Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

Aanhangsel van de Handelingen

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

155

Vragen van de leden **Van Wijngaarden** en **Rajkowski** (beiden VVD) aan de Minister van Defensie over *het bericht «Minister Bijleveld en Admiraals Kramer en Tas uiten zorgen tijdens commando-overdracht»* (ingezonden 13 september 2021).

Antwoord van Minister **Kamp** (Defensie) (ontvangen 4 oktober 2021).

Vraag 1
Kunt u een nadere duiding geven van de waarschuwing dat «De aanwezigheid van Russische onderzeeërs in de Noordzee is reden tot zorg. Soms vertonen zij verdacht gedrag, wat erop kan duiden dat mogelijk datakabels worden afgetapt met vitale informatie over onze economie en veiligheid»?[1]

Antwoord 1
De opbouw van het Russisch militair vermogen oefent druk uit op het NAVO-bondgenootschap. Een specifieke dreiging gaat uit tegen onderzeese infrastructuur (bijvoorbeeld onderzeekabels). Russische entiteiten brengen deze infrastructuur in kaart en ondernemen activiteiten die mogelijk duiden op spionage en op voorbereidingshandelingen voor verstoring en sabotage.[2]

Vraag 2
Kunt u aangeven hoeveel datakabels en data er Nederland in- en uitstromen via de zee in vergelijking met andere relevante landen, en daarbij tenminste ingaan op Frankrijk, Groot-Brittannië, België, Denemarken, Noorwegen en Zweden? Kunt u hierbij ook aangeven in hoeverre het gaat om data van Nederlandse instellingen, dan wel data van buitenlandse entiteiten die via Nederland wordt doorgeleid?

Antwoord 2
Landen worden onderling met elkaar verbonden door glasvezelverbindingen over land en door de zee. Verbindingen door de zee zijn daarbij essentieel om continenten met elkaar te verbinden en om lange afstanden af te leggen. Er landen in Nederland op dit moment elf kabels aan waarvan zeven kabels Nederland met de oostkust van Groot-Brittannië verbinden, één kabel met het

[1] https://marineschepen.nl/nieuws/vice-admiraal-rene-tas-nieuwe-commandant-zeestrijdkrachten-090921.html
[2] Dreigingsbeeld Statelijke Actoren, Kamerstuk 30 821, nr. 124 Bijlage 968015, 04 februari 2021

ah-tk-20212022-155
ISSN 0921 - 7398
's-Gravenhage 2021

zuiden van Groot-Brittannië, twee kabels met Denemarken en één kabel met België. Groot-Brittannië is vervolgens met meerdere zeekabels verbