Eerste Kamer der Staten-Generaal

Minister van Defensie
De heer R.P. Brekelmans
Postbus 20701
2500 ES Den Haag

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

telefoon 070 312 92 00
fax 070 312 93 90

e-mail postbus@eerstekamer.nl
internet www.eerstekamer.nl

datum *27 januari 2026*
betreft *Nadere vragen inzake kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid'*
ons kenmerk *179666*

Geachte heer Brekelmans,

De leden van de commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingshulp (BDO) hebben met belangstelling kennisgenomen van uw brief[1] van 2 december 2025 in beantwoording op de brief met vragen van de commissie van 1 oktober 2025 over de kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid'. De leden van de fractie van de **PvdD** en de **Fractie-Van de Sanden** 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 de PvdD maken zich zorgen of er wel voldoende wordt toegewerkt naar gedegen opleidingen van cyber-specialisten die voor Defensie en voor de inlichtingen- en veiligheidsdiensten kunnen werken. In het antwoord op vraag 1c verwijst u naar het functioneren van het CWTC en het doorontwikkelen daarvan naar een 'Cyber Academy'. Uit de informatie die daarover te vinden is, maken deze leden op dat het niveau laag is en dat een 'Cyber Academy' die specialisten aflevert die zich kunnen meten met hackers en cyber-specialisten uit Rusland en China nog in de kinderschoenen staat. Uit de Defensiekrant van maart 2023 blijkt dat over de eerste lichting die toen de opleiding voltooide, werd gezegd dat zij niet 'vak'-bekwaam zijn maar slechts 'start'-bekwaam. CWTC-teamleider kapitein Jeroen Oosterbos: "Je moet de CTO echt als een opstap zien. Na de opleiding ben je start-, niet vakbekwaam."[2]

Vraag 1a
Kunt u aangeven op welke termijn opleidingen beschikbaar zullen zijn die specialisten op voldoende niveau zullen kunnen afleveren?

[1] *Kamerstukken I,* 2024-2025, 30821, C.
[2] Defensiekrant, 'Eerste lichting Cyber Technische Opleiding zwaait af', defensiekrant 12, https://magazines.defensie.nl/defensiekrant/2023/12/03_cto_12.

Vraag 1b
Welke stappen worden ondernomen om personen die op dit moment al in het veld van de cybersecurity werkzaam zijn, over te halen om voor Defensie of voor de inlichtingen- en veiligheidsdiensten te werken?

Vraag 1c
Is het kabinet bereid om budget beschikbaar te stellen waarmee zulke personen kunnen worden overgehaald om over te stappen naar Defensie of een inlichtingen- en veiligheidsdienst?

Vraag 1d
Hebben Defensie en de inlichtingen- en veiligheidsdiensten contacten met de wereld van zogeheten ethische hackers die erop gericht zijn hen bij het werk van Defensie en inlichtingen- en veiligheidsdiensten te betrekken om de samenleving te beschermen tegen cyberaanvallen van statelijke actoren?

Vraag 2
In uw antwoord op vraag 1d stelt u dat er reservisten zijn die in hun civiele baan als ethisch hacker werken en in opleidingen betrokken kunnen worden.

Vraag 2a
Om hoeveel personen gaat dat?

Vraag 2b
Welke stappen kunnen worden ondernomen om die groep uit te breiden?
Zijn er contacten met HBO- of andere beroepsopleidingen gericht op werving van (toekomstige) cyberspecialisten voor Defensie en de inlichtingen- en veiligheidsdiensten?

Vraag 2c
In reclamefilmpjes voor Defensie komen heel andere ‘spannende’ taakuitoefeningen aan de orde dan het werken op cybergebied. Deelt u het oordeel van de leden van de PvdD-fractie dat werving van personen die voor cyberweerbaarheid kunnen worden ingezet, meer prioriteit moet krijgen?

Vraag 3
In uw antwoord op vraag 1a verwijst u naar de Motie-Erkens en naar de jaarverslagen van de inlichtingen- en veiligheidsdiensten.

Vraag 3a
Zien deze leden het goed dat niet alle cyberaanvallen waarvan die diensten kennis hebben gehad, in de jaarverslagen worden genoemd of met de Kamer worden gedeeld?

Vraag 3b
Wordt het aan het beleid of inzicht van die diensten overgelaten of en zo ja welke voorvallen openbaar worden gemaakt?

Vraag 3c
De vraag doet zich voor of een volledige transparantie over alle gevallen van cyber-aanvallen op bedrijven, instellingen en voorzieningen niet méér zou bijdragen aan het vergroten van de weerbaarheid van de samenleving dan het 'geheim' houden van bepaalde voorvallen. En of dat ook niet zou gelden voor alle eventuele tegenmaatregelen die tegen zulke aanvallen zijn ondernomen. Is er onderzoek verricht dat op die vraag betrekking heeft? Zo ja, welke onderzoeken zijn dat en wat zijn de bevindingen? Zo nee, bent u bereid om zulk onderzoek te laten uitvoeren en de Kamer van de resultaten daarvan op de hoogte te stellen?

Vraag 4
In uw antwoord op de vraag van de leden van de PvdD-fractie over eventuele 'tegenmaatregelen' tegen cyberaanvallen, wijst u op bevoegdheden van de inlichtingen- en veiligheidsdiensten die op dit moment naar Nederlandse wetgeving reeds bestaan.

