

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2429

Vragen van de leden **Bontenbal** en **Boswijk** (beiden CDA) aan de Ministers van Klimaat en Groene Groei en van Binnenlandse Zaken en Koninkrijksrelaties over *het bericht dat Amerikaanse experts geheime communicatieapparatuur hebben aangetroffen in Chinese zonne-omvormers* (ingezonden 21 mei 2025).

Mededeling van Minister **Hermans** (Klimaat en Groene Groei) (ontvangen 13 juni 2025).

Vraag 1

Bent u bekend met het artikel «Rogue communication devices found in Chinese solar power inverters»¹?

Vraag 2

Is het feit dat er naar schatting in totaal 200 gigawatt (GW) aan Europese zonne-energiecapaciteit (een vermogen dat gelijk is aan dat van meer dan 200 kerncentrales) is gelinkt aan in China gemaakte omvormers voor u reden tot zorg?

Vraag 3

Deelt u de mening dat dit laat zien dat we in Europa te afhankelijk zijn geworden van Chinese omvormers en dat dit grote risico's met zich mee kan brengen voor onze energie-infrastructuur?

Vraag 4

Vallen de zonne-energiecapaciteit en de bijbehorende omvormers onder de vitale objecten waarvan de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) de wettelijke taak heeft maatregelen te bevorderen voor een adequate beveiliging (c-taak)? Ziet de AIVD redenen om naar aanleiding van het genoemde bericht redenen om maatregelen te bevorderen? Zo ja, welke? Zo nee, waarom niet?

¹ Reuters, 14 mei 2025, «Rogue communication devices found in Chinese solar power inverters». (<https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/>)

Vraag 5

In hoeverre wordt er binnen de Europese Unie (EU) nagedacht over maatregelen om gezamenlijk op te treden tegen de import en het gebruik van potentieel onveilige Chinese omvormers? Wordt er bijvoorbeeld overwogen om in navolging van Litouwen het gebruik van deze omvormers in installaties boven een bepaalde capaciteit te verbieden?

Vraag 6

Welke initiatieven zijn er nationaal en in Europees verband om Europese fabrikanten van veilige en betrouwbare omvormers te ondersteunen en het gebruik van in Europa geproduceerde omvormers te stimuleren en daarmee de afhankelijkheid van Chinese producten te verminderen?

Vraag 7

Kunt u aangeven in hoeverre en op welke schaal omvormers van Chinese makelij momenteel in Nederland zijn geïnstalleerd?

Vraag 8

Wat zijn de potentiële risico's voor de Nederlandse energievoorziening als ook in (een deel van) deze omvormers geheime communicatieapparatuur is geïnstalleerd?

Vraag 9

Welke waarborgen en controles zijn er om te voorkomen dat dergelijke apparatuur wordt geïnstalleerd in bijvoorbeeld omvormers die ook in Nederland worden gebruikt?

Vraag 10

In hoeverre bestaan er in Nederland en in de EU systemen of procedures waarmee verdachte communicatie vanuit omvormers kan worden gedetecteerd of geblokkeerd? Worden daar actief controles op uitgevoerd?

Vraag 11

Is bestaande wet- en regelgeving die ervoor moet zorgen dat ook fabrikanten en leveranciers hun verantwoordelijkheid nemen om de risico's van door hen geleverde apparatuur voor het elektriciteitsnet te verkleinen voldoende om te voorkomen dat er alsnog bijvoorbeeld geheime communicatieapparatuur in wordt geïnstalleerd?

Vraag 12

Hoe groot acht u het risico dat kwaadwillende actoren via ongeautoriseerde communicatieapparatuur in zonne-omvormers gecoördineerde verstoringen kunnen veroorzaken in het Nederlandse elektriciteitsnet, bijvoorbeeld door duizenden huishoudens of installaties tegelijkertijd uit te schakelen?

Vraag 13

Welke maatregelen zijn er genomen sinds de waarschuwing van de Rijksinspectie Digitale Infrastructuur (RDI) van mei 2023² over de kwetsbaarheid van zonne-omvormers voor hacking en sabotage?

Vraag 14

Welke stappen zijn er specifiek gezet naar aanleiding van de bevinding van de RDI dat geen enkele van de onderzochte omvormers voldeed aan de norm en daardoor eenvoudig was te hacken, van afstand uit te schakelen of in te zetten voor DDoS-aanvallen?

Vraag 15

Heeft de RDI hier in de afgelopen twee jaar nieuw onderzoek naar gedaan en is daarbij verbetering geconstateerd?

² Rijksinspectie Digitale Infrastructuur, 30 mei 2023, «Omvormers kunnen storing veroorzaken en zijn vaak makkelijk te hacken». (<https://www.rdi.nl/actueel/nieuws/2023/05/30/omvormers-kunnen-storing-veroorzaken-en-zijn-vaak-makkelijk-te-hacken>)

Vraag 16

Heeft het onderzoek van de RDI uit 2023 ertoe geleid dat er een bredere evaluatie is uitgevoerd van bestaande zonne-energie-installaties in Nederland om te bepalen welke omvormers mogelijk een beveiligingsrisico vormen? Zo ja, wat zijn daarvan de resultaten en welke vervolgstappen worden er genomen? Zo nee, bent u bereid om hier alsnog vervolgonderzoek naar te laten doen?

Vraag 17

Hoe verloopt de implementatie van de Critical Entities Resilience Directive (CER) en de Network- and Information Security 2 Directive (NIS2) in Nederland?

Vraag 18

Kunt u uiteenzetten hoe er bij de implementatie van deze Europese richtlijnen die gaan over het verbeteren van de bescherming van vitale infrastructuur in Nederland aandacht wordt besteed aan verbeterde beveiliging van zonne-omvormers en andere componenten van het elektriciteitsnet?

Mededeling

De vragen van de leden Bontenbal en Boswijk (beiden CDA) over het bericht dat Amerikaanse experts geheime communicatieapparatuur hebben aangetroffen in Chinese zonne-omvormers (kenmerk 2025Z09993) kunnen niet binnen de gebruikelijke termijn worden beantwoord. De reden van uitstel is dat interdepartementale afstemming meer tijd vraagt. Het kabinet zal de Kamer zo spoedig mogelijk de antwoorden op de vragen doen toekomen.