Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Eerste Kamer
der Staten-Generaal
Kazernestraat 52
2500 EA Den Haag

Ministerie van Defensie
Plein 4
MPC 58 B
Postbus 20701
2500 ES Den Haag
www.defensie.nl

Onze referentie
D2025-004783
MINDEF20250042047

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

Datum	26 november 2025
Betreft	Vragen inzake kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid’

Geachte voorzitter,

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 30 september 2025 met kenmerk 178289.

Hoogachtend,

DE MINISTER VAN DEFENSIE

Ruben Brekelmans

DE MNISTER VAN BUITENLANDSE ZAKEN

D.M. van Weel

DE MNISTER VAN BINNENLANDSE ZAKEN
EN KONIKRIJKSRELATIES

F. Rijkaart

Vragen en opmerkingen van de leden van de Partij voor de Dieren-fractie

De leden van de fractie van de Partij voor de Dieren wensen de volgende vragen te stellen en verzoeken u de (sub)vragen afzonderlijk te beantwoorden.

Vraag 1

Onderdeel van hybride aanvallen zijn cyberaanvallen en digitale desinformatie door statelijke actoren, zo constateren de leden van de Partij voor de Dieren-fractie. De aanbevelingen 1 t/m 5 hebben onder meer daarop betrekking en worden door het kabinet onderschreven. De inlichtingen- en veiligheidsdiensten hebben zicht op cyberaanvallen en digitale desinformatie door statelijke actoren.

Vraag 1a

Bent u bereid om de Kamer vertrouwelijk regelmatig door die diensten inzicht te laten geven in geconstateerde cyberaanvallen en digitale desinformatie door statelijke actoren?

De inlichtingen- en veiligheidsdiensten beschrijven in hun openbare jaarverslagen de dreigingen tegen de nationale veiligheidsbelangen, waaronder digitale dreigingen op het gebied van cyber en desinformatie. Indien daar aanleiding toe is, informeren de inlichtingen- en veiligheidsdiensten het parlement via de daarvoor bestemde kanalen.

Daarnaast worden, conform de motie Erkens (Kamerstuk 36 410 X nr. 46), cyberaanvallen en bijhorende technische werkwijzen zo veel mogelijk openbaar gemaakt om het bewustzijn en de weerbaarheid in Nederland op het gebied van cyberveiligheid te vergroten.

Vraag 1b

Kunt u een overzicht verschaffen van alle maatregelen die worden genomen om cyberaanvallen en digitale desinformatie door statelijke actoren te bestrijden en te voorkomen, en wie daartoe bevoegd zijn?

Aangezien het tegengaan van cyberaanvallen en digitale desinformatie deel uitmaakt van al het cyberbeleid, cyberactiviteiten en cyberrapportages van de overheid, is een uitputtend overzicht hiervan niet te geven. Enkele voorbeelden van cyberbeleid, -activiteiten en -rapportages zijn de Nederlandse Cybersecuritystrategie, de Internationale Cyberstrategie 2023-2028, de implementatie van de NIS2-richtlijn in de Cyberbeveiligingswet, de activiteiten van het Nationaal Cyber Security Center, de Defensie Cyberstrategie, de Rijksbrede strategie voor de effectieve aanpak van desinformatie en de publiekscampagnes om de bewustwording rondom digitale risico’s onder burgers te vergroten.

Ook treden de inlichtingen- en veiligheidsdiensten waar mogelijk vaker naar buiten met informatie over ‘onzichtbare dreigingen’ om inzage te geven in de aard van de problematiek en handelingsperspectief te bieden ter bevordering van de digitale weerbaarheid.

Vraag 1c

Welke maatregelen zijn of worden getroffen om militairen, medewerkers van de inlichtingen- en veiligheidsdiensten of ander overheidspersoneel op te leiden tot deskundigen die in staat zijn cyberaanvallen te bestrijden of een cybertegenaanval uit te voeren?

Het is van belang dat Nederland beschikt over voldoende gekwalificeerd cyberpersoneel om slagkracht te kunnen leveren in het cyberdomein. Binnen de verschillende departementen die zich bezighouden met operaties in het cyberdomein bestaan unieke mogelijkheden tot verbreding en

verdieping van kennis en kunde. De bestaande intensieve samenwerking tussen departementen en diensten verhoogt het cyberkennisniveau van overheidspersoneel.

Ook de herziene Defensie Cyberstrategie, die recent naar het parlement is gestuurd (Kamerstuk 26 643 nr. 1422), onderkent de noodzaak van voldoende gekwalificeerd cyberpersoneel als randvoorwaarde voor een slagvaardige Defensieorganisatie in het cyberdomein. Defensie zet in op de integratie van cyber(kennis) op alle niveaus van trainen en opleiden en gerichte opleidingen voor operationele functies. Binnen Defensie speelt het Cyber Warfare & Training Centre (CWTC) van het Defensie Cyber Commando als centraal opleidings- en trainingscentrum op het gebied van militaire cyber een cruciale rol in de opleiding en training van defensiepersoneel. Het CWTC wordt doorontwikkeld tot een Cyber Academy, die het volledige palet aan opleidingen gaat geven, zoals aangekondigd in de Defensienota 2024.

Vraag 1d

Worden zogeheten ethische hackers betrokken bij zulke opleidingen?

Cyberopleidingen worden verzorgd door zowel Defensiepersoneel als externe partijen. In beide gevallen is daarbij, waar relevant, ook expertise over ethisch hacken aanwezig. Daarnaast worden er ook opleidingen door cyberreservisten gegeven, die in sommige gevallen in hun civiele baan een aanstelling als ethisch hacker hebben.

Vraag 1e

Is een wijziging van de Wet op de inlichtingen- en veiligheidsdiensten (Wiv) nodig om de diensten (verdere) bevoegdheden te geven om cyberaanvallen te verstoren? Zo ja, welke voorstellen daartoe worden ontwikkeld?

De Wiv 2017 biedt reeds een grondslag voor de diensten om cyberaanvallen te verstoren. Tegelijkertijd werkt het kabinet nu aan een brede herziening van de Wiv 2017 die beter recht doet aan (het mitigeren van) de digitale bedreigingen van de nationale veiligheid.

Versterking van de slagkracht van de diensten, waaronder in het cyberdomein, en een toekomstbestendig wettelijk kader zijn een belangrijk doel van deze brede herziening. Uitgangspunt is dat de diensten hun bevoegdheden effectiever kunnen inzetten en sneller mee kunnen bewegen met de dreiging voor de nationale veiligheid. De reeds opgedane ervaringen met de Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma worden hierbij betrokken.

Vraag 2

In de kabinetsreactie wordt ingegaan op '*deterrence by punishment*'.

Vraag 2a

Wie zijn bevoegd om een cyber-aanval met een cyber-tegenaanval te beantwoorden?

De MIVD heeft, evenals de AIVD, bevoegdheden om cyberoperaties uit te voeren, waaronder verstorende (cyber)operaties op grond van artikel 73 van de Wiv 2017.

Zoals het kabinet eerder heeft aangegeven en consequent uitdraagt, is het internationaal recht van toepassing op het cyberdomein. In de bijlage bij de brief "Internationaal recht in het digitale domein (cyberspace)" (Kamerstuk 33 694 nr. 47) is het kabinet nader ingegaan op een aantal belangrijke internationaalrechtelijke regels die gelden in het cyberdomein. Ook is toegelicht hoe het kabinet tegen de toepassing van deze regels aankijkt. In deze bijlage wordt voorts ingegaan op de mogelijkheden van staten om cyberoperaties te attribueren alsmede de diverse responsopties bij

ongewenst cyberoptreden, zoals retorsie[1], tegenmaatregelen en zelfverdediging. Naast het optreden door de inlichtingen- en veiligheidsdiensten kan Nederland ook met de krijgsmacht reageren (Kamerstuk 26 643 nr. 785). Zo kan het Defensie Cyber Commando *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 2b

Bent u bereid om de Kamer vertrouwelijk op te hoogte te stellen van reeds door Nederland uitgevoerde cyber-tegenaanvallen die gericht zijn tegen statelijke actoren?

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

Vraag 3

Cyberaanvallen vallen onder internationale regelingen die het uitvoeren daarvan kunnen beperken. De leden van de fractie van de Partij voor de Dieren vragen u of u een overzicht kunt verstrekken van zulke beperkingen en daarin de volgende regelingen betrekken: het verdrag van Boedapest, Europees Verdrag voor de Rechten van de Mens, Internationaal verdrag inzake burgerrechten en politieke rechten, Verdragen van Geneve en aanvullende protocollen, VN-Handvest en het *Tallinn Manual*?

Zoals hierboven aangegeven 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 een uitgebreide toelichting van de visie van Nederland op de toepassing van een aantal belangrijke regels in het cyberdomein, zie de bijlage "Internationaal recht in het digitale domein (cyberspace)" bij Kamerstuk 33 694 nr. 47. Hierin stelt het kabinet onder meer dat mensenrechten evenzeer gelden in het cyberdomein als in het fysieke domein en dat er geen verschil bestaat tussen online en offline rechten.

Vragen en opmerkingen van de leden van de JA21-fractie

Vraag 1

De leden van de JA21-fractie vragen u of het kabinet erkent dat het volledig sluiten van Groningen onze crisisopties bij energie-chantage drastisch heeft verkleind. Neemt de weerbaarheidsopgave scenario's op voor tijdelijke reactivering van binnenlandse productie of vergelijkbare noodopties om de meervoudige redundantie van de energievoorziening te borgen?

Voorop staat dat het uitgangspunt voor de gasleveringszekerheid in Nederland goed is. De gasinfrastructuur is robuust en betrouwbaar, ook bij lagere temperaturen. Daarnaast zijn er diverse back-up voorzieningen en redundanties in het gassysteem. Meer specifiek heeft het kabinet een groot aantal maatregelen getroffen om ervoor te zorgen dat het sluiten van het Groningerveld verantwoord doorgang kon vinden. Voorbeelden hiervan zijn de bouw van een nieuwe stikstofinstallatie om de conversiecapaciteit van hoogcalorisch gas te vergroten, het omzetten van Gasopslag Grijpskerk naar een opslag van laagcalorisch gas en de versnelde afbouw van de export van laagcalorisch gas. Ook zijn de industriële grootverbruikers allemaal omgeschakeld naar hoogcalorisch gas. Deze maatregelen zorgen voor een robuust gassysteem. Ook tijdens de

[1] Met retorsie wordt verwezen naar handelingen die weliswaar onvriendelijk zijn, maar niet in strijd met het internationaal recht. Deze optie is daarmee altijd beschikbaar voor staten die willen reageren op onwenselijk
gedrag van een andere staat, omdat het gaat om de rechtmatige uitoefening van de bevoegdheden die zij als soevereine staat hebben. Staten zijn vrij om dit soort maatregelen te nemen zolang ze binnen de grenzen blijven van hun internationaalrechtelijke verplichtingen.

energiecrisis in 2022 is het niet nodig gebleken om de gasproductie uit het Groningenveld op te voeren. Daarnaast heeft het kabinet diverse maatregelen getroffen om de leveringszekerheid van gas te waarborgen, zie daarvoor verder het antwoord op vraag 2.

Vraag 2

Actualiseert het kabinet de gasbufferstrategie voor crisissituaties? Deze leden vragen u om een reflectie op verplichte vulling van gasopslagen, diversificatie van LNG-aanvoerpunten en noodscenario's voor leveringsonderbreking.

Het kabinet heeft de afgelopen jaren een breed spectrum aan maatregelen getroffen in het belang van de leveringszekerheid en het voorbereiden op en mitigeren van crisissituaties. Aan de vraagzijde werkt het kabinet aan een lagere gasvraag door energietransitie en besparing. Aan de aanbodzijde staat het kabinet voor een optimale productie in Nederland en een zo divers mogelijke import per pijpleiding (uit het Noorwegen, het Verenigd Koninkrijk en België) en in de vorm van LNG, waarvoor de LNG-importcapaciteit op peil is en wordt gehouden. De LNG-importcapaciteit in Nederland is in 2022 verdubbeld en er wordt gewerkt aan verdere uitbreiding. Tevens is er veel aandacht voor de rol van de gasopslagen die naast productie en import ook flexibiliteit geven in de winter. Sinds de Russische inval in Oekraïne houdt het kabinet de leveringszekerheid nauwlettend in de gaten en informeert het parlement hier zeer regelmatig over, laatstelijk bij brieven van 14 juli, 16 september en 30 september 2025 (Kamerstukken 29 023, nrs. 591, 594 en 596). Daarin is uitgebreid toegelicht welke maatregelen er op dit vlak lopen. In het bijzonder heeft het kabinet toegelicht dat wordt gestart met de aanleg van een noodvoorraad en is de vultaak toegelicht die Energie Beheer Nederland (EBN) heeft gekregen en welke middelen daarvoor beschikbaar zijn gesteld.

Voor de situatie dat er onverhoopt een tekort ontstaat of dreigt te ontstaan, ligt het noodplan op grond van de EU-verordening gasleveringszekerheid klaar, het zogenoemde Bescherm- en Herstelplan Gas (BH-G). Dit BH-G is in 2023 en 2024 uitgebreid geëvalueerd en geactualiseerd (Kamerstuk 29 023, nr. 494). Verder heeft het kabinet een voorstel voor de Wet bestrijden energieleveringscrisis (Wbe) in voorbereiding. Hiermee wil het kabinet de weerbaarheid van het gassysteem verder verbeteren, onder meer door maatregelen op gebied van gasopslag, en een duidelijker kader opstellen op welke manier de overheid kan ingrijpen als dat nodig is. Het kabinet verwacht begin 2026 het voorstel ter advisering voor te leggen aan de Afdeling advisering van de Raad van State.

Vraag 3

Bent u bereid het luchtalarm (WAS) als waarschuwingslaag te behouden en moderniseren (naast NL-Alert/radio), zodat alle inwoners ook bij grootschalige uitval of cyberattack tijdig worden bereikt?

NL-Alert is het primaire alerteringsmiddel om burgers te alerteren in Nederland bij rampen en crises. Dit volstaat in vredestijd. Bij een scenario van hybride en militaire dreigingen, is het echter kwetsbaar om enkel over NL-Alert – als sluitstuk van een in te richten civiel-militaire waarschuwingsketen – in de huidige vorm te beschikken.

Op dit moment wordt door het ministerie van Defensie en het ministerie van Justitie en Veiligheid onderzoek gedaan naar deze in te richten civiel-militaire waarschuwingsketen. Onderdeel van dit onderzoek is dat in het kader van redundantie in beeld wordt gebracht welke aanvullende mogelijkheden en middelen geschikt zijn om de samenleving te kunnen alerteren in het geval van een moderne lucht-, raket- of droneaanval. Hierbij wordt ook onderzocht of onderdelen van de huidige, verouderde infrastructuur van het Waarschuwings- en Alarmeringssysteem (WAS) hergebruikt kunnen worden. Als blijkt dat een doorontwikkeling van het huidige systeem wenselijk is in het kader van een hybride of militair dreiging, dan dienen daarvoor financiële middelen ter beschikking te worden gesteld. Ook als blijkt dat een ander middel het meest effectief is in een

hybride of militair scenario geldt dat voldoende budget noodzakelijk is. Zie voor een laatste stand van zaken op het onderwerp ‘alerteren’ de verzamelbrief Brandweerzorg, Crisisbeheersing en Meldkamers van de minister van Justitie en Veiligheid van 3 oktober 2025 (Kamerstuk 29 517 nr. 273).

In de verzamelbrief geeft de minister van Justitie en Veiligheid aan dat het huidige WAS sterk verouderd en end-of-life is. Ook is het WAS technisch en organisatorisch gezien niet ingericht als middel dat effectief kan worden ingezet bij het alerteren van de bevolking in het geval van een moderne lucht-, raket- of droneaanval.

Concrete informatie over hoe en wanneer het besluit van 29 februari 2024 (Kamerstuk 29 517 nr. 252) tot uitfasering met maatwerk voor hoogrisicolocaties wordt uitgevoerd, volgt wanneer er meer duidelijkheid is over de invulling van een redundante en robuuste waarschuwingsketen (waaronder alerteringsmiddelen), inclusief duidelijkheid over de financiering hiervan. Daarnaast worden met de veiligheidsregio’s verdere gesprekken gevoerd over het benodigde lokaal maatwerk bij de hoogrisicolocaties (zoals chemische industrie).

Vraag 4

Ten slotte vragen de leden van de JA21-fractie welke concrete stappen het kabinet zet voor bescherming van onderzeekabels en Noordzee-infrastructuur (detectie, patrouille, zeebodem-sensoren, juridische bevoegdheden), bovenop de al eerder ingezette EU- en NAVO-inspanningen.

Het kabinet neemt verschillende maatregelen om de weerbaarheid en bescherming van vitale infrastructuur op de Noordzee te verbeteren. In het interdepartementaal Programma Bescherming Noordzee Infrastructuur (PBNI) wordt hiervoor samengewerkt met zes departementen en verschillende uitvoeringsorganisaties (Kamerstuk 33 450 nr. 128). Zo is er de afgelopen jaren onder andere geïnvesteerd in het verbeteren van zicht op en in de Noordzee, het verhogen van de digitale en fysieke weerbaarheid van de infrastructuur en het verbeteren van de crisisbeheersing. Om uitvoering te kunnen geven aan het Actieplan heeft het vorige kabinet voor de jaren 2024 en 2025 ca. 44 mln. euro beschikbaar gesteld. Het is aan het nieuwe kabinet om een besluit te nemen over het vervolg van het PBNI.

Ministerie van Defensie

Aan	MINDEF
Van	DGB
Afgestemd met	CDS, HDFC, DJZ, DCo, BZ, BZK, JenV, KGG
In afschrift aan	STASDEF

TER BESLISSING

Datum
19 november 2025

Onze referentie
D2025-004783
MINDEF20250041268

Opgesteld door
[redacted]
KD:Ambtelijke leiding
[redacted]@mindef.nl

Aantal bijlagen
1

Nota

Aanleiding
Op 4 juni 2024 werd het advies 'Hybride dreigingen en maatschappelijke weerbaarheid' door de Adviesraad Internationale Vraagstukken (AIV) gepubliceerd. Op 6 december 2024 heeft u samen met de minister van Buitenlandse Zaken de kabinetsreactie op het AIV-advies naar de voorzitters van beide kamers van de Staten-Generaal gezonden. Naar aanleiding van de kabinetsreactie werden op 30 september vragen van de Eerste Kamer-fracties van de Partij voor de Dieren en JA21 naar u gezonden.

Geadviseerd besluit
U wordt geadviseerd in te stemmen met de antwoorden op vragen inzake de kabinetsreactie op het AIV-advies 'Hybride dreigingen en maatschappelijke weerbaarheid' en deze brief naar de Eerste Kamer te versturen.

Kernpunten
- De fractie van de Partij voor de Dieren stelt acht (deel)vragen over cyberaanvallen, cybertegenaanvallen, desinformatie en juridische kaders.
- De fractie van JA21 stelt vier vragen over weerbaarheid en bescherming gericht op aardgasvoorziening, het waarschuwings- en alarmeringssysteem (WAS) en Noordzee-infrastructuur.
- Bij de beantwoording zijn naast Defensie, BZ, BZK, JenV en KGG betrokken.
  - De minister van BZ is medeondertekenaar gelet op het eerder gezamenlijk met u ondertekenen van de kabinetsreactie en onderliggende adviesaanvraag bij de AIV.
  - De minister van BZK is medeondertekenaar vanwege zijn verantwoordelijkheid voor de AIVD, aanpak desinformatie en medeverantwoordelijkheid voor de (herziening van de) Wiv.
  - De vraag over het WAS (vraag 3 van JA21) is afgestemd met de minister van JenV.
  - De vragen over energievoorziening en gasbufferstrategie (vragen 1 en 2 van JA21) zijn afgestemd met de minister van KGG.

Toelichting

Financiële overwegingen
Uit de beantwoording van de vragen volgen geen financiële consequenties.

Juridische overwegingen
Uit de beantwoording van de vragen volgen geen juridische consequenties.

Communicatie
Er zijn geen communicatie-uitingen voorzien.

Informatie die niet openbaar wordt gemaakt
Persoonsgegevens van de steller en ondertekenaar worden afgeschermd met het oog op de bescherming van de persoonlijke levenssfeer.

DE DIRECTEUR-GENERAAL BELEID