Vraag 4a
Kunt u nader aangeven welke wettelijke voorschriften in een niet-oorlogssituatie tot een tegenaanval mogen leiden en feitelijke voorbeelden geven van zo'n geoorloofde aanval?

Vraag 4b
Zijn de inlichtingen- en veiligheidsdiensten tot een tegenaanval bevoegd zonder dat daartoe een kabinetsbesluit wordt genomen?

Vraag 5
U verwijst in uw antwoord naar uw brief van 13 augustus 2019[3] waarin u ingaat op het advies Digitale oorlogsvoering van de AIV en de CAVV van 2011.

Vraag 5a
Acht u dat advies nog voldoende actueel? Bent u bereid om die advieslichamen een nieuw advies te vragen in het licht van de actuele situatie die niet meer overeenstemt met die van bijna 15 jaar geleden?

Vraag 5b
In de bijlage van uw brief schrijft u "Zoals het kabinet meerdere malen heeft aangegeven en consequent uitdraagt, is het internationaal recht van toepassing op het cyberdomein. Dit wordt ook internationaal erkend."
Past die stelling nog in de huidige tijd, met name gelet op standpunten van de VS over eventuele beperkingen die uit internationaal recht voorvloeien voor verhoudingen tussen staten?

Vraag 5c
U schrijft ook in die bijlage: "Volgens sommige landen en juristen vormt het soevereiniteitsbeginsel niet een zelfstandige regel van internationaal recht".

[3] *Kamerstukken II,* 2018-2019, 33694/ 26643 nr. 47.

Welke landen nemen een ander standpunt in dan Nederland?

Vraag 6
Als Rusland met een cyberaanval erin slaagt om door verstoring van computers en luchtverkeergeleiding Schiphol 'plat te leggen' of de Rotterdamse haven 'plat te leggen' door verstoring van digitaal verkeer dat de logistiek ondersteunt, ziet u dat dan als geweldgebruik en een inbreuk op de soevereiniteit van Nederland?

Vraag 7
Vanuit Nederland wordt tegen als tegenmaatregel tegen een cyberaanval door Rusland die grote impact heeft, als volgt gehandeld:
a. de stroomvoorziening in Sint-Petersburg wordt met een cyberaanval gedurende een week onderbroken;
b. het internet in delen van Rusland wordt gedurende met een cyberaanval een week plat gelegd.

Vraag 7a
Kan zo'n tegenaanval gerechtvaardigd zijn?

Vraag 7b
Mogen zulke aanvallen worden gerealiseerd door de MIVD of door de Nederlandse krijgsmacht?

Vraag 7c
Is het naar internationaal recht verplicht om Rusland vooraf te waarschuwen?

Vraag 7d
Vindt u dat de voorschriften die in zulke gevallen door Nederland in acht moeten worden genomen, voldoende kenbaar en duidelijk?

Vragen en opmerkingen van het lid van de Fractie-Van de Sanden
1. Wettelijke kaders
Het lid van de Fractie-Van de Sanden vraagt of u kunt toelichten hoe alle genoemde cybermaatregelen en tegenaanvallen binnen de bestaande nationale wetgeving en internationale verdragen passen, en hoe wordt geborgd dat er geen schending van grondrechten plaatsvindt.

2. Transparantie naar de Kamer
Op welke wijze wordt de Kamer tijdig en adequaat geïnformeerd over cyberoperaties en tegenmaatregelen, zonder operationele geheimhouding te schenden?

3. Proportionaliteit van maatregelen
Hoe beoordeelt de regering de proportionaliteit van digitale tegenaanvallen en andere preventieve maatregelen, zodat burgers, bedrijven en organisaties niet onevenredig worden getroffen?

4. Rechtsbescherming van betrokkenen
Welke mechanismen bestaan om de rechtsbescherming van burgers, ambtenaren en bedrijven te waarborgen die mogelijk gevolgen ondervinden van cybermaatregelen?

5. Controle en toezicht
Welke vormen van intern en extern toezicht zijn er op de uitvoering van cyberoperaties en maatregelen tegen hybride dreigingen, en hoe wordt verantwoording afgelegd aan de Kamer?

6. Precedentwerking
Hoe voorkomt de regering dat toegepaste cybermaatregelen precedenten scheppen die de scheiding der machten of democratische besluitvorming kunnen uithollen?

7. Evaluatie van effectiviteit
Welke evaluatie- en monitoringsprocedures zijn ingericht om te beoordelen of de maatregelen effectief én rechtsstatelijk verantwoord zijn?

8. Privacy en gegevensbescherming
Kunt u toelichten welke stappen worden genomen om privacy en gegevensbescherming te waarborgen bij het verzamelen en verwerken van gegevens in het kader van hybride dreigingen?

9. Internationale samenwerking
Hoe wordt gewaarborgd dat internationale samenwerking en uitwisseling van informatie op het gebied van cyberveiligheid niet leidt tot schending van nationale rechtsstatelijke normen?

10. Rapportage over uitvoering
Kunt u concreet aangeven wie, hoe en wanneer rapporteert aan de Kamer over de uitvoering van deze maatregelen, zodat de democratische controle volledig wordt geborgd?

De leden van de vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingshulp (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 Ontwikkelingshulp