Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2025–2026

30 821 Nationale veiligheid

E

VERSLAG VAN EEN NADER SCHRIFTELIJK OVERLEG

Vastgesteld 26 maart 2026

De vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking[1] heeft nader schriftelijk overleg gevoerd met de Minister van Defensie over **de 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 27 januari 2026.
- Een uitstelbericht van 9 maart 2026
- De antwoordbrief van 23 maart 2026.

De griffier van de vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingssamenwerking,
Van Luijk

[1] Samenstelling:
Van Apeldoorn (SP), Van Ballekom (VVD), Beukering (Fractie-Beukering), Van Bijsterveld (JA21), Croll (D66), Crone (GroenLinks-PvdA), Dessing (FVD) (ondervoorzitter), Van Gasteren (BBB), 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), Prins (CDA), 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)

kst-30821-E
ISSN 0921 - 7371
's-Gravenhage 2026

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

Aan de Minister van Defensie

Den Haag, 27 januari 2026

De leden van de commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingshulp (BDO) hebben met belangstelling kennisgenomen van uw brief[2] 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 cyberspecialisten 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 cyberspecialisten 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.»[3]

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

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

---

[2] *Kamerstukken I*, 2024–2025, 30 821, C.
[3] Defensiekrant, «Eerste lichting Cyber Technische Opleiding zwaait af», defensiekrant 12, https://magazines.defensie.nl/defensiekrant/2023/12/03_cto_12.

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[4] 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 adviescollegia 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».
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?

---

[4] *Kamerstukken II*, 2018–2019, 33 694/26 643, nr. 47.

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.

Voorzitter van de vaste commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingshulp,
K. Petersen

BRIEF VAN DE MINISTER VAN DEFENSIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 9 maart 2026

Hierbij deel ik u mee dat beantwoording van de vragen gesteld door de leden van de fractie van de PvdD en de Fractie-Van de Sanden [179666] binnen de gestelde termijn niet haalbaar is gebleken. De beantwoording heeft met het oog op een zorgvuldige en volledige beantwoording meer tijd nodig.

Uw Kamer zal de schriftelijke beantwoording zo spoedig mogelijk ontvangen.

De Minister van Defensie,
D. Yeşilgöz-Zegerius

BRIEF VAN DE MINISTER VAN DEFENSIE

Aan de Voorzitter van de Eerste Kamer der Staten-Generaal

Den Haag, 23 maart 2026

Hierbij ontvangt u de antwoorden op de inbreng van de commissie voor Buitenlandse Zaken, Defensie en Ontwikkelingshulp (BDO) inzake de kabinetsreactie van 6 december 2024 op het AIV-advies «Hybride dreigingen en maatschappelijke weerbaarheid». De vragen en opmerkingen van de commissie werden ingezonden op 28 januari 2026 met kenmerk 179666.

De Minister van Defensie,
D. Yeşilgöz-Zegerius

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 cyberspecialisten 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 cyberspecialisten 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: «Je moet de CTO echt als een opstap zien. Na de opleiding ben je start-, niet vakbekwaam.»

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

Het Cyber Warfare Training Center (CWTC), onderdeel van het Defensie Cyber Commando (DCC) is verantwoordelijk voor het startbekwaam maken van instromend cyberpersoneel. Vervolgens worden deze specialisten binnen hun eenheden gereedgesteld voor inzet in hun specifieke functie. Door middel van aanvullende trainingen en oefeningen wordt hier de operationele gereedheid verder verhoogd.

Defensie werkt continu aan de verbetering van opleidingstrajecten. Dit geldt zeker voor het snel ontwikkelende cyberdomein. Hiertoe werkt Defensie aan de oprichting van een Cyber Academy bij het DCC. Binnen deze Cyber Academy zal bijvoorbeeld worden gewerkt met een assessmentcenter om het instapniveau en het ontwikkelpotentieel van kandidaten vast te stellen, zodat zij niet méér of langer worden opgeleid dan nodig is.

Op dit moment worden in een aantal trajecten specialisten al volgens deze nieuwe opzet tot een inzetbaar startniveau gebracht, waarna zij via vervolgmodules, praktijktraining en operationele ervaring doorgroeien naar een hoger vakbekwaamheidsniveau. De komende jaren wordt deze gelaagde en modulaire aanpak verder uitgewerkt en gestandaardiseerd binnen de toekomstige Cyber Academy, zodat per functieprofiel zo effectief en efficiënt mogelijk kan worden opgeleid.

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?

Werving en selectie van cyberspecialisten vindt plaats via het Dienstencentrum Personeel & Logistiek (DCPL). Gelijk aan andere specialismes binnen Defensie, bestaat er schaarste op het gebied van cyberspecialisten. Volgens het adagium «binden, boeien & behouden» tracht Defensie een zo aantrekkelijk mogelijke werkgever te zijn die voldoende perspectief biedt om cyberspecialisten aan te kunnen trekken en te behouden. Zo richt het DCC zich met een eigen wervingsplan specifiek op deze doelgroep, bijvoorbeeld door middel van gerichte arbeidsmarktcommunicatie en deelname aan beurzen en symposia.

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?

Zoals in eerdere beantwoording wordt gesteld tracht Defensie een zo aantrekkelijk mogelijke werkgever te zijn die voldoende perspectief biedt om cyberspecialisten aan te kunnen trekken en te behouden. De middelen voor werving zijn ingebed in de bestaande begroting.

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?

Defensie beschikt over cybersecurityspecialisten als onderdeel van de cyberreservisteneenheid. Deze specialisten ondersteunen de Nederlandse strijdkrachten als doelmatige, innovatieve en flexibele capaciteit bij het behalen van militaire effecten in en via het cyberdomein. Zoals in de vorige beantwoording van 2 december 2025 is aangegeven, is er ook binnen de cyberopleidingen van Defensie expertise over ethisch hacken aanwezig.

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?

We doen vanwege veiligheidsredenen geen uitspraken over aantallen cyberspecialisten die in dienst zijn van Defensie.

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?

Defensie voert een Defensiebreed innovatief personeelsbeleid om schaars en specialistisch cyberpersoneel te vinden, binden, boeien en inspireren. Dat doet Defensie onder meer door strategische partnerschappen met bedrijven, scholen en andere kennisinstellingen op het gebied van trainen en opleiden, en detacheringen aan te gaan.

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?

Zoals in de Defensie Cyberstrategie is beschreven is voldoende kwalitatief cyberpersoneel een essentiële randvoorwaarde om de taken van Defensie in het cyberdomein uit te voeren. Zoals in antwoord 1b is aangegeven, streeft Defensie ernaar een zo aantrekkelijk mogelijk werkgever te zijn die voldoende perspectief kan bieden om cyberspecialisten aan te trekken en

te behouden. De werving van voldoende cyberspecialisten heeft dus prioriteit binnen Defensie.
Zo zal nog dit jaar een specifieke wervingsvideo voor het cyberdomein deel uitmaken van de Defensiebrede wervingscampagne.

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?

Over de werkzaamheden en het kennisniveau van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD) kan in de openbaarheid geen uitspraak worden gedaan. Uw Kamer wordt over de vertrouwelijke aspecten van de werkzaamheden van de diensten via de geëigende kanalen geïnformeerd. Conform motie-Erkens (*Kamerstukken II* 2023/24, 36 410 X, nr. 46), worden zoveel mogelijk cyberaanvallen en bijhorende technische werkwijzen openbaar gemaakt om het bewustzijn en de weerbaarheid in Nederland op het gebied van cyberveiligheid te vergroten.

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

Conform motie Erkens worden cyberaanvallen zo veel mogelijk openbaar gemaakt om het bewustzijn en de weerbaarheid in Nederland op het gebied van cyberveiligheid te vergroten en handelingsperspectief tegen de dreiging te bieden. In het kader van een goede taakuitvoering zijn de diensten bevoegd om inlichtingen(analyses) te verstrekken aan ieder die dat aangaat, waaronder het publiek (Wiv 2017, art.62). Bij publieke attributie van cyberaanvallen is bronbescherming een primaire afweging, daarnaast kan het diplomatieke consequenties of andere effecten met zich meebrengen. Derhalve vereist een dergelijke attributie een kabinetsbesluit.

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?

Nee, volledige transparantie is in het geval van cyberaanvallen niet altijd mogelijk of wenselijk.

Het kan voorkomen dat bepaalde informatie omtrent cyberaanvallen voortkomt uit een gevoelige bron waardoor desbetreffende informatie niet openbaar kan worden gemaakt. Daarnaast is attributie van cyberaanvallen, dus het vaststellen aan wie een aanval kan worden toegeschreven, niet altijd (technisch) mogelijk.

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.

Op grond van artikel 73 van de Wet op de inlichtingen- en veiligheidsdiensten 2017 zijn de AIVD en MIVD bevoegd tot het bevorderen of treffen van maatregelen ter bescherming van de door de diensten te behartigen belangen, al dan niet met een technisch hulpmiddel.

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?

Indien een dergelijke aanval 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 AIVD en/of MIVD in beeld komen. Zo stelt de Wiv 2017 de diensten 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.

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

Het bevorderen of treffen van maatregelen ter bescherming van de door de diensten te behartigen belangen, zoals neergelegd in artikel 73 van de Wiv 2017, is slechts toegestaan indien door of namens de betrokken Minister daarvoor toestemming is verleend. Indien sprake is van een aanval die wordt gezien als een geweldshandeling, dan wordt verwezen naar het antwoord op vraag 6.

Vraag 5
U verwijst in uw antwoord naar uw brief van 13 augustus 2019 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 adviescolleges een nieuw advies te vragen in het licht van de actuele situatie die niet meer overeenstemt met die van bijna 15 jaar geleden?

Volgens het kabinet is het op dit moment niet nodig de AIV en CAVV te vragen een nieuw advies over dit onderwerp op te stellen.

Het kabinetsstandpunt over de toepassing van het internationaal recht in het cyberdomein is verwoord in de bijlage *Kamerstukken II* 2018/19, 33 694, nr. 47 uit 2019. Dit stuk is dus van recentere datum en biedt volgens het kabinet voldoende handvatten binnen de context van cyberoperaties in de huidige geopolitieke realiteit.

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?

Ja, zoals omschreven in de Internationale Cyberstrategie 2023–2028 is het voor het kabinet kraakhelder dat het internationaal recht en mensenrechten zowel online als offline gelden. Dit standpunt wordt ook onderschreven door de Verenigde Naties. Dat bepaalde landen een andere visie op het internationaal recht uitdragen, doet hier niet aan af.

Vraag 5c
U schrijft ook in die bijlage: «Volgens sommige landen en juristen vormt het soevereiniteitsbeginsel niet een zelfstandige regel van internationaal recht». Welke landen nemen een ander standpunt in dan Nederland?

Het kabinet acht het niet passend om in te gaan op de juridische opvattingen van andere staten.

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?

Dergelijke aanvallen kunnen, afhankelijk van de schaal en impact, gezien worden als geweldgebruik en een inbreuk op de soevereiniteit van Nederland. Zo kan, in het ergste geval, een cyberaanval dermate impact hebben dat het aanleiding kan geven om artikel 5 van de NAVO te activeren. Dit geldt ook voor Art. 42.7 van het Verdrag betreffende de Europese Unie.

Vraag 7
Vanuit Nederland wordt 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?

Het wordt niet opportuun geacht om uitspraken te doen over hypothetische scenario's.

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

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 diensten 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 Inlichtingen- en Veiligheidsdiensten kan Nederland ook met de krijgsmacht reageren (*Kamerstukken II* 2021/22, 26 643, nr. 785). Zo kan het Defensie Cyber Commando (DCC) *ad ultimo* 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.

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

Dat is afhankelijk van de specifieke omstandigheden van het geval. Het wordt daarom niet opportuun geacht om uitspraken te doen over hypothetische scenario's.

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

Dat is afhankelijk van de specifieke omstandigheden van het geval. Het wordt daarom niet opportuun geacht om uitspraken te doen over hypothetische scenario's.

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.

Een uitputtend overzicht van alle maatregelen die worden genomen om cyberaanvallen en digitale desinformatie te bestrijden is niet te geven. Veel vijandelijke activiteiten in cyberspace zijn context specifiek en vergen derhalve specifieke tegenmaatregelen.

Voor zover het cybermaatregelen betreffen in de zin van cyberoperaties die worden uitgevoerd door de MIVD of de krijgsmacht, gelden daarvoor de vigerende nationaal- en internationaalrechtelijke kaders.

Waar het de activiteiten betreft die door de MIVD worden uitgevoerd, zoals verstorende cyberactiviteiten, geldt de Wiv 2017. De CTIVD houdt toezicht op de rechtmatigheid van het handelen van de MIVD en de AIVD. Zo zal ook iedere verstorende cyberactiviteit moeten voldoen aan de wettelijke vereisten van noodzakelijkheid, proportionaliteit en subsidiariteit.

Voor zover het inzet van de krijgsmacht betreft, is een regeringsbesluit vereist. Het parlement wordt vooraf geïnformeerd in geval van inzet of ter beschikking stellen van de krijgsmacht in het kader van handhaving of bevordering van de internationale rechtsorde of humanitaire hulpverlening in het kader van een gewapend conflict (artikel 100, eerste lid, van de Grondwet). Als «dwingende redenen» het vooraf informeren van het parlement niet mogelijk maken, wordt het parlement zo spoedig mogelijk alsnog geïnformeerd (artikel 100, tweede lid, van de Grondwet). De vaste procedures voor de toepassing hiervan worden gevolgd.

Zoals is toegelicht in de brief van 2 december jl., is het internationaal recht van toepassing in het cyberdomein. Bij het uitvoeren van cyberoperaties moet iedere staat zich dan ook houden aan het internationaal recht. Voor militaire cyberoperaties gelden dezelfde kaders, afspraken en toetsing als voor andere militaire operaties. Controle en toezicht op militaire operaties zijn op verschillende niveaus geborgd, variërend van democratische controle door het parlement tot externe en interne toezichthouders en interne juridische advisering.

2. Transparantie naar de Kamer

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

Indien daar aanleiding toe is, wordt het parlement via de geëigende kanalen geïnformeerd.

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?

Zie antwoord op vraag 1 en antwoord 7b van de PvdD fractie.

4. Rechtsbescherming van betrokkenen

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

In principe geldt dat de gangbare mechanismen omtrent rechtsbescherming van toepassing zijn, ook voor gevolgen uit eventuele getroffen cybermaatregelen.

Zie ook antwoord op vraag 8.

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?

Zie antwoorden op vragen 1 en 4.

6. Precedentwerking

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

Zie ook antwoord op vraag 1.

Daarin speelt parlementaire controle een belangrijke rol. Bij het toepassen van zogenoemde cybermaatregelen, dient uiteraard ook de Grondwet te worden nageleefd, waarin de waarborgen voor grondrechten en de democratische rechtsstaat zijn vastgelegd.

7. Evaluatie van effectiviteit

Welke evaluatie- en monitoringsprocedures zijn ingericht om te beoordelen of de maatregelen effectief én rechtsstatelijk verantwoord zijn?

Een uitputtend overzicht van alle maatregelen die worden genomen om cyberaanvallen en digitale desinformatie te bestrijden is niet te geven.

Zo verre het cybermaatregelen betreffen in de zin van cyberoperaties die worden uitgevoerd door de MIVD of de krijgsmacht, gelden daarvoor nationale en internationale wetgeving en verdragen. Hiervoor gelden de controlemechanismen zoals beschreven in het antwoord op vraag 1.

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?

Voor zover gegevens in het kader van hybride dreigingen worden verzameld door de inlichtingen- en veiligheidsdiensten gelden daarvoor de regels rondom de verwerking van persoonsgegevens van de Wiv 2017.

Voor zover maatregelen worden uitgevoerd door de krijgsmacht gelden de kaders van de AVG, of de Regeling Gegevensverwerking Militaire Operaties in geval van inzet.

Ook voor overige delen van de overheid gelden voor het uitvoeren van maatregelen de kaders van de AVG. Dit betekent dat bij het verzamelen en verwerken van persoonsgegevens in het kader van hybride dreigingen waarborgen zoals rechtmatigheid, dataminimalisatie, bewaartermijnen en informatiebeveiliging in acht worden genomen.

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?

Voorafgaand aan het aangaan van een samenwerkingsrelatie met een buitenlandse inlichtingen- en veiligheidsdienst wordt door de diensten een zogenoemde wegingsnotitie opgesteld. In de wegingsnotitie wordt de buitenlandse dienst onder andere gewogen aan de criteria «respect voor de mensenrechten» en het «geboden niveau van gegevensbescherming». Op basis van de weging kan worden samengewerkt onder standaard, aanvullende of strikte voorwaarden. Daarnaast wordt voor iedere

gegevensverstrekking op het daartoe geëigende niveau toestemming gevraagd en wordt getoetst aan eventueel onderkende risico's. Aan de verstrekking van gegevens worden ook voorwaarden verbonden, zogenoemde *disclaimers*. De CTIVD houdt hier toezicht op en heeft hierover de toezichtsrapporten nr. 60 en nr. 73 gepubliceerd.[5]

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?

Zo verre het cybermaatregelen betreffen in de zin van cyberoperaties die worden uitgevoerd door de MIVD of de krijgsmacht, zie antwoord op vraag 1 en op vraag 3a van de PvdD-fractie.

Voor cybermaatregelen zoals gedefinieerd in de Defensie Cyberstrategie 2025 geldt dat deze maatregelen en de voortgangsbewaking ervan de integrale beleidscyclus en het reguliere plannings- en investeringsproces volgen. De effectiviteit van cyberstrategie als geheel wordt bewaakt door iedere twee jaar de strategie en het onderliggende beleid en plannen te evalueren, en indien nodig bij te stellen.

[5] *Kamerstukken II* 2018/19, 29 924, nr. 177 en *Kamerstukken II* 2021/22, 29 924, nr. 221.