Ministerie van Defensie

> Retouradres Postbus 20701 2500 ES Den Haag

de Voorzitter van de Tweede Kamer
der Staten-Generaal
Bezuidenhoutseweg 67
2594 AC Den Haag

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

Onze referentie
MINDEF20260047956

Bij beantwoording, datum, onze referentie en onderwerp vermelden.

Datum	28 september 2026
Betreft	Beantwoording vragen van de leden Van Lanschot, Bühler en Boelsma-Hoekstra over het bericht dat ''Defensie wil dat kwetsbare informatie per direct offline gaat, maar dat andere ministeries nog in gesprek hierover zijn."

Geachte voorzitter,

Hierbij bied ik u, mede namens de minister van Economische Zaken en Klimaat, de minister van Klimaat en Groene Groei, de staatssecretaris van Infrastructuur en Waterstaat en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties de antwoorden aan op de schriftelijke vragen gesteld door de leden Van Lanschot, Bühler en Boelsma-Hoekstra (allen CDA) over het bericht dat ‘Defensie wil dat kwetsbare informatie per direct offline gaat, maar dat andere ministeries nog in gesprek hierover zijn’. Deze vragen werden ingezonden op 17 juni 2026 met kenmerk 2026Z13381.

Hoogachtend,

DE MINISTER VAN DEFENSIE

Dilan Yeşilgöz-Zegerius

Vraag 1: Klopt het dat medio 2025 ambtelijk is gesignaleerd dat mogelijk defensiegevoelige infrastructuurgegevens openbaar beschikbaar waren op websites en in registers van de overheid, maar dat deze gegevens nog steeds online staan?

Antwoord: Medio 2025 is gesignaleerd dat mogelijk defensiegevoelige infrastructuurgegevens online staan. In de daaropvolgende periode is gewerkt aan beter inzicht om welke data en registers het precies gaat en welke data volgens Defensie als eerste afgeschermd moet worden. Het overgrote deel van de door Defensie gevraagde informatie is inmiddels afgeschermd, wat hieronder wordt toegelicht. Hierbij hanteer ik een driedeling: (1) informatie die al offline is gehaald of dat zeer binnenkort zal gaan, (2) informatie die meer tijd kost om te bepalen wat er precies offline kan en (3) informatie die niet offline wordt gehaald vanwege andere veiligheidsbelangen. Ik geef hieronder direct een update per categorie.

1) *Al offline*: Er is bij de netbeheerders een verwijderingsverzoek ingediend voor het offline halen van gegevens over aansluitingen van infrastructuur op defensieterreinen. De netbeheerders hebben bevestigd dat zij de gevraagde gegevens hebben verwijderd van hun publieke websites. Daarnaast heeft Defensie ten aanzien van de pijpleidingen die in eigen beheer zijn een restrictief publicatiebeleid geïmplementeerd. Dit houdt in dat binnen de kaders van de Omgevingswet gevoelige technische details niet langer gedeeld worden of enkel inzichtelijk zijn voor bevoegde instanties, zoals veiligheidsdiensten. Beperking van publicatie van gegevens in het Register Externe Veiligheidsrisico's (REV) is onderdeel van deze aanpak. Momenteel wordt het Informatiemodel Externe Veiligheid aangepast zodat rubricering van gegevens in het REV vanaf november structureel mogelijk wordt. In de tussentijd wordt gewerkt aan tijdelijke maatregelen om gevoelige gegevens af te schermen. Met deze stappen zijn de door Defensie hoogst geprioriteerde militaire geo-data succesvol afgeschermd.

2) *Nog te beoordelen*: Hoge resolutie lucht- en satellietfotografie van Defensielocaties is onwenselijk, maar complexer om in te dammen. Dit komt onder meer door het grote aantal (commerciële) aanbieders en doordat satellietfotografie buiten Nederlandse jurisdictie valt. Momenteel wordt onderzocht of het (gedeeltelijk) intrekken van het verlof luchtfotografie in combinatie met gerichte verzoeken aan publicatieportalen van lucht- en satellietbeelden effectief kan zijn om online beschikbaarheid van hoge resolutie beelden van Defensie infrastructuur te reduceren.

3) Een derde categorie betreft informatie die *online moeten blijven*, omdat verwijdering bijvoorbeeld andere veiligheidsrisico's veroorzaakt. Zo kan het volledig afschermen van informatie over vervoer en opslag van gevaarlijke stoffen de kans op onbedoelde schade vergroten en de effectiviteit van de reactie bij calamiteiten verminderen.

Vraag 2: Deelt u de opvatting dat bij een concreet risico op sabotage van militaire infrastructuur de nationale veiligheid leidend moet zijn en dat informatie daarom bij twijfel op zijn minst eerst tijdelijk moet worden afgeschermd, waarna de juridische discussie kan worden afgerond? Zo nee, waarom niet?

Antwoord 2: Ja, de ministers van Defensie, van Economische Zaken en Klimaat, van Klimaat en Groene Groei, de staatssecretaris van Infrastructuur en Waterstaat en de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties zijn van mening dat wanneer door publicatie van bepaalde informatie de nationale veiligheid van Nederland in het geding is, deze informatie niet openbaar mag worden gemaakt. In de praktijk moet er vaak een afweging worden gemaakt tussen nut en noodzaak van openbaarheid en de nationale veiligheid. Zo draagt de publicatie van pijpleidingen bij aan een betere ruimtelijke planning en reductie van andere maatschappelijke (veiligheids)risico's.

Het gaat hier 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.

Vraag 3: Kan de minister van Defensie andere ministeries daadwerkelijk opdragen defensiegevoelige informatie onmiddellijk af te schermen? Zo nee, wie kan binnen het kabinet bij een acute dreiging wel een bindend besluit nemen?

Antwoord 3: Nee, de minister van Defensie kan een ander ministerie geen opdracht geven om informatie onmiddellijk af te schermen. De ministeries van Defensie, van Binnenlandse Zaken en Koninkrijksrelaties, van Economische Zaken en Klimaat en van Infrastructuur en Waterstaat staan eensgezind achter het belang van nationale veiligheid en spreken daarom met elkaar over situaties waarin deze veiligheid in het geding kan komen. In dit verband voeren de genoemde ministeries gerichte acties uit om data af te schermen, waarbij gezamenlijk een zorgvuldige belangenafwegingen wordt gemaakt.

Vraag 4: Welke maatregelen zijn direct na de ambtelijke signalering van deze veiligheidsrisico's medio 2025 genomen?

Antwoord 4:
In de zomer van 2025 zijn de signalen over de risico's van (het combineren van) openbare bronnen ambtelijk gedeeld en is de minister van Binnenlandse Zaken en Koninkrijksrelaties hierover geïnformeerd. Dit betrof een eerste analyse en geen verzoek tot verwijdering van bepaalde gegevens. Vervolgens is Defensie in kaart gaan brengen welke informatie risicovol wordt geacht, onder andere in samenwerking met de MIVD. Tegelijk is in verschillende gremia op ambtelijk niveau aandacht en actie gevraagd voor het onderwerp en is de politieke urgentie toegenomen. Dit heeft in juni 2026 geleid tot gerichte verzoeken tot verwijdering van bepaalde gegevens door Defensie aan bronhouders in samenwerking met andere departementen.

Tegelijkertijd heeft het ministerie van Binnenlandse Zaken en Koninkrijksrelaties in oktober 2025 de interdepartementale werkgroep Openbaarheid en Nationale Veiligheid geïnitieerd. De formele start van de werkgroep was in maart 2026. De werkgroep ontwikkelt een beleidslijn die Q1 wordt opgeleverd en vervolgens verder uitgewerkt.

Vraag 5: Klopt het dat pas in het najaar van 2025 is begonnen met het verwijderen of afschermen van deze informatie? Kunt u toelichten waarom dit na de eerste signalering nog maanden heeft geduurd?

Antwoord 5: Dit komt omdat nationale veiligheidsrisico's moeten worden afgewogen tegen andere maatschappelijke (veiligheids)belangen. Bovendien is de publicatieplicht van gegevens in sommige gevallen juridisch verankerd ter bescherming van andere maatschappelijke (veiligheids)belangen. Veel van de betreffende data bevindt zich bovendien niet bij een ministerie, maar bij derde partijen die moeten worden betrokken. Zoals bij vraag 1 toegelicht heeft dit proces nu wel degelijk tot concreet resultaat geleid.

Vraag 6: Wat is de reden dat de ministeries van Infrastructuur en Waterstaat en Economische Zaken en Klimaat vooralsnog geen volledige uitvoering hebben gegeven aan het verzoek van de minister van Defensie om kwetsbare informatie per direct offline te halen?

Antwoord 6: Hier is opvolging aan gegeven. In juni 2026 had Defensie een specifiek genoeg beeld bij de gegevens en de bronhouders om gerichte verwijderingsverzoeken uit te zetten. Het ministerie van Defensie heeft daarom in juni 2026 aan het ministerie van Economische Zaken en Klimaat verzocht om informatie over het in gebruik zijnde ondergrondse elektriciteitsnet op specifieke defensielocaties en objecten te depubliceren. De netbeheerders zijn bronhouders van deze informatie en publiceren deze informatie mede gelet op het belang van het functioneren van het energiesysteem en transparantie rond de energietransitie. In constructief overleg met het ministerie van Economische Zaken en Klimaat en de netbeheerders is gevoelige militaire geo-informatie reeds gedepubliceerd.

Het ministerie van Infrastructuur en Waterstaat beheert het Register Externe Veiligheidsrisico's (REV). De informatie komt van door de wet aangewezen (gedelegeerde) bronhouders, waaronder specifieke onderdelen binnen Defensie. Met het ministerie van Infrastructuur en Waterstaat wordt momenteel gewerkt aan aanpassing van het Informatiemodel Externe Veiligheid waardoor rubricering van gegevens structureel door de bronhouder kan worden ingevuld. Gerubriceerde gegevens zijn daarna niet langer automatisch zichtbaar. Naar verwachting wordt deze werkwijze vanaf november geïmplementeerd. Tot aan november wordt gewerkt aan tijdelijke maatregelen om gevoelige data niet langer op het publieke internet te publiceren en reeds gepubliceerde data grotendeels af te schermen.

Vraag 7: Waarom is pas in maart 2026 een interdepartementale werkgroep "Openbaarheid en nationale veiligheid" ingesteld, terwijl al sinds medio 2025 bekend was dat mogelijk gevoelige informatie openbaar was?

Antwoord 7: De kwestie rond openbaarheid en nationale veiligheid is complex en raakt meerdere maatschappelijke (veiligheids)belangen. Om een effectieve en breed gedragen aanpak te waarborgen, was het nodig om eerst met de diverse betrokken partijen goed af te stemmen. Dat proces heeft onder meer geleid tot de instelling van de interdepartementale werkgroep Openbaarheid en Nationale Veiligheid onder leiding van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Vraag 8: Deelt u de opvatting dat het instellen van een ambtelijke werkgroep geen alternatief kan zijn voor een onmiddellijk bestuurlijk besluit wanneer informatie per direct offline moet worden gehaald vanwege risico's op spionage en sabotage? Zo nee, waarom niet?

Antwoord 8: Ja, het doel van de werkgroep Openbaarheid en Nationale Veiligheid onder leiding van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties is niet bedoeld om besluitvorming te organiseren die leidt tot het offline halen van bepaalde informatie en vormt daarmee geen alternatief voor een onmiddellijk bestuurlijk besluit. De werkgroep Openbaarheid en Nationale Veiligheid onder leiding van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties richt zich op het ontwikkelen van een beleidslijn en een afwegingskader die de departementen helpen structureel met dit vraagstuk om te gaan, zodat bij de publicatie van informatie vooraf rekening wordt gehouden met de huidige geopolitieke veiligheidssituatie.

Vraag 9: Zijn de MIVD, AIVD en de NCTV betrokken bij deze ambtelijke werkgroep? Zo nee, waarom niet? Zo ja, hoe beoordelen zij dat deze gevoelige informatie nog niet offline is gehaald?

Antwoord 9: Ja, de MIVD, AIVD en de NCTV zijn door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties benaderd voor betrokkenheid bij het ontwikkelen van de beleidslijn en het afwegingskader en zijn op de hoogte van de situatie en de werkgroep. Als belangrijke kennisbron worden de veiligheidsdiensten en de NCTV gevraagd advies te geven over de producten van de werkgroep Openbaarheid en Nationale Veiligheid onder leiding van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties, zowel op de vraag welke informatie gevoelig is als op de vraag hoe daarmee omgegaan moet worden.

Vraag 10: Erkent u dat deze gang van zaken – eerst signaleren, vervolgens maanden overleggen, daarna een werkgroep instellen en uiteindelijk nog steeds geen volledige verwijdering realiseren – niet past bij de snelheid en slagkracht die nodig zijn in de huidige veiligheidssituatie? Zo nee, waarom niet?

Antwoord 10: Nee, want meerdere veiligheidsrisico's moeten integraal worden afgewogen en verwijdering moet gericht plaatsvinden. Er is een werkwijze gevolgd waarin (1) is gesignaleerd, (2) onderzoek is gedaan om welke informatie het gaat, (3) afstemming met andere departementen is gezocht en (4) samen met bronhouders gericht is gewerkt aan afscherming. Dit heeft onder meer geleid tot een gerichte analyse welke informatie precies offline moest. In samenwerking met het ministerie van Economische Zaken en Klimaat en de netbeheerders is vervolgens de betreffende informatie sinds 24 augustus 2026 offline. In samenwerking met het ministerie van Infrastructuur en Waterstaat wordt de gevraagde informatie in het Register Externe

Veiligheidsrisico's (REV) tijdelijk afgeschermd en kan vanaf november 2026 structureel door Defensie worden gerubriceerd. Parallel hieraan is de werkgroep openbaarheid en nationale veiligheid ingericht die zich richt op de ontwikkeling van een toekomstbestendige beleidslijn en het afwegingskader. De gedeelde beleidslijn en afwegingskader dragen eveneens bij aan de snelheid en slagkracht die nodig is op een dergelijk onderwerp.

Vraag 11: Bent u bereid zo spoedig mogelijk alle gegevens die Defensie als potentieel sabotagegevoelig beoordeelt in ieder geval tijdelijk af te schermen? Zo nee, waarom niet.

Antwoord 11: Ja, de huidige veiligheidssituatie dwingt ons tot een heroverweging van welke informatie gepubliceerd mag worden. Wanneer er sprake is van een direct risico voor de veiligheid van de Staat of wanneer het belang van nationale veiligheid zwaarder weegt dan andere maatschappelijke (veiligheids)belangen, moet deze informatie zo spoedig mogelijk worden afgeschermd. De betrokken ministers zijn hierin eensgezind.

Vraag 12: Bent u bereid één bewindspersoon aan te wijzen die doorzettingsmacht krijgt bij conflicten tussen openbaarmakingsverplichtingen en de nationale veiligheid, zodat niet opnieuw maandenlang interdepartementaal overleg nodig is voordat wordt ingegrepen? Zo nee, waarom niet?

Antwoord 12: Dit sluit niet aan bij de ministeriele verantwoordelijkheid voor het eigen beleidsterrein. Momenteel worden concrete stappen gezet richting afscherming en met resultaat. De interdepartementale werkgroep Openbaarheid en Nationale Veiligheid onder leiding van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties ontwikkelt daarnaast een beleidslijn en afwegingskader die bronhouders ondersteunen bij het maken van een afweging die past bij het huidige veiligheidsbeeld. Defensie heeft hier een belangrijke rol in. Ten derde is Defensie bezig structurele capaciteit in te richten die de online aanwezigheid van defensiegevoelige infrastructuurgegevens monitort en gerichte verzoeken uitzet ter afscherming.

Indien er een conflict ontstaat, kan dit snel door het kabinet worden besproken en besloten.