Eerste Kamer der Staten-Generaal **I**

Vergaderjaar 2025-2026

30 821 Nationale veiligheid

F **VERSLAG VAN EEN NADER SCHRIFTELIJK OVERLEG**
Vastgesteld 23 juni 2026

De vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking[1] heeft nader schriftelijk overleg gevoerd met de minister van Defensie over Kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid**.** Bijgaand brengt de commissie hiervan verslag uit. Dit verslag bestaat uit:

- De uitgaande brief van 19 mei 2026.
- Een uitstelbericht van 17 juni 2026
- De antwoordbrief van 23 juni 2026.

De griffier van de vaste Commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking,

Van Luijk

[1] Samenstelling:
Van Apeldoorn (SP), Bakker-Klein (CDA), Van Ballekom (VVD), Beukering (Fractie-Beukering), Van Bijsterveld (JA21), Croll (D66), Crone (GroenLinks-PvdA), Dessing (FVD) (ondervoorzitter), Van Gasteren (Fractie-Van Gasteren), Goossen (BBB), Van der Goot (OPNL), Hartog (Volt), Huizinga-Heringa (CU) (ondervoorzitter), Karimi (GroenLinks-PvdA), Marquart Scholtz (BBB), Martens (GroenLinks-PvdA), Moonen (D66), Nicolaï (PvdD), Petersen (VVD) (voorzitter), Van Rooijen (50PLUS), Roovers (GroenLinks-PvdA), Van de Sanden (fractie-Van de Sanden), Van Strien (PVV), Thijssen (GroenLinks-PvdA), Van Toorenburg (CDA), Visseren-Hamakers (Fractie-Visseren-Hamakers), Vogels (VVD), De Vries (SGP), Walenkamp (Fractie-Walenkamp)

BRIEF VAN DE VOORZITTER VAN DE VASTE COMMISSIE VOOR BUITENLANDSE ZAKEN, DEFENSIE EN ONTWIKKELINGSSAMENWERKING

Aan de minister van Defensie

Den Haag, 19 mei 2026

De leden van de commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking (BDO) hebben met belangstelling kennisgenomen van uw brief[2] 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[3], 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
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[4] – 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

[2] Zie verslag nader schriftelijk overleg: *Kamerstukken I,* 2025-2026, 30821, E.
[3] 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.
[4] Idem, blz. 9.

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”.[5]
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[6] 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
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.

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

BRIEF VAN DE MINISTER VAN DEFENSIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

[5] Nationaal Coördinator Terrorismebestrijding en Veiligheid, ‘Cybersecuritybeeld Nederland in 2025. Riskante mix in een onvoorspelbare wereld’, november 2025, blz. 46.
[6] 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.

Den Haag, 17 juni 2026

Hierbij deel ik u mee dat beantwoording van de vragen gesteld door de leden van de PvdD-fractie (uw referentie: 181118) binnen de gestelde termijn niet haalbaar is gebleken en meer tijd vergt.

Uw Kamer zal de schriftelijke beantwoording zo spoedig mogelijk ontvangen.

De minister van Defensie,

Dilan Yeşilgöz-Zegerius

BRIEF VAN DE MINISTER VAN DEFENSIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 23 juni 2026

Bijgaand treft u de beantwoording van de nadere vragen van de leden van de Partij voor de Dieren-fractie inzake de kabinetsreactie op het AIV-advies ‘Hybride dreigingen en maatschappelijke weerbaarheid’. Deze vragen zijn ingezonden op 19 mei jl. met kenmerk 181118.

De minister van Defensie,

Dilan Yeşilgöz-Zegerius

Antwoorden op de schriftelijke vragen van de leden van de fractie van de Partij voor de Dieren inzake kabinetsreactie op het AIV-advies ‘Hybride dreigingen en maatschappelijke weerbaarheid’.

Ingezonden op 19 mei 2026

Vraag 1a
De leden van de fractie van Partij voor 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, 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.

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?

Het kabinet onderkent de structurele schaarste aan cyberspecialisten en de verwachte toename van de vraag, zowel bij Defensie als breder bij de overheid en private sector. Voldoende gekwalificeerd cyberpersoneel is een belangrijk thema binnen de Defensie Cyberstrategie. Defensie zet langs verschillende lijnen in op het werven, opleiden en behouden van eigen en nieuw personeel.

Defensie, andere overheidsdiensten en de veiligheidsdiensten putten uit dezelfde, beperkte arbeidsmarkt. Dat zorgt voor zowel onderlinge concurrentie als samenwerking. Het kabinet zet erop in om de samenwerking binnen de overheid te versterken, onder meer door kennisuitwisseling en het delen van schaarse expertise.

Over de feitelijke bezettingsgraad van de (cyber)personeelsbehoefte van Defensie worden geen publieke uitspraken gedaan. Inzicht in de mate waarin Defensie haar (cyber)personeelsbehoefte heeft ingevuld, geeft namelijk inzicht in de operationele gereedheid van deze capaciteit. Dergelijke informatie zou door een statelijke of criminele actor kunnen worden misbruikt.

Vraag 1b
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?

De Defensie Cyber Academy is weliswaar nog in oprichting, maar binnen de krijgsmacht worden ook nu al bekwame cyberspecialisten opgeleid en afgeleverd. Met de Defensie Cyber Academy wordt een gelaagde en modulaire aanpak verder uitgewerkt en gestandaardiseerd, zodat per functieprofiel effectiever en efficiënter kan worden opgeleid.

Over de mate waarin de Nederlandse cybercapaciteiten zich verhouden tot die van specifieke statelijke actoren doet het kabinet geen uitspraken, omdat dit inzicht zou geven in de operationele slagkracht. Wel kan worden gesteld dat Nederland beschikt over hoogwaardige cybercapaciteiten en dat doorlopend wordt geïnvesteerd om hiermee gelijke tred te houden met de snel ontwikkelende dreigingen.

Vraag 1c
Het Defensie Cyber Commando heeft – zo blijkt uit uw antwoord op vraag 1b in de beantwoording 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’?

De verwachting is dat de ingezette wervingsaanpak structureel zal bijdragen aan een betere en aantrekkelijke positionering van het Defensie Cyber Commando (DCC) op de arbeidsmarkt voor deze schaarse doelgroepen. De wervingsaanpak creëert de randvoorwaarden om de instroom structureel te vergroten en beter voorspelbaar te maken. Over de operationele invulling van de (cyber)personeelsbehoefte kunnen zoals eerder aangegeven geen publieke uitspraken worden gedaan.

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?

Het kabinet ziet op dit moment geen aanleiding om dergelijke wetgeving te laten onderzoeken. Zoals eerder benadrukt, streeft het kabinet ernaar zo lang mogelijk in een vrijwillig systeem te blijven. Voor de werving en het behoud van specialistische capaciteit is een benadering gericht op motivatie, autonomie en maatschappelijke betrokkenheid effectiever dan een verplichtend instrumentarium.

Ondanks de krappe arbeidsmarkt voor cyberspecialisten, zijn er tot op heden voldoende mogelijkheden om genoeg cybertalent aan te trekken. De eerdergenoemde wervingsaanpak draagt daaraan bij. Daarnaast beschikt de krijgsmacht over cyberreservisten die als flexibele schil kunnen worden ingezet en zet het in op de verdere uitbreiding hiervan.

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”. 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?

Het Cybersecuritybeeld Nederland 2025 (CSBN2025) wijst terecht op het gevaar van het gebruik van Large Language Models door actoren met een offensief cyberprogramma gericht tegen Nederlandse belangen. Zoals het CSBN2025 echter ook stelt, gaat het hierbij niet om een nieuwsoortige dreiging, maar om de versterking van bestaande dreigingen. Dit onderstreept de noodzaak van cybersecuritymaatregelen die ervoor zorgen dat de basis op orde is.

Er wordt daarom actief ingezet op de eigen cyberveiligheid in alle omstandigheden, zoals beschreven in de Defensie Cyberstrategie. Daarnaast zet Defensie in op capaciteit om eigen counter-AI-maatregelen te ontwikkelen, onder andere in samenwerking met kennispartners. Dit wordt als noodzakelijk geacht om verweer te kunnen bieden tegen vijandelijk gebruik van AI. Ook is het van belang dat Nederland zich blijft inzetten op het vergaren van inlichtingen omtrent de AI-capaciteiten van actoren met een offensief cyberprogramma gericht tegen de Nederlandse belangen, zodat tijdig de juiste tegenmaatregelen kunnen worden getroffen.

Ten slotte heb ik recent met waardering kennisgenomen van de inspanningen van de EU om samen met lidstaten te komen tot een actieplan voor AI & Cybersecurity. Nederland zal hier een actieve bijdrage aan leveren.

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

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?

Zoals het Nationaal Cyber Security Centrum (NCSC) actief uitdraagt, vormen AI-modellen als Mythos een reële dreiging voor de cyberveiligheid van Nederland. Het gaat daarmee niet om een nieuwe dreiging, maar de snelheid en de schaal waarop kwetsbaarheden kunnen worden gevonden en misbruikt nemen toe. Doordat AI-modellen steeds toegankelijker en goedkoper in gebruik zijn, komen deze capaciteiten binnen bereik van een groeiend aantal actoren. Het is dan ook aannemelijk dat dergelijke modellen in voorkomend geval tegen Nederlandse belangen zullen worden gebruikt.

Tegelijkertijd bieden dezelfde modellen ook mogelijkheden om onze cyberveiligheid juist te versterken, doordat kwetsbaarheden er sneller mee kunnen worden opgespoord en verholpen. Omdat publieke technische details op dit moment nog ontbreken, is de daadwerkelijke impact van modellen zoals Mythos niet met zekerheid vast te stellen.
Wel staat nu vast dat dergelijke modellen een structurele verschuiving betekenen in het tempo van zowel aanvallen als verdediging. Die ontwikkeling onderstreept de noodzaak om de algehele cyberweerbaarheid van Nederland te verhogen en hier adequaat op in te spelen.

Vraag 4b

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

De genoemde Europese wetten en richtlijnen dragen er actief aan bij om cyberrisico's te verkleinen, ook de risico's die generatieve AI als Mythos met zich mee kan brengen, en verkleinen zo de kans op ontwrichting. Geen enkel instrument biedt op zichzelf volledige zekerheid tegen ontwrichting door digitale dreigingen, maar deze wetten en richtlijnen vormen, in samenhang met voortdurende inzet op weerbaarheid, een belangrijk en groeiend fundament.

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?
Het Nationaal Cyber Security Centrum (NCSC) communiceert actief met organisaties in Nederland over de risico's van deze frontier AI-modellen. Daarbij is de 'basis op orde' het belangrijkste wat organisaties op dit moment kunnen doen. De komende periode gaat het NCSC, in samenwerking met andere partners, proactief over communiceren.

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

Ik deel het oordeel dat het dreigingslandschap complexer wordt. De verdeling van taken en bevoegdheden is echter wettelijk verankerd, waardoor het niet onduidelijk is welk overheidsorgaan bevoegd is om op te treden. Juist omdat dreigingen domeinoverschrijdend zijn, wordt er sterk ingezet op een integrale samenhangende aanpak, onder coördinatie van de NCTV.

Of de wetgeving op alle punten toereikend is, heeft doorlopend de aandacht. Waar nodig wordt het instrumentarium versterkt. Zo is de Kamer op 29 mei 2026 (Kamerstukken II 2025/26, 29 688, nr. 74) geïnformeerd over de voortgang modernisering staatsnoodrecht en wat gezien het dreigingsniveau de prioriteiten daarbij zijn.

In de koersbrief (Kamerstukken II 2025/26, 29 911, nr. 505), bij het op 26 mei jl. verzonden Dreigingsbeeld Ondermijning Nederland (DON), wordt onderschreven dat de huidige integrale aanpak van ondermijning op de juiste punten ingrijpt en dat deze aanpak met kracht wordt doorgezet en op punten wordt geïntensiveerd of aangescherpt. Daarnaast stuurt het kabinet met het Rijksbrede Responskader tegen statelijke dreigingen en de maatschappijbrede verhoging van de

weerbaarheid tegen militaire en hybride dreigingen ook op de integrale aanpak van deze dreigingen.

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

De inlichtingendiensten zijn onder de Wiv 2017 bevoegd om onder bepaalde omstandigheden bepaalde maatregelen te bevorderen of te treffen ter bescherming van de belangen die de desbetreffende inlichtingendienst behartigt. Dit kunnen ook maatregelen in het cyberdomein zijn.

Dergelijke maatregelen zijn met waarborgen omkleed. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) houdt toezicht op de rechtmatigheid van de door de MIVD uitgevoerde maatregelen. Iedere verstorende cyberactiviteit moet daarbij voldoen aan de wettelijke vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit, en aan geldende internationaalrechtelijke kaders.

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?
Zoals gesteld in de beantwoordingsbrief van 9 maart 2026, verschillen de mandaten en verantwoordelijkheden van de veiligheidsdiensten en de krijgsmacht. Bepalend is in de eerste plaats de aard en ernst van de aanval: indien een cyberaanval op Nederland de drempel overschrijdt van een (zich manifesterende) dreiging voor de nationale veiligheid, bijvoorbeeld door het uitvallen van vitale sectoren, dan kan de inzet van de inlichtingen- en veiligheidsdiensten en de krijgsmacht in beeld komen.
Zo stelt de Wiv 2017 de inlichtingendiensten onder meer in staat tot het verrichten van attributieonderzoek en tot handelend optreden. Een voorbeeld van het laatste is het offline (laten) halen van ICT-infrastructuur die onderdeel is van aanvalsinfrastructuur of misbruikt wordt voor digitale spionage of sabotage. De Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten (CTIVD) is bevoegd op dergelijke activiteiten toezicht te houden om te toetsen of de bevoegdheid door de MIVD rechtmatig wordt uitgevoerd. Zo zal iedere verstorende cyberactiviteit moeten voldoen aan de wettelijke vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.
Naast het optreden door de inlichtingendiensten kan Nederland ook met de krijgsmacht reageren (Kamerstukken II 2021/22, 26 643, nr. 785). Zo kan het Defensie Cyber Commando (DCC) in laatste instantie een tegenaanval uitvoeren om een vijandelijke actie af te wenden of om een essentieel belang van de staat te beschermen.
Wat een staat mag doen onder het internationaal recht tegen een cyberaanval zal sterk afhankelijk zijn van de omstandigheden en vergt derhalve per geval een regeringsbesluit.