Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2023–2024

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1866

Vragen van het lid **Eerdmans** (JA21) aan de Ministers van Economische Zaken en Klimaat en van Justitie en Veiligheid over *de (cyber)veiligheid van Nederlandse offshore olie- en gasplatforms* (ingezonden 26 april 2024).

Antwoord van Minister **Yeşilgöz-Zegerius** (Justitie en Veiligheid) (ontvangen 29 mei 2024).

Vraag 1
Wat is het actuele dreigingsbeeld betreffende offshore olie- en gasplatforms in de Nederlandse Noordzee, mede in het licht van de aanstaande intensivering van gasboring?

Antwoord 1
Het dreigingsbeeld voor maritieme infrastructuur is onder meer beschreven in jaarverslagen van de AIVD[1] en MIVD[2], en in stukken zoals het Dreigingsbeeld Statelijke actoren[3] en het Cybersecuritybeeld Nederland 2023[4]. In het openbare jaarverslag van de MIVD over 2023 staat dat Rusland deze infrastructuur heimelijk in kaart brengt en activiteiten onderneemt die duiden op spionage en voorbereidingshandelingen voor verstoring en sabotage jegens onze nationale veiligheidsbelangen (economische veiligheid, fysieke en digitale veiligheid) met potentiële impact op de leveringszekerheid.

Vraag 2
Welke maatregelen heeft u genomen om de veiligheid van offshore olie- en gasplatforms in de Noordzee te garanderen tegen mogelijke dreigingen?

Antwoord 2
Om deze dreigingen het hoofd te bieden en onze nationale veiligheidsbelangen te beschermen, werken wij op verschillende niveaus samen om de digitale, fysieke en economische weerbaarheid te versterken. Er lopen verschillende beleidsinitiatieven, wetsvoorstellen en crisisvoorbereidingen om dit te realiseren. Hieruit volgen bepaalde (wettelijke) taken om aanbieders van de energie-infrastructuur zorg te laten dragen om hun (digitale) systemen weerbaar en veerkrachtig te maken.

---

[1] Jaarverslagen AIVD
[2] Jaarverslag MIVD
[3] Dreigingsbeeld Statelijke Actoren 2
[4] Cybersecuritybeeld Nederland 2023

ah-tk-20232024-1866
ISSN 0921 - 7398
's-Gravenhage 2024

Hierna zet ik de voornaamste voor u op een rij:
Onder coördinatie van de Minister van IenW wordt binnen het interdepartementale Programma Bescherming Noordzee Infrastructuur gewerkt aan de bescherming van vitale offshore infrastructuur, waaronder energie-infrastructuur, op de Noordzee [5].
Sectorspecifiek wordt gewerkt aan de veiligheid op grond van in Europa aangescherpte wettelijke verplichtingen voor de offshore olie- en gaswinning en opsporing[6], die offshore olie- en gasoperators verplicht tot het opstellen van een Rapport inzake Grote Gevaren (RiGG) voor een productielocatie op zee. De richtlijn heeft tot doel de kans op zware ongevallen met betrekking tot olie- en gasactiviteiten verder te verkleinen en de gevolgen hiervan te beperken.
Zoals aangegeven in een brief verzonden aan uw Kamer op 6 december 2022[7] wordt olie- en gaslevering gezien als een vitale processen voor de leveringszekerheid van energie, bijvoorbeeld de processen transport, opslag en distributie. Voor verschillende gasproductielocaties op zee wordt onderzocht of de aanbieders vitaal zijn, onder andere, in het licht van nieuwe Europese wet- en regelgeving. De olieproductie in de Noordzee heeft een beperkte rol in de voorzieningszekerheid van olie en aardolieproducten in Nederland.
Zodra de productielocaties van gas op de Noordzee worden aangewezen als vitale energieaanbieders, dan vallen die onder de door het Ministerie van Justitie en Veiligheid gecoördineerde versterkte aanpak vitaal. Binnen deze aanpak werken overheden, bedrijven, organisaties en inlichtingen- en veiligheidsdiensten samen aan het beschermen van de vitale infrastructuur. Binnen het digitale domein zien de plichten voor vitale energieaanbieders, die krachtens de Wet beveiliging netwerk- en informatiesystemen (Wbni) worden aangewezen als aanbieder van een essentiële dienst (AED), onder meer op het treffen van passende maatregelen ter beveiliging van netwerk- en informatiesystemen, op grond van de Wbni. Aanwijzing als AED kan alleen als deze organisatie een vestiging in Nederland heeft. Daarnaast hebben alle vitale aanbieders krachtens diezelfde wet recht op bijstand (informatie, advies, etc.) bij digitale dreigingen of incidenten door het Nationaal Cyber Security Centrum (NCSC). Momenteel wordt ook gewerkt aan een (verdere) verankering van rechten en plichten binnen het digitale en fysieke domein door de nationale implementatie van de CER-richtlijn (Wet weerbaarheid kritieke entiteiten) en de herziene NIS2-richtlijn (Cyberbeveiligingswet) waarover op 31 januari 2024 de laatste stand van zaken met u is gedeeld door de Minister van Justitie en Veiligheid.[8] Zoals nu voorzien zal de Nederlandse wetgeving ter implementatie van deze richtlijnen in het tweede of derde kwartaal van 2025 in werking treden. Aan de weerbaarheid van vitale infrastructuur wordt naast de versterkte aanpak vitaal onder coördinatie van het Ministerie van Justitie en Veiligheid gewerkt aan de uitwerking van Rijksbrede beleidsinitiatieven zoals de Nationale Veiligheidsstrategie van het Koninkrijk der Nederlanden[9], Aanpak Statelijke Dreigingen[10] en de Nederlandse Cybersecuritystrategie[11].

Vraag 3
Hoe beoordeelt u de huidige internationale samenwerking bij de fysieke bescherming van maritieme infrastructuur, en zijn er plannen om deze samenwerking te intensiveren?

Antwoord 3
Het kabinet ziet en grijpt kansen om namens Nederland internationaal positie in te nemen en samen te werken op het gebied van de bescherming van maritieme infrastructuur, actief bij te dragen aan het NAVO-bondgenootschap en in andere samenwerkingsverbanden rondom de Noordzee.

---

[5] Kamerstuk 22 450, nr. 118
[6] Offshore Safety Directive 2013/30/EU, kortweg de OSD
[7] Kamerstuk 30 821, nr. 176
[8] Kamerstuk 22 112, nr. 3868.
[9] Veiligheidsstrategie voor het Koninkrijk der Nederlanden
[10] Aanpak statelijke dreigingen
[11] Nederlandse Cybersecuritystrategie 2022–2028

De Minister van Infrastructuur en Waterstaat heeft in april jl. samen met België, Denemarken, Duitsland, Groot-Brittannië en Noord-Ierland, en Noorwegen een verklaring ondertekend om gezamenlijk stappen te zetten om onze belangen op de Noordzee nog beter te beschermen. Ook wordt binnen de North Seas Energy Cooperation opgeroepen tot versterkte samenwerking op het gebied van offshore energieveiligheid, waaronder het delen van methodologieën, integratie van security by design en het gezamenlijk ontwikkelen van detectie-technologie.
De bescherming van onderzeese infrastructuur geniet ook binnen het NAVO-bondgenootschap de aandacht. In februari 2023 heeft de NAVO de Critical Undersea Infrastructure Coordination Cell opgericht die een coördinerende rol speelt bij de uitwisseling van informatie en afstemming van activiteiten tussen bondgenoten, partners en private sector partijen. Bovendien wordt er gewerkt aan de oprichting van een nieuw centrum (Maritime Centre for the Security of Critical Undersea Infrastructure). Daarnaast patrouilleren beide noordelijke vlootverbanden van de NAVO geregeld in de Noordzee en Oostzee en dragen daarmee bij aan beeldopbouw en afschrikking. Nederlandse marineschepen maken hier regelmatig deel van uit.
Tot slot maakt Nederland ook deel uit van de Joint Expeditionary Force (JEF), een multinationaal militair samenwerkingsverband van tien gelijkgezinde landen. Binnen deze organisatie wordt samengewerkt voor het tegengaan van spionage en sabotage tegen maritieme infrastructuur.

Vraag 4
Zijn er incidenten bekend waarbij Nederlandse offshore-installaties doelwit waren van spionage of verdacht gedrag, bijvoorbeeld met drones (Noorwegen, 2022)[12] of scheepsmanoeuvres, en wat zijn de geleerde lessen?

Antwoord 4
Geconstateerd is dat statelijke actoren actief zijn in het in kaart brengen van vitale marine infrastructuur op de Noordzee (zie ook in het antwoord op vraag 1 genoemde jaarverslagen van de inlichtingen en -veiligheidsdiensten). De betrokken organisaties op de Noordzee blijven waakzaam. Sabotage (digitaal of fysiek) van vitale processen kan de nationale veiligheid van Nederland bedreigen. Voor bedrijven in die sectoren maken de inlichtingen- en veiligheidsdiensten specifieke, op hen toegesneden dreigingsbeelden en (veiligheids)adviezen, zoals ook vermeld in de jaarverslagen van de AIVD en de MIVD. Vanwege veiligheidsredenen kan ik niet ingaan op individuele casussen.
Het kabinet zet in op interdepartementale, publiek-private en internationale samenwerking om met deze dreiging en eventuele incidenten om te gaan. Binnen het interdepartementale Programma Bescherming Noordzee Infrastructuur wordt onder coördinatie van de Minister van IenW gewerkt aan een geïntegreerde aanpak en concrete verbetering betreffende de veiligheid van de infrastructuur op de Noordzee. Onderdeel van het programma is herijking van de huidige crisis-en incidentbestrijdingsplannen op basis van de actuele dreiging.

Vraag 5, 8 en 9
Hoe beoordeelt u mogelijke cyberveiligheidsrisico's voor offshore windparken in Nederland?
Welke stappen onderneemt het kabinet om de samenwerking tussen universiteiten, cybersecurity experts, en de offshore windindustrie te versterken om cyberdreigingen aan te pakken?
Welk toekomstperspectief kan het kabinet schetsen om de weerbaarheid tegen cyberaanvallen in kritieke infrastructuur zoals windparken te blijven garanderen?

Antwoord 5, 8 en 9
Digitale dreigingen staan veelal niet op zichzelf en zijn onderdeel van een dynamisch, complex en breder dreigingslandschap. Cybersecuritybeleid in de energiesector wordt daarom zoveel mogelijk vanuit een risicogestuurde visie

[12] https://www.pbs.org/newshour/world/unidentified-drones-over-norways-offshore-platforms-fuel-fears-of-russian-threat

opgepakt. Dit beleid wordt vormgegeven in samenhang met organisaties zoals het Nationaal Cybersecurity Centrum (NCSC), de Rijksinspectie Digitale Infrastructuur, de Nationaal Coördinator Terrorismebestrijding en Veiligheid, de inlichtingen- en veiligheidsdiensten, TNO en de Topsector Energie/TKI offshore Energy.
Ten aanzien van offshore windparken betekent een groeiend opgesteld vermogen in de toekomst potentieel meer impact op de elektriciteitsvoorziening bij cyberincidenten. De noodzaak om cybersecurity verbeterd in te richten bij nieuwe infrastructuur op de Noordzee is evident en daarom heb ik verschillende maatregelen genomen.
Het net op zee en de daarop aangesloten windparken op zee zijn aangewezen als vitale energie-infrastructuur[13]. Toeleverende partijen voor het net op zee dienen daarom te voldoen aan de voorwaarden die zijn gesteld in de Veiligheidsstrategie voor het Koninkrijk der Nederlanden. Deze bepaling is opgenomen in het ontwikkelkader windenergie op zee[14], waarmee ik TenneT formeel opdracht geef voor de aanleg van het net op zee.
Binnen de vitale processen voor transport, distributie en productie van elektriciteit zijnzogeheten AED's aangewezen onder de Wbni. AED's moeten hierdoor onder meer voldoen aan de zorgplicht om hun netwerk- en informatiesystemen met passende maatregelen te beveiligen. De Rijksinspectie Digitale Infrastructuur houdt toezicht op de naleving van die plichten door deze aanbieders, zo ook op TenneT en de windparken op zee. Het NCSC staat deze aanbieders, net als andere vitale aanbieders, bij (door informeren, adviseren, etc.) in geval van cybersecuritydreigingen en -incidenten). Als gevolg van de herziening van de Netwerk- en Informatiebeveiligingsrichtlijn (NIS2-richtlijn) zullen meer energiebedrijven dan nu het geval is in de toekomst moeten voldoen aan wettelijke verplichtingen in relatie tot de beveiliging van hun netwerk- en informatiesystemen. Specifiek betekent dit dat bijvoorbeeld elektriciteitsbedrijven met productie-installaties (met uitzondering van micro- en kleine bedrijven) onder de verplichtingen in NIS2-richtlijn zullen komen te vallen. De uit de NIS2-richtlijn voortvloeiende verplichtingen bestaan uit een meldplicht bij significante incidenten en een plicht om passende maatregelen te nemen om risico's voor de beveiliging van netwerk- en informatiesystemen te beheersen. Hierbij dient ook rekening gehouden te worden met risico's die afkomstig zijn van leveranciers. Ter implementatie van NIS2-richtlijn zal naar verwachting in het tweede of derde kwartaal van 2025 de Cyberbeveiligingswet in werking treden.
Tevens wordt gewerkt aan de implementatie van de sectorspecifieke gedelegeerde handeling over grensoverschrijdende cybersecurity in de elektriciteitssector (Netcode). De Netcode stelt (ten opzichte van NIS2 concretere) bindende grensoverschrijdende cybersecurityvoorschriften vast voor elektriciteitsentiteiten die, wanneer zij mikpunt zouden worden van een cyberaanval, een risico vormen voor de stabiliteit van het Europese elektriciteitsnet. De Netcode zal naar verwachting in het vierde kwartaal van 2024 in werking treden. Onder andere Rijksinspectie Digitale Infrastructuur en de Autoriteit Consument en Markt zullen toezicht gaan houden en het Nationaal Cyber Security Centrum zal cyberhulp en bijstand verlenen.
Daarnaast gelden voor nieuwe windparken op zee, te beginnen met de kavels IJmuiden Ver Alpha en Beta, regels in het Kavelbesluit voor het hebben en het toepassen van een veiligheidsstrategie voordat de bouw van het windpark start geldend tot einde levensduur van het windpark. Onderdeel van deze verplichte veiligheidsstrategie zijn cybersecurity, economische veiligheid en fysieke weerbaarheid.
Tevens is de Uitvoeringsregeling windenergie op zee aangepast met ingang van 1 januari 2024, wat het mogelijk maakt om bij wijziging van zeggenschap of overdracht van vergunning een marktpartij te toetsen op risico's voor de openbare veiligheid, voorzieningszekerheid of leveringszekerheid, ook voordat een windpark operationeel is. Deze toets zal worden uitgevoerd bij de vergunningverlening van toekomstige windparken op zee en bij een wijziging van zeggenschap van reeds vergunde windparken op zee.
Als laatste hebben verschillende belanghebbenden FLECS (Field Lab Energy Cyber Security) geïnitieerd. FLECS wordt mogelijk in de toekomst een

---

[13] Kamerstuk 26 643, nr. 759
[14] Ontwikkelkader windenergie op zee

kenniscentrum voor cybersecurity in windenergie op zee. Het doel is kennis te ontwikkelen en oplossingen te creëren om een digitaal veerkrachtig offshore energiesysteem te bereiken samen met overheidspartijen, marktpartijen en academische en kennisinstellingen. Vanuit kennis- en innovatie doelstellingen van de Nederlandse Cybersecuritystrategie[15] is dit initatief ondernomen.

Vraag 6 en 7
Bent u zich ervan bewust dat als offshore windparken steeds meer in het energiesysteem worden geïntegreerd, de potentiële impact van een cyberaanval toeneemt? Kunt u antwoord uitgebreid toelichten?
Hoe schetst het kabinet de huidige balans tussen het standaardiseren voor efficiëntie en het diversifiëren om veiligheidsrisico's te minimaliseren?

Antwoord 6 en 7
De Nederlandse energie-infrastructuur is robuust en betrouwbaar. Bij het ontwerp van het Nederlandse elektriciteitssysteem wordt rekening gehouden met systeemveiligheid, zoals redundantie. Daarbij is het Nederlandse elektriciteitssysteem in hoge mate verbonden met elektriciteitssystemen van buurlanden. De maatregelen beschreven in het antwoord op vraag 5, 8 en 9 neem ik om de cyber veiligheid van offshore windparken te verhogen.
Ten aanzien van de potentiële impact van een cyberaanval op het energiesysteem is het daarnaast relevant toe te lichten dat TenneT op basis van Europese wetgeving reservevermogen inkoopt om eventuele uitval van elektriciteitscentrales (daarmee ook windparken op zee en bijbehorende platforms) op te vangen en systeemveiligheid te borgen. Vanaf het moment dat de momenteel geplande 2 GW transformatorplatformen aangesloten en gebruikt gaan worden, zal er (bij veel wind) meer reservevermogen door TenneT moeten worden ingekocht. Bovendien zorgt de geïntegreerde West-Europese elektriciteitsmarkt ervoor dat verstoringen op Europese schaal worden opgevangen[16] [17].
Nederland zet voor de komende windparken in op de 2GW HVDC platform standaard van Tennet. Net als voor de 0.7GW AC platform standaard, die voor de huidige parken wordt gebruikt, is (cyber)veiligheid in de ontwikkeling van de platformen een hoge prioriteit.

[15] Nederlandse Cybersecuritystrategie 2022–2028
[16] Ondersteunende diensten (Nederland) (tennet.eu)
[17] tennet.eu/nl/balanceringsmarkten