Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2026-2027

36 875 Uitvoering van Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voorproducten met digitale elementen en tot wijziging van Verordeningen (EU) nr. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Uitvoeringswet verordening cyberweerbaarheid)

B **VERSLAG VAN DE VASTE COMMISSIE VOOR DIGITALISERING**[1]
Vastgesteld 3 november 2026

Het wetsvoorstel heeft de commissie aanleiding gegeven tot het maken van de volgende opmerkingen en het stellen van de volgende vragen.

1. Inleiding

De leden van de fractie van **PRO** hebben met belangstelling kennisgenomen van de Uitvoeringswet Verordening Cyberweerbaarheid (CRA) en hebben hierover enkele vragen.

De leden van de **PVV**-fractie hebben kennisgenomen van het wetsvoorstel ‘Uitvoeringswet verordening cyberweerbaarheid’, die onder andere belangrijke eisen stelt ten aanzien van digitale producten die vanaf 11 december 2027 op de Europese markt worden gebracht alsook verantwoordelijke autoriteiten aanwijst en toezicht en handhaving regelt en hebben daarover nog enkele vragen.

De leden van de **50PLUS**-fractie hebben met belangstelling kennisgenomen van het wetsvoorstel en hebben hierover nog enkele vragen.

2. Uitvoerbaarheid

De leden van de fractie van **PRO** constateren dat de beschikbare uitvoerbaarheidstoetsen van het Nationaal Cyber Security Centrum (NCSC) en Rijksinspectie Digitale Infrastructuur (RDI) van enige tijd geleden zijn, toen een aantal zaken nog niet bekend of onzeker waren.[2] De oordelen over de uitvoerbaarheid zijn daarom niet eenduidig, bevatten veel aannames, schetsen verschillende mogelijke scenario’s en noemen noodzakelijke randvoorwaarden waarvan onduidelijk is of deze ingevuld zijn. Daarom vragen deze leden om een actuele uitvoerbaarheidstoets van het NCSC en de RDI op basis van de voorliggende wet en de actuele stand van zaken.

De RDI noemt drie aandachtpunten, namelijk de bevoegdheden ten opzichte van conformiteitsbeoordelingsinstanties, samenloop met de Cyberbeveiligingswet (NIS2) en de

[1] Samenstelling:
Baumgarten (JA21), Beukering (Fractie-Beukering), Fiers (PRO), Van Gasteren (Fractie-Van Gasteren), Goossen (BBB), Hartog (Volt), Van Hattem (PVV), Janssen (SP), Kanis (D66), Lievense (BBB), Van Meenen (D66), Musa (VVD), Nicolaï (PvdD), Van den Oetelaar (FVD), Panman (BBB) (ondervoorzitter), Petersen (VVD), Ramsodit (PRO), Recourt (PRO), Van Rooijen (50PLUS), Roovers (PRO), Van de Sanden (Fractie-Van de Sanden), Steenkamp (CDA), Talsma (ChristenUnie), Veldhoen (PRO) (voorzitter), Visseren-Hamakers (Fractie-Visseren-Hamakers), De Vries (SGP), Walenkamp (Fractie-Walenkamp)
[2] Bijlage bij *Kamerstukken II* 2025/26, 36875, nr. 3.

AI-verordening en de geharmoniseerde normen en capaciteit bij aangemelde instanties. Graag zien deze leden in de herziene uitvoerbaarheidstoets ook aandacht voor deze drie punten.

De NCSC stelt in de uitvoerbaarheidstoets dat er aanvullend beleid nodig is ten aanzien van de bevoegdheid om het publiek over een bij zo'n melding betrokken kwetsbaarheid te informeren. Deze bevoegdheid is volgens artikel 17 lid 2 van de CRA beperkt tot die gevallen waarin "*bewustmaking van het publiek noodzakelijk is om een ernstig incident met gevolgen voor de beveiliging van het product met digitale elementen te voorkomen of te beperken of om een lopend incident af te handelen, of indien de bekendmaking van het incident anderszins in het algemeen belang is*". Dit kan alleen plaatsvinden na raadpleging van de betrokken fabrikant. Het informeren van gebruikers van het product onder de CRA is primair belegd bij de betreffende fabrikant. Het als coördinator aangewezen Computer Security Incident Response Team (CSIRT) kan echter, wanneer dit informeren van gebruikers niet tijdig door de fabrikant plaatsvindt, tot een dergelijk informeren overgaan, indien dit evenredig en noodzakelijk wordt geacht om de gevolgen van die kwetsbaarheid of dat incident te voorkomen of te beperken. Deze leden stellen hierover de volgende vragen.

Kan de regering aan deze leden toelichten of het afwegingskader inmiddels vastgesteld is? Zo nee, waarom niet, terwijl de meldplicht en de bevoegdheden sinds 11 september 2026 gelden?

Deze leden vragen wie het kader vaststelt en wie ervoor verantwoordelijk is. Is dat de minister van Justitie en Veiligheid, de minister van Economische Zaken of het NCSC zelf?

Kan de regering aan deze leden toelichten of het afwegingskader een openbare beleidsregel wordt of een intern werkdocument? Is het voor fabrikanten en burgers kenbaar? Zo nee, hoe wordt gewaarborgd dat de criteria voor fabrikanten, gebruikers en de rechter kenbaar zijn?

Deze leden vragen hoe de criteria 'noodzakelijk', 'ernstig incident' en 'algemeen belang' worden ingevuld. Worden er drempels gehanteerd, bijvoorbeeld voor het aantal getroffen gebruikers, toepassing in vitale processen of risico's voor fysieke veiligheid?

Tevens vragen deze leden wanneer een fabrikant 'niet tijdig' informeert. Hanteert het NCSC een termijn en hoe stelt het NCSC vast dat gebruikers niet of onvoldoende zijn geïnformeerd? Wanneer acht het NCSC het informeren van gebruikers 'evenredig en noodzakelijk'?

Kan de regering aan deze leden toelichten hoe het afwegingskader zich verhoudt tot het bestaande *Coordinated Vulnerability Disclosure* (CVD)-beleid van het NCSC, waarin de hoofdregel is dat openbaarmaking pas volgt nadat een kwetsbaarheid is verholpen? In welke gevallen weegt het belang van snelle waarschuwing zwaarder dan die terughoudendheid?

Kan de regering tevens aan deze leden toelichten hoe de raadpleging van de fabrikant is ingericht? Welke termijn krijgt de fabrikant om te reageren en hoe verloopt de raadpleging bij spoed? Welk gewicht krijgt de reactie van de fabrikant? Wat gebeurt er

als hij niet reageert of bezwaar maakt tegen openbaarmaking? Is zijn standpunt adviserend of kan hij publicatie in feite tegenhouden?

Fabrikanten melden bij het CSIRT van de lidstaat van hun hoofdvestiging. Kan de regering aan deze leden toelichten of het NCSC het Nederlandse publiek of Nederlandse gebruikers informeren over een kwetsbaarheid die bij een CSIRT in een andere lidstaat is gemeld? Wie beslist dan over openbaarmaking en hoe wordt dit binnen het CSIRT-netwerk en met het Europees Agentschap voor netwerk- en informatiebeveiliging (ENISA) afgestemd?

Deze leden vragen de regering hoe wordt afgestemd met de RDI. Die heeft als markttoezichtautoriteit eigen bevoegdheden om het publiek te waarschuwen en corrigerende maatregelen te nemen. Wie communiceert wat en wanneer?

De leden van de **50PLUS**-fractie vragen hoe bij de regering ervoor zorgt dat informatie over de cyberveiligheid en de ondersteuningsduur van producten ook consumenten bereikt die niet zelf op veiliginternetten.nl naar deze informatie zoeken. Deze leden vragen daarbij hoe rekening gehouden wordt met consumenten die minder digitaal vaardig zijn.

3. Hoofdlijnen wetsvoorstel

De leden van de fractie van **PRO** vragen de regering of de toepassing van de openbaarmakingsbevoegdheden meegenomen worden in de evaluatie van de wet, zoals voorgesteld in het amendement over een evaluatie na drie jaar.[3]

De leden van de fractie van de **PVV** lezen in Artikel 3.3 van de Uitvoeringswet: "*een woning te betreden zonder toestemming van de bewoner*". Dit vloeit voort uit Artikel 14 van de Markttoezichtverordening die eist dat toezichthouders alle gebouwen en terreinen van marktdeelnemers moeten kunnen betreden. De bevoegdheid om een woning te betreden is echter strikt gekoppeld aan de fysieke locatie waar de handelsactiviteiten daadwerkelijk plaatsvinden. Kan de regering toelichten wat hiervan de toegevoegde waarde is, in ogenschouw nemende dat bijvoorbeeld een directeur van een vennootschap onder firma (VoF), maar ook een grotere besloten vennootschap (bv) of naamloze vennootschap (nv), ook werk mee naar huis neemt en zelfstandigen met óf zonder personeel een werkplek kunnen huren in een bedrijfsverzamelgebouw en daarmee ook buiten de grondslag van dit artikel vallen? Hoe proportioneel is dit artikel dan?

Deze leden lezen tevens, bij de reikwijdte van de wet, dat motorvoertuigen uitgezonderd worden. Kan de regering toelichten, met het oog op alle ophef rondom bijvoorbeeld de "killswitches" waar de afgelopen jaren veel over te doen was in de politiek alsook in de media, in hoeverre de in deze verordening gestelde eisen al dan niet worden toegepast, waar hier de grootste cyberrisico's schuilen en hoe deze worden ondervangen?

Voortbordurend op de vorige vraag, constateren deze leden dat medische (in vitro) apparaten zijn uitgezonderd. Nu dienen deze apparaten te voldoen aan de Medical Device Regulation (MDR). Is in beeld op welke punten de MDR, in vergelijking met de CRA, tekortschiet? Hierbij denken deze leden bijvoorbeeld aan de snelheid van de meldplicht. Welke acties gaat de regering concreet ondernemen om deze tekortkomingen aan te pakken?

4. Verhouding tot overig EU-recht

[3] *Kamerstukken II* 2025/26, 36.875, nr. 8.

De leden van de fractie van **PRO** vragen of de regering het openbaar maken van informatie door het NCSC kwalificeert op grond als feitelijk handelen of als besluit in de zin van artikel 1 lid 3 van de Algemene wet bestuursrecht. Kan een fabrikant er vooraf tegen opkomen, bijvoorbeeld met een voorlopige voorziening? Wie is aansprakelijk voor schade door een onjuiste, onzorgvuldige of voortijdige openbaarmaking en wie is aansprakelijk voor schade door het ten onrechte achterwege laten van een waarschuwing?

Kan de regering aan deze leden toelichten hoe de openbaarmakingsbevoegdheid onder de CRA zich verhoudt tot verzoeken op grond van de Wet open overheid om informatie uit CRA-meldingen?

Het NCSC wijst op een strikte scheiding tussen zijn taken als CSIRT onder de Cyberbeveiligingswet (NIS2) en als coördinerend CSIRT onder de CRA. Kan de regering aan deze leden toelichten hoe de openbaarmakingsbevoegdheid onder de CRA zich verhoudt tot de informatiedeling onder de Cyberbeveiligingswet, onder meer via schakelorganisaties (OKTT's)?

De leden van de **PVV**-fractie vragen de regering hoe een "China Export"-markering de veiligheid van onze digitale producten dient te borgen. Hoe kan een bijna exacte kopie van die markering als superveilige garantie dienen op een manier dat het zelfs voor een peuter helder zou zijn dat CE en CE geheel verschillend zijn en dat het absoluut, onder geen beding, met elkaar te verwarren is?

De leden van de **50PLUS**-fractie constateren dat de Europese Commissie de mogelijkheid heeft om nadere voorschriften vast te stellen voor etiketten of pictogrammen met informatie over de cyberveiligheid en de ondersteuningsperiode van producten. Deze leden vragen hoe de regering aankijkt tegen een eenvoudige en herkenbare aanduiding waarmee consumenten bij aankoop kunnen zien tot wanneer een product beveiligingsupdates ontvangt. Is de regering bereid zich hiervoor in Europees verband in te zetten?

5. Gevolgen regeldruk qua capaciteitsbeslag

Voor beoordeling, opvolging en helpdesk ging de Quick-scan uit van twee fte, uitdrukkelijk als eerste basis.[4] De leden van de fractie van **PRO** vragen de regering of dat genoeg is voor zorgvuldige en snelle afwegingen, ook buiten kantooruren.

6. Advies en consultatie

De leden van de **PVV**-fractie lezen dat er vanuit de markt tijdens de internetconsultatie werd gepleit voor een centraal register, maar dat de regering daar afwijzend tegenover stond, omdat dit geen onderdeel uitmaakte van de Verordening. Kan de regering toelichten hoe zij staat tegenover zo'n register en heeft de regering zicht op de voor- en nadelen van een register, rekening houdende met het feit dat een register uit meerdere schillen kan bestaan om zo kwetsbaarheden om tot de bulkdata te komen uit te sluiten.

7. Inwerkingtreding

[4] Bijlage bij *Kamerstukken II* 2025/26, 36875, nr. 3.

De leden van de fractie van **PRO** vragen of de Europese Commissie aan geharmoniseerde richtsnoeren werkt. Zo ja, wacht Nederland daarop? Wat geldt er in de tussentijd?

De leden van de **50PLUS**-fractie constateren dat de meeste verplichtingen uit de Verordening niet gelden voor producten die voor 11 december 2027 in de handel zijn gebracht. Deze leden vragen hoe consumenten worden geïnformeerd wanneer bij dergelijke producten de beveiligingsondersteuning wordt beëindigd en het veilig gebruik daardoor niet langer kan worden gegarandeerd.

De vaste commissie voor Digitalisering ziet met belangstelling uit naar de nota naar aanleiding van het verslag en ontvangt deze graag binnen **vier weken** na vaststelling van dit verslag.

De voorzitter van de vaste commissie voor Digitalisering,
Veldhoen

De griffier van de vaste commissie voor Digitalisering,
Van Dooren