2026Z08988

(ingezonden 24 april 2026)

Vragen van de leden El Boujdaini (D66) en Kathmann (GroenLinks-PvdA) aan de minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat over het bericht AI-model Mythos geprezen en gevreesd lijkt in handen gevallen van onbevoegden.

1. Bent u bekend met het bericht in het NRC over het AI-model Mythos dat mogelijk in handen is gevallen van onbevoegden? 1)

2. Deelt u de analyse dat ongecontroleerde verspreiding van geavanceerde AI-modellen risico's kan vergroten op cyberaanvallen, geautomatiseerde fraude en andere schadelijke toepassingen? Zo ja, welke risico's acht u het meest urgent? Zo nee, waarom niet?

3. Welke rol spelen geavanceerde AI-modellen op dit moment in het dreigingsbeeld? Welke gevolgen heeft de uitrol van Mythos, binnen afzienbare tijd ook aan het grotere publiek, voor dit dreigingsbeeld?

4. Bent u van mening dat overheden toegang moeten krijgen tot Mythos zodat zij het kunnen gebruiken om preventief kwetsbaarheden op te sporen en te dichten? Kan dit op een veilige en verantwoorde manier?

5. Hoe bereidt u overheidsorganisaties voor op de cyberveiligheidsrisico's die gepaard gaan met de uitrol van Mythos? Kunt u uiteenzetten welke acties u neemt om de veiligheid van persoonsgegevens van burgers en de ICT-processen van de overheid te garanderen?

6. Welke rol zou een onafhankelijke AI-raad, zoals voorgesteld in de motie-Kathmann/Six Dijkstra (Kamerstuk 26643, nr. 1403), kunnen spelen om de veiligheidsrisico's van geavanceerde AI te monitoren en af te dekken? Hoe wordt deze motie nu uitgevoerd?

7. Heeft u voldoende zicht op de risico's van *model leakage*, *model theft* en ongeautoriseerde verspreiding van geavanceerde AI-systemen in Nederland en Europa? Zo ja, hoe wordt dit inzicht benut voor beleid en toezicht? Zo nee, welke maatregelen neemt u om dit inzicht te verbeteren?

8. Hoe beoordeelt u de toereikendheid van bestaande beveiligingsnormen en toezichtmechanismen voor ontwikkelaars en beheerders van krachtige AI-modellen, mede in relatie tot de implementatie van de AI-verordening?

9. Welke kansen ziet u om via veilige ontwikkeling en deployment van AI de digitale veiligheid te versterken, bijvoorbeeld voor cyberdetectie, opsporing en publieke dienstverlening?

10. Ziet u in deze casus aanleiding om in Europees verband te pleiten voor versterkte samenwerking rond monitoring van toegangsbeheer, auditing en incidentrespons? Zo ja, op welke wijze?

11. Hoe beoordeelt u de wenselijkheid van meer transparantieverplichtingen voor aanbieders van geavanceerde AI-systemen over beveiligingsmaatregelen, incidenten en misbruikrisico's?

12. Kunt u de vragen afzonderlijk beantwoorden en in ieder geval vóór het rondetafelgesprek cyberveiligheid en informatiebeveiliging van 20 mei 2026?

1) NRC, 12 april 2026, AI-model Mythos - geprezen en gevreesd - lijkt in handen gevallen van onbevoegden (www.nrc.nl/nieuws/2026/04/22/ai-model-mythos-geprezen-en-gevreesd-lijkt-in-handen-gevallen-van-onbevoegden-a4926120).