre dit als een serieuze negatieve consequentie van de wet wordt gezien. Het gaat dan om de werklast van kritieke entiteiten binnen de sector overheid, maar ook over de werklast van degenen die toezien op de uitvoering van de wet.

Het opstellen van een risicobeoordeling wordt gezien als basismaatregel om de weerbaarheid van kritieke entiteiten, inclusief aangewezen organisaties van de centrale overheid, op orde te brengen. Deze risicobeoordeling is vormvrij. Zodoende hebben kritieke entiteiten de ruimte voor maatwerk, kunnen zij reeds bestaande documenten gebruiken en biedt het hen ook de mogelijkheid om bijvoorbeeld verplichtingen uit verschillende wettelijke kaders te combineren. Een voorbeeld hiervan is dat kritieke entiteiten zelf kunnen kiezen welke methode of systematiek zij gebruiken bij het in kaart brengen van hun risico’s. Ook kunnen kritieke entiteiten bijvoorbeeld het uitvoeren van de risicobeoordeling in het kader van de Cbw en de Wwke combineren om administratieve lasten te verminderen. Dit beperkt de werklast met betrekking tot de risicobeoordeling. De regering acht de werklast voor overheidsorganisaties daarom proportioneel in verhouding tot de gevolgen die een incident bij bepaalde kritieke onderdelen van de Nederlandse overheid kan hebben.

Daarnaast heeft de regering aangeven dat de Europese Commissie momenteel een richtsnoer ontwikkelt om kritieke entiteiten te ondersteunen. Deze leden vragen of hier inhoudelijk al meer over bekend is. Bovendien vragen zij of het duidelijk is wanneer deze richtsnoeren opgesteld zullen zijn.

De Europese Commissie werkt in samenwerking met alle lidstaten van de Europese Unie aan een niet-bindend richtsnoer voor het nemen van weerbaarheidsverhogende maatregelen door kritieke entiteiten conform artikel 13 CER-richtlijn. Dit richtsnoer wordt opgesteld zodat die bij toepassing moeten leiden tot een zoveel mogelijk vergelijkbaar en geharmoniseerd niveau van weerbaarheid van kritieke entiteiten in de Europese Unie. Het richtsnoer geeft niet-uitputtende handvaten en voorbeelden waar kritieke entiteiten rekening mee kunnen houden bij het nemen van technische, beveiligings- en organisatorische maatregelen onder de wettelijke zorgplicht.

De Europese Commissie heeft een brede consultatie van Europese brancheverenigingen gehouden met ruimte voor inbreng van het Nederlandse bedrijfsleven, om tot het richtsnoer te komen. De relevante sectoren in Nederland zijn daarnaast geconsulteerd bij eerdere conceptversies van dit richtsnoer via het betreffende vakdepartement en belangenverenigingen.

De Europese Commissie heeft aangegeven ernaar te streven om het niet-bindend richtsnoer voor de zomer van 2026 te publiceren.

Verder merken deze leden op dat het gaat hier gaat om het implementeren van een richtlijn en niet om een verordening. De CER-richtlijn heeft als doel om een minimumniveau aan harmonisatie te creëren. Het staat lidstaten vrij om verder te gaan dan de CER-richtlijn. Heeft de regering in dit kader momenteel plannen voor aanvullende nationale wetgeving ten aanzien van kritieke entiteiten? Zijn er uit de besprekingen ten aanzien van de CER-richtlijn inzichten opgedaan voor nieuwe nationale wetgeving, bijvoorbeeld doordat op Europees niveau punten besproken zijn die uiteindelijk niet in de richtlijn terecht zijn gekomen, maar wel als wenselijk worden gezien? Ten aanzien van de sector overheid vragen deze leden of minimumharmonisatie in dit geval met zich meebrengt dat op nationaal niveau aanvullende maatregelen zouden kunnen worden genomen ten aanzien van belangrijke overheidsinstanties die niet onder de definitie van overheid vanuit de CER-richtlijn vallen. Zo ja, acht de regering het wenselijk dat dezelfde bepalingen vanuit de CER-richtlijn ook van toepassing zullen zijn op overheidsinstanties waar de CER-richtlijn niet op toeziet, zoals de rechterlijke macht en de Raad van State?

Er zijn op dit moment geen plannen voor aanvullende nationale wetgeving ten aanzien van kritieke entiteiten in de zin van de Wwke. Het kabinet is op dit moment van mening dat de Wwke – met inbegrip van de in artikel 7 Wwke opgenomen mogelijkheid om aanvullende (sub)sectoren en categorieën van entiteiten aan te wijzen waarbinnen kritieke entiteiten kunnen worden aangewezen – op dit moment een voldoende niveau van weerbaarheid van de vitale infrastructuur waarborgt en kijkt uit naar de uitvoering van de wet in de praktijk. Ook zijn de belangrijkste punten die het kabinet onder de aandacht heeft gebracht tijdens de onderhandelingen over de CER-richtlijn, conform het BNC-fiche (Beoordeling Nieuwe Commissievoorstellen), in de CER-richtlijn meegenomen.[27]

De regering geeft aan dat het een aandachtspunt is dat informatie-uitwisseling vanuit de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), bijvoorbeeld aan de Europese Commissie, plaatsvindt via een betrouwbaar en veilig proces en vertrouwelijkheid zou moeten borgen. Is het nodig dat dit een aandachtspunt is en is het daarmee op dit moment geen gegeven dat informatie-uitwisseling op die manier zal plaatsvinden? Op wat voor manier is de regering voornemens om hier aandacht aan te besteden of dit onder de aandacht te brengen?

Hoewel er op dit moment geen aanleiding tot zorg is, blijft de regering het belang onderstrepen om oog houden voor betrouwbare en veilige informatie-uitwisseling, waaronder met de Europese Commissie, zodat de vertrouwelijkheid van de informatie geborgd blijft. In de zogenaamde Groep voor de weerbaarheid van kritieke entiteiten (*Critical Entities Resilience Group*) heeft het Ministerie van Justitie en Veiligheid de Europese Commissie gevraagd om continu oog te blijven houden voor de betrouwbare informatie-uitwisseling van vertrouwelijke informatie met lidstaten.

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 Wet weerbaarheid kritieke entiteiten voor decentrale overheden. Daarbij wordt onder andere gewezen op financiële en organisatorische consequenties die uitvoering van de Wet weerbaarheid kritieke entiteiten met zich brengt. Deze leden vragen de regering toe te lichten hoe deze zorgen worden ondervangen.

Waterschappen zijn via de Unie van Waterschappen actief betrokken geweest bij het wetgevingsproces. Gedurende het implementatietraject is uitvoering gegeven aan de UDO. Zo is bij de voorbereidingen voor de lagere regelgeving onder de Wwke, zoals de Regeling weerbaarheid kritieke entiteiten IenW, uitvoerig overleg geweest tussen het Ministerie van Infrastructuur en Waterstaat en de waterschappen over de uitvoerbaarheid van de drempelwaarden in het kader van de meldplicht. Ook is bij de voorgenomen aanwijzing van waterschappen als kritieke entiteiten onder de Wwke met hen overleg gevoerd over de impact en uitvoerbaarheid van de verplichtingen uit de Wwke die voor hen van toepassing zullen zijn zodra zij zijn aangewezen als kritieke entiteit.

Gemeenten en provincies zijn 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 al 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.

6. Kosten

De leden van de fractie van de BBB vragen de regering hoe groot zij de totale extra kosten van de kritieke entiteiten schat om de eerste vijf jaren om aan de eisen van deze wet, zoals beveiligings- en veiligheidsmaatregelen, te gaan voldoen? In hoeverre staan deze of anderen wetten toe dat zij deze kosten aan burgers en bedrijven doorbelasten? Is hier additionele wetgeving voor nodig?

[27] *Kamerstukken II* 2020/21, 22112, nr. 3054.

De regering heeft onderzoek gedaan naar de verwachte regeldrukkosten voor kritieke entiteiten als gevolg van de Wwke. Gemiddeld wordt geschat dat bedrijven eenmalig € 347.000,– en € 173.000,– structureel per jaar kwijt zijn aan de uitvoering van de Wwke en de onderliggende regelgeving. Dit betreft een gemiddelde op basis van interviews met bedrijven. De Wwke beslaat een zeer grote variëteit aan bedrijven in meerdere sectoren. Deze kosten kunnen dus voor bedrijven en organisaties afwijken, bijvoorbeeld vanwege het verschil in grootte en draagkracht. Deze kosten zien daarnaast onder meer op de uitvoering van de zorgplicht, waarbij passende en evenredige maatregelen genomen dienen te worden. Dit betekent dat een maatregel of coherente set van maatregelen in verhouding dient te staan tot het te beheersen risico. Dat betekent dat een kritieke entiteit kan kiezen voor de maatregelen die het minst belastend zijn voor haar organisatie om het risico te beheersen.

7. Overgangsrecht

Kan de regering voor de leden van de fractie van FVD uiteenzetten waarom Nederland ervoor heeft gekozen om de CER-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 CER-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 CER-richtlijn biedt voor lidstaten en welke keuzes Nederland daarin heeft gemaakt. De transponeringstabel gaat uit van de bepalingen uit de CER-richtlijn. Voor de CER-richtlijn geldt dat er daarnaast ook één overweging is (specifiek: overweging 41) waarin beleidsruimte voor lidstaten is opgenomen. In die overweging is opgenomen dat de lijst van essentiële diensten in de CER-richtlijn niet uitputtend is en dat lidstaten de lijst kunnen aanvullen met andere essentiële diensten op nationaal niveau, om rekening te houden met nationale bijzonderheden bij de verlening van essentiële diensten. De regering acht het wenselijk om gebruik te kunnen maken van deze ruimte en heeft daarom in artikel 7 Wwke een grondslag opgenomen om ook entiteiten in andere sectoren onder het toepassingsbereik van de Wwke te kunnen brengen.

8. Overig

De leden van de fractie van de BBB vragen of de regering bereid is de komende tijd vertrouwelijke, besloten technische briefings aan het parlement te verzorgen om inzicht te geven in de uitdagingen die de invoering van deze wet oplevert?

De Minister van Justitie en Veiligheid moet op grond van artikel 40a, eerste lid, Wwke elk jaar aan de Eerste Kamer en de Tweede Kamer een geanonimiseerd verslag uitbrengen over de uitvoering van de Wwke, waarin in elk geval wordt ingegaan op het aantal kritieke entiteiten, gemelde incidenten en de uitvoering van toezicht en handhaving. Indien dit gewenst wordt door het parlement, is de regering bereid om hierover aanvullend besloten technische briefings te geven.

De Minister van Justitie en Veiligheid,

D.M. van Weel