Eerste Kamer der Staten-Generaal

Minister van Defensie
Mevrouw D. Yeşilgöz-Zegerius
Postbus 20701
2500 ES Den Haag

Kazernestraat 52
2514 CV Den Haag
postbus 20017
2500 EA Den Haag

telefoon 070 312 92 45

e-mail postbus@eerstekamer.nl

datum *19 mei 2026*
betreft *Nadere vragen inzake kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid'*
ons kenmerk *181118*

Geachte mevrouw Yeşilgöz-Zegerius,

De leden van de commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking (BDO) hebben met belangstelling kennisgenomen van uw brief[1] van 9 maart 2026 in beantwoording op de brief met nadere vragen van de commissie van 27 januari 2026 over de kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid'. De leden van de fractie van de **Partij voor de Dieren** hebben naar aanleiding hiervan nog een aantal nadere vragen en opmerkingen. Zij vragen u hierbij de sub(vragen) afzonderlijk te beantwoorden.

Vragen en opmerkingen van de leden van de PvdD-fractie

Vraag 1
De leden van de fractie van Partij van de Dieren constateren dat zowel in uw beantwoording van de eerdere vragen, als tijdens de technische briefing van de Eerste Kamer van de commissie Justitie en Veiligheid die op 31 maart 2026 plaatsvond[2], is erkend dat er een grote schaarste aan cybersecurity-specialisten bestaat.
De verwachting is dat de vraag naar zulke specialisten nog zal toenemen, terwijl uit berichten van de NCSC, de NCTV, de MIVD en de AIVD blijkt dat cyberaanvallen van statelijke en criminele actoren toenemen.

Vraag 1a
Kunt u aangeven wat de verwachting is met betrekking tot het kunnen voldoen aan de vraag naar cyberspecialisten van Defensie? Kunt u daarbij betrekken dat ook bij andere overheidsdiensten en bij de veiligheidsdiensten een behoefte bestaat aan cyberspecialisten?

Vraag 1b

[1] Zie verslag nader schriftelijk overleg: *Kamerstukken I,* 2025-2026, 30821, E.
[2] Commissie Justitie & Veiligheid van de Eerste Kamer, Technische briefing over weerbaarheid tegen hybride dreigingen in het kader van E250005 - Commissiemededeling: een nieuwe Europese strategie voor interne veiligheid, 31 maart 2026, https://www.eerstekamer.nl/commissievergadering/20260331_j_v/verslag.

Valt uit uw antwoord op vraag 1a af te leiden dat het nog een aantal jaren zal duren voordat de Cyber Academy van Defensie-cyberspecialisten zal afleveren die zich kunnen meten met specialisten die aangestuurd worden door Rusland, China, Noord-Korea en andere statelijke actoren?

Vraag 1c
Het Defensie Cyber Commando heeft – zo blijkt uit uw antwoord op vraag 1b in de beantwoording[3] – een "eigen wervingsplan". Levert dat plan voldoende op? Hoeveel specialisten zijn er nodig en hoeveel worden er binnengehaald? Wat zijn de verwachtingen van de "specifieke wervingsvideo voor het cyberdomein'?

Vraag 2
Blijkens uw antwoorden en de informatie die tijdens de technische briefing werd gegeven, constateren de leden van de Partij voor de Dieren-fractie dat de overheid afhankelijk is van de arbeidsmarkt voor cyberspecialisten. Op andere gebieden - zoals bijvoorbeeld in de ruimtelijke ordening en bij grondbeleid – beschikt de overheid over publiekrechtelijke instrumenten ('voorkeursrecht') die kunnen worden ingezet om niet volledig afhankelijk te zijn van de markt. Bent u bereid om te laten onderzoeken of eisen van veiligheid en weerbaarheid een grondslag kunnen bieden voor wetgeving waarmee – bij een tekort aan cyberspecialisten die bereid zijn in dienst te treden van de overheid – cyberspecialisten die in de private sector werkzaam zijn, of willen zijn, kunnen worden verplicht om voor Defensie of voor andere cruciale overheidsdiensten te werken? Is het realistisch om aan invoering van een vorm van 'dienstplicht' op dat terrein te denken?

