Eerste Kamer der Staten-Generaal

Vergaderjaar 2026-2027 Aanhangsel van de Handelingen

Vragen door de leden der Kamer gesteld overeenkomstig artikel 105 van het Reglement van Orde, en de daarop door de regering schriftelijk gegeven antwoorden

AH
2

Vragen van de leden Van de Sanden (Fractie-Van de Sanden), Van Gasteren (Fractie-Van Gasteren), Beukering (Fractie-Beukering) en Marquart Scholtz (BBB), op 22 juni 2026 medegedeeld aan de minister van Defensie, de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Infrastructuur en Waterstaat, de minister van Economische Zaken en Klimaat en de minister-president naar aanleiding van de antwoorden van 9 juni 2026 op de vragen van 4 mei 2026 over de publieke beschikbaarheid van locatiegegevens van militaire en defensie gerelateerde infrastructuur (Aanhangsel Handelingen EK 2025–2026, nr. 9) en de nadere vragen over dit onderwerp van 16 juni 2026.

Antwoorden van de minister van Defensie ontvangen op 28 september 2026.

Vraag 1
Heeft de minister van Defensie expliciet verzocht aan het ministerie van Economische Zaken en Klimaat en het ministerie van Infrastructuur en Waterstaat de in haar antwoord aan de Eerste Kamer der Staten-Generaal van 9 juni 2026 genoemde vertrouwelijke militaire informatie “per direct” te verwijderen?

Antwoord 1
Ja, beide ministeries zijn hiertoe verzocht.

Vraag 2
Zo ja, wanneer en hoe is dit gebeurd en waarom is aan dat verzoek niet onmiddellijk gevolg gegeven? Was de minister-president hiervan op de hoogte en heeft hij zich met deze kwestie beziggehouden aangezien dit immers een zaak van nationale veiligheid betreft.

Antwoord 2
Op 11 juni 2026 heeft Defensie via een ambtelijk verzoek beide ministeries, Economische Zaken en Klimaat en Infrastructuur en Waterstaat, verzocht de defensiegevoelige infrastructuurgegevens per direct te verwijderen. Na ontvangst van dit verzoek is direct een analyse uitgevoerd om de volledige dataketens in kaart te brengen, de wettelijke kaders voor afscherming te toetsen en de afweging te maken tussen nationale veiligheidsrisico’s en andere maatschappelijke belangen, zoals het voorkomen van graafschade. Deze voorbereidende fase was noodzakelijk om te waarborgen dat de depublicatie op een juridisch correcte en technisch beheersbare manier kon worden uitgevoerd. Gevolg is dat daardoor de informatie niet onmiddellijk offline werd gehaald.
In juli 2026 zijn vervolgens de relevante bronhouders, zowel binnen als buiten Defensie, formeel aangeschreven met de opdracht de betreffende gegevens te verwijderen of niet langer openbaar te maken. Deze opdrachten zijn inmiddels opgevolgd en voor het Register Externe Veiligheidsrisico’s (REV) in uitvoering.

De minister-president is in een eerder stadium niet over deze specifieke afstemming geïnformeerd, omdat er geen aanwijzingen waren voor een concrete of acute dreiging tegen deze infrastructuur.

Vraag 3
Kan de regering uiteenzetten welke juridische analyses zijn verricht voordat door de minister van Defensie werd besloten dat en welke informatie over vitale en militaire infrastructuur direct diende te worden verwijderd, welke ministeries daarbij betrokken waren en op welke wettelijke grondslagen deze afwegingen zijn gebaseerd?

Antwoord 3
Voorafgaand aan het verzoek tot verwijdering heeft Defensie een veiligheidsappreciatie gemaakt van de online beschikbare gegevens. Het betreft hierbij civiele vitale infrastructuur die zich op defensielocaties bevindt (dus onder de verantwoordelijkheid van Defensie) en defensie-pijpleidingen. Het verzoek tot verwijdering gaf daarbij aanleiding tot direct overleg tussen Defensie en andere betrokken ministeries. Zoals bij vraag 2 genoemd is in deze interdepartementale afstemming gezamenlijk geconcretiseerd welke data verwijderd of verminderd moet worden en welke juridische grondslagen hierbij van belang zijn. Zowel de veiligheidsanalyse als de juridische analyse wordt momenteel voortgezet om de reikwijdte van de risico’s en relevante wet- en regelgeving steeds volledige in kaart te brengen.

Vraag 4
Welke minister of ministers waren ten tijde van het verzoek van Defensie bestuurlijk verantwoordelijk voor de besluitvorming over het al dan niet onmiddellijk afschermen van de betreffende gegevens en hoe is de komende coördinatie tussen de betrokken departementen vormgegeven?

Antwoord 4
De ministers van Defensie, Economische Zaken en Klimaat, Klimaat en Groene Groei, Volkshuisvesting en Ruimtelijke Ordening, de staatssecretaris van Infrastructuur en Waterstaat en van Binnenlandse Zaken en Koninkrijksrelaties zijn bestuurlijk verantwoordelijk voor kritische infrastructuurdata die als eerste moest worden afgeschermd. De data is verspreid over meerdere ministeries en uitvoeringsorganisaties, waarbij verschillende registers en publicatieportalen een rol spelen. Defensie, betrokken ministeries en de bronhouders coördineren het afschermen van de geo-data gezamenlijk. Dit heeft ertoe geleid dat een belangrijk deel van de desbetreffende gevoelige geo-data niet langer op het open internet wordt gepubliceerd.

Ten aanzien van defensiegevoelige infrastructuurgegevens zal Defensie zelf de eigen risicoanalyse blijven bijwerken en proactief verzoeken uitzetten tot afscherming van defensiegevoelige infrastructuurgegevens. Defensie informeert andere bestuursorganen die informatie publiceren welke publicaties een risico vormen en waarop maatregelen moeten worden toegepast. De uitvoering van de maatregelen ligt bij het betreffende ministerie en de daarbinnen aangewezen uitvoeringsorganisaties. Eventuele blokkades bij het afschermen als gevolg van interdepartementale afstemming worden direct geëscaleerd, indien nodig op het niveau van de ministerraad. Daarnaast wordt de coördinatie tussen de betrokken departementen onder meer versterkt door de interdepartementale werkgroep Openbaarheid en Nationale Veiligheid onder leiding van Binnenlandse Zaken en Koninkrijksrelaties, als stelstelverantwoordelijke voor het openbaarheidsbeleid.

Vraag 5
Welk departement en/of directie heeft besloten om het verzoek van de minister van Defensie niet onmiddellijk uit te voeren?

Antwoord 5

Hiervan is geen sprake geweest. Het verzoek van Defensie leidde direct tot een geïntensiveerd overleg met betrokken ministeries om de dataketens in kaart te brengen, afscherming te toetsen aan wettelijke kaders en een afweging te maken met andere risico’s, zoals onbedoelde schade door bouwwerkzaamheden. Dit is gevolgd door gerichte verzoeken en daadwerkelijk afscherming van gegevens, zoals de eerdergenoemde data van de netbeheerders die per 24 augustus 2026 offline is gehaald. Voor het afschermen van data in het Register Externe Veiligheidsrisico’s (REV) wordt vanaf november rubricering van data via het Informatiemodel Externe Veiligheid gefaciliteerd. Momenteel wordt gewerkt aan een tijdelijke oplossing om informatie in de tussentijd af te schermen. Defensie is als bronhouder zelf verantwoordelijk voor de data die in het register wordt aangeleverd, het ministerie van Infrastructuur en Waterstaat is verantwoordelijk voor het beheer van het register.

Vraag 6
Acht de regering het wenselijk dat een verzoek van de minister van Defensie die primair verantwoordelijk is voor de nationale veiligheid en de bescherming van militaire infrastructuur eerst door andere departementen wordt afgewogen, alvorens al dan niet tot uitvoering wordt overgegaan?

Antwoord 6
Als minister van Defensie ben ik primair verantwoordelijk voor de nationale veiligheid en de bescherming van militaire infrastructuur. Een dergelijk verzoek wordt door mij eerst onder de aandacht gebracht van de relevante ministeries zodat een gezamenlijke afstemming kan plaatsvinden.

Bij een acuut en concreet veiligheidsrisico is het uitgangspunt om direct maatregelen te nemen om de veiligheid te waarborgen, maar hiervoor was geen concrete aanwijzing. Het gaat in het geval van defensiegevoelige infrastructuurgegevens niet om een keuze tussen nationale veiligheid en andere belangen, maar om een integrale afweging van verschillende veiligheidsrisico's. Het volledig afschermen van bepaalde gegevens kan nieuwe risico's creëren voor de publieke veiligheid, zoals bij de inzet van hulpdiensten tijdens een crisis. Door deze risico's in samenhang te beoordelen, wordt de meest effectieve vorm van veiligheidsborging voor Nederland gerealiseerd. Daarbij moet altijd beoordeeld worden op welke juridische grond informatie mogelijk moet worden uitgezonderd van openbaarmaking.

Vraag 7
Welke concrete belangen rechtvaardigden het voortgezet online beschikbaar houden van de informatie gedurende de periode tussen het verzoek van Defensie en de uiteindelijke verwijdering?

Antwoord 7
Kennis over de aanwezigheid van defensiegevoelige infrastructuur kan deze netwerken ook beschermen tegen ongewenste incidenten, zoals bijvoorbeeld door bouwwerkzaamheden. Daarnaast kan schade aan bijvoorbeeld een kerosinepijpleiding verstrekkende gevolgen hebben voor de omgeving.

Vraag 8
Wegen deze belangen zwaarder dan het belang van de nationale veiligheid? Kunt u dit gemotiveerd toelichten?

Antwoord 8
Aangezien de militaire infrastructuur van groot belang is voor de veiligheid van Nederland, moet deze waar mogelijk afgeschermd worden. Beperkte openbaarheid kan tegelijk ook bijdragen aan veiligheid. Onbedoelde schades aan infrastructuur komen regelmatig voor in Nederland. Het afschermen van deze gegevens moet dan ook gebeuren zonder andere onacceptabele risico’s te introduceren. Het gaat er dus om dat we verschillende vormen van veiligheidsrisico's in samenhang beoordelen, zoals ook in het antwoord op vraag 7 is toegelicht.

Vraag 9
Is gedurende deze periode een expliciete risicoanalyse gemaakt van de gevolgen van het online beschikbaar blijven van de informatie? Zo ja, kan deze analyse vertrouwelijk met de Staten-Generaal worden gedeeld?

Antwoord 9
Defensie heeft een analyse gemaakt van de online gegevens die het meest risicovol zijn voor defensielocaties en gerelateerde infrastructuur. Deze analyse wordt doorlopend bijgewerkt. Een recente versie kan vertrouwelijk worden gedeeld.

Vraag 10
Heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) inzake deze kwestie advies uitgebracht? Zo ja, welk advies, zo nee, waarom niet? Is de Landsadvocaat gevraagd om hierover advies uit te brengen? Zo ja, welk advies, zo nee, waarom niet?

Antwoord vraag 10
De NCTV neemt deel aan de klankbordgroep van de interdepartementale werkgroep 'Openbaarheid en Nationale Veiligheid'. De NCTV heeft op dit moment nog geen specifiek advies uitgebracht over deze individuele kwestie.

De Landsadvocaat is betrokken bij deze kwestie en draagt bij aan de juridische analyse die nu in samenspraak met en de betrokken departementen nader wordt uitgewerkt.

Vraag 11
Was er binnen de rijksoverheid verschil van inzicht tussen Defensie enerzijds en de ministeries van Economische Zaken respectievelijk Infrastructuur en Waterstaat anderzijds over het al dan niet verwijderen van openbaar gemaakte geheime militaire infrastructuurgegevens? Zo ja, waaruit bestond (of bestaat) dat verschil van inzicht precies?

Antwoord 11
Nee, er is geen sprake van een verschil van inzicht. Wij zijn het erover eens dat de huidige geopolitieke situatie een heroverweging noodzaakt van welke defensiegevoelige informatie wij publiceren en op welke wijze dit gebeurt.

Vraag 12
De regering antwoordt de Kamer – in dit geval bij monde van de minister van Defensie – steeds als één orgaan. Kan de minister-president aangeven welk kabinetsstandpunt uiteindelijk leidend was/is en kunnen alle verantwoordelijke ministers zich hiermee verenigen?

Antwoord 12
Er is een breed gedragen inzicht dat zowel de bescherming van de nationale veiligheid als de fundamentele waarde van openbaarheid essentieel zijn.

Vraag 13
Indien de minister van Defensie kennelijk van oordeel is dat er sprake is van een acuut veiligheidsrisico, waarom is dan niet gekozen voor toepassing van het voorzorgsbeginsel: eerst depubliceren en vervolgens de juridische grondslag nader beoordelen? Weegt juridische zorgvuldigheid en/of transparantie dan zwaarder dan het belang van nationale veiligheid?

Antwoord 13
Bij een acuut en concreet veiligheidsrisico is het uitgangspunt altijd om direct maatregelen te nemen om de veiligheid te waarborgen. Echter zou het volledig offline halen van gegevens nieuwe veiligheidsrisico’s introduceren. Daarom zijn vanuit het voorzorgsbeginsel veiligheidsrisico’s getoetst en is geborgd dat afscherming van gegevens geen nieuwe onacceptabele risico’s introduceert.

Vraag 14
Bestaat er een nationaal protocol voor situaties waarin een bewindspersoon die verantwoordelijk is voor nationale veiligheid verzoekt om onmiddellijke afscherming van gevoelige/geheime informatie? Zo nee, acht de regering het wenselijk een dergelijk protocol alsnog vast te stellen?

Antwoord 14

Er zijn verschillende kaders, zoals het VIRBI (Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie) en de uitzonderingsgronden van de Woo, op grond waarvan het veiligheidsbelang kan worden meegewogen bij de publicatie van informatie. Deze kaders worden momenteel in kaart gebracht in de eerdergenoemde juridische analyse, waarvan het huidige beeld is dat deze voldoende grond geven voor het afschermen van defensiegevoelige infrastructuurgegevens. Daarom wordt op dit moment geen aanleiding gezien voor het instellen van een aanvullend protocol.

Vraag 15
Kan de regering uitsluiten dat gedetailleerde informatie over militaire installaties, brandstofvoorzieningen, communicatienetwerken, radarinstallaties en/of vitale defensieobjecten momenteel nog steeds via overheidsplatforms openbaar toegankelijk is?

Antwoord 15
Defensie stelt dat online beschikbaarheid van kritische infrastructuurgegevens van defensielocaties in augustus sterk is teruggebracht, onder meer door de netbeheerders. Tussen september en november volgen nog verschillende aanvullende maatregelen die de online beschikbaarheid van defensiegevoelige infrastructuur gegevens verder reduceren.

Het volledig offline halen van alle infrastructuurgegevens is niet wenselijk. Een zekere mate van bekendheid van de ligging van kritieke infrastructuur zoals buisleidingen beschermt deze infrastructuur tegen onbedoelde incidenten of verstoring. Belangrijk is wel dat er geen onnodige details kenbaar worden gemaakt en kwetsbare gegevens zoveel mogelijk in afgeschermde omgevingen worden geplaatst. Defensie gaat hier ten aanzien van de eigen infrastructuur proactief op monitoren en andere departementen waar nodig verzoeken tot verdere afscherming.

Vraag 16
Welke lessen trekt de regering uit deze casus voor de samenwerking tussen Defensie, Algemene Zaken, Economische Zaken en Infrastructuur en Waterstaat in een tijd waarin sabotage, hybride dreigingen en statelijke inmenging nadrukkelijk onderdeel vormen van het veiligheidsbeeld?

Antwoord 16
De betrokken ministers zijn van mening dat het vergroten van de weerbaarheid van Nederland een gezamenlijke prioriteit is. Dit betekent dat veel bewuster omgegaan moet worden met publicatie van defensiegevoelige gegevens op het open internet, en tegelijkertijd wel voldoende gegevens beschikbaar moeten blijven om onbedoelde schade te voorkomen en bij calamiteiten effectief te handelen. Een belangrijke les is dat de correcte classificatie en rubricering van informatie bij de bron essentieel is. Daarnaast is het belangrijk om realistisch te zijn: gegevens die eenmaal online staan of verzameld worden buiten de overheid om, zijn lastig om weer offline te krijgen.

De samenwerking tussen de betrokken ministeries is door deze kwestie verbeterd en leidt inmiddels tot concrete resultaten.

Vraag 17
Deelt de regering de opvatting dat bij twijfel over de verenigbaarheid van wettelijke openbaarmakingsverplichtingen met de bescherming van nationale veiligheid, tijdelijke afscherming van de informatie in beginsel de voorkeur

verdient boven voortgezette publicatie totdat een juridische analyse is afgerond? Zo nee, waarom niet?

Antwoord 17
Bij een concrete en acute dreiging met voldoende onderbouwd risico voor de nationale veiligheid verdient tijdelijke afscherming in beginsel de voorkeur.

Vraag 18
Welke rol heeft het ministerie van Algemene Zaken gespeeld bij de coördinatie van deze kwestie en op welk moment is de minister-president hierover geïnformeerd?

Antwoord 18

Het gesprek over deze kwestie is primair gevoerd tussen de ministeries van Defensie, Binnenlandse Zaken en Koninkrijksrelaties, Infrastructuur en Waterstaat en Economische Zaken en Klimaat. Het ministerie van Algemene Zaken en de minister-president zijn daarbij niet betrokken.

Vraag 19
Indien een minister van Defensie aangeeft dat openbaar beschikbare informatie een risico vormt voor de nationale veiligheid, op welke juridische grondslag kan een uitvoeringsorganisatie of een ander ministerie besluiten die informatie niet te verwijderen?

Antwoord 19
De minister van Defensie kan niet zelfstandig een ander ministerie opdracht geven om reeds gepubliceerde informatie uit het openbare register onmiddellijk af te schermen of te verwijderen. Verschillende wetten, zoals de Wet open overheid, bevatten een uitzonderingsgrond om informatie al dan niet af te schermen. De lopende juridische analyse wijst uit dat er voldoende juridische mogelijkheden zijn om een restrictief publicatieregime te hanteren. Inmiddels zijn in goed overleg verschillende verwijderingsverzoeken gerealiseerd zonder dat er sprake is van juridische blokkades. Wel moet er sprake zijn van een goede afweging, omdat publicatie in specifieke gevallen ook bij kan dragen aan maatschappelijke (veiligheids)belangen.

Vraag 20
Kan de regering uitsluiten dat vergelijkbare situaties zich ook ten aanzien van andere vitale infrastructuur voordoen, waaronder energievoorzieningen, telecommunicatienetwerken, drinkwater-infrastructuur, transport-infrastructuur en crisiscommunicatiesystemen? Zo nee, deelt de regering de opvatting dat dit erop wijst dat het huidige wettelijke stelsel onvoldoende is toegerust gevoelige infrastructuur gegevens te beschermen tegen misbruik door statelijke factoren, sabotage of hybride dreigingen?

Antwoord 20
In de huidige geopolitieke realiteit kunnen risico's als gevolg van sabotage of hybride dreigingen tegen vitale infrastructuur nooit volledig worden uitgesloten. De bescherming van gevoelige gegevens heeft daarom de hoogste prioriteit. Het huidige wettelijke stelsel biedt met specifieke weigeringsgronden voor nationale veiligheid reeds belangrijke instrumenten, maar de dynamische dreiging vraagt om voortdurende scherpte.
Daarnaast kijkt de Nationaal Coördinator Terrorismebestrijding en Veiligheid doorlopend naar de risico's voor de continuïteit van onze kritieke infrastructuur om de nationale weerbaarheid te verhogen.