Vraag 3
Het verslag 'Cybersecuritybeeld Nederland 2025' sluit af met een paragraaf over het gevaar als generatieve AI de bestaande digitale dreigingen gaat versterken. Er wordt geconcludeerd: "De diensten achten dit een zorgwekkende ontwikkeling".[4]
Is Nederland voldoende voorbereid op deze ontwikkeling? Welke stappen worden gezet om het gebruik van *Large Language Models* door statelijke actoren het hoofd te kunnen bieden?

Vraag 4
In de NRC van 6 mei 2026[5] wordt aandacht besteed aan het nieuwste AI-model Mythos, dat grote zorgen baart, zo constateren de leden van deze fractie.

Vraag 4a
Is het aannemelijk dat dit model "duizenden ernstige kwetsbaarheden ontdekt in vrijwel elk belangrijk besturingssysteem", zodat het in handen van statelijke actoren een instrument biedt om zoveel geslaagde hack-operaties uit te voeren dat de maatschappij volledig ontwricht zal raken?

Vraag 4b

[3] Idem, blz. 9.
[4] Nationaal Coördinator Terrorismebestrijding en Veiligheid, 'Cybersecuritybeeld Nederland in 2025. Riskante mix in een onvoorspelbare wereld', november 2025, blz. 46.
[5] NRC, 'Vrees voor 'cyber-bloedbad' in het Europees Parlement nu doemscenario's over AI overheersen', 6 mei 2026, https://www.nrc.nl/nieuws/2026/05/06/vrees-voor-cyber-bloedbad-in-het-europees-parlement-nu-doemscenarios-over-ai-overheersen-a4927199.

Zullen de AI Act, de Cyber Resilience Act en de implementatie van de NIS2-richtlijn middelen aanreiken waarmee zulke ontwrichting kan worden voorkomen?

Vraag 4c
Is de samenleving voldoende geïnformeerd over en voorbereid op de risico's die verbonden zijn aan het 'op de markt komen' van modellen van generatieve AI die voor geslaagde hack-operaties kunnen worden ingezet?

Vraag 5
Uit de informatie bij de technische briefing en uit de rapporten van NCTV, AIVD en MIVD merken de leden van de Partij voor de Dieren-fractie op dat het dreigingsbeeld steeds complexer wordt. Actoren en criminele actoren werken samen. Actoren die de binnenlandse veiligheid bedreigen zijn verweven met hybride oorlogsvoering door statelijke actoren.
Naar het oordeel van deze leden worden de grenzen tussen oorlogshandelingen (Defensie), binnenlandse veiligheid (BZK) en criminaliteitsbestrijding (J&V) steeds onduidelijker en daarmee wordt ook de vraag welk overheidsorgaan bevoegd is om tegenmaatregelen te treffen, steeds lastiger te beantwoorden.

Vraag 5a
Deelt u dat oordeel? Sluit de huidige wetgeving wel voldoende aan op die situatie?

Vraag 5b
Als de AIVD of de MIVD bij cyber-aanvallen 'tegenmaatregelen' treft, kan dat dan onder omstandigheden als een 'oorlogshandeling' worden gezien?

Vraag 5c
Welke criteria worden gehanteerd om cyberhandelingen van de overheid die gericht zijn op het bestrijden van een cyberaanval die in opdracht van een statelijke actor is uitgevoerd, te rekenen tot de bevoegdheid van hetzij Defensie, hetzij de MIVD, hetzij de AIVD?

De leden van de vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking (BDO) zien uw reactie met belangstelling tegemoet en ontvangen deze graag binnen vier weken na dagtekening van deze brief.

Hoogachtend,

Koen Petersen
Voorzitter van de vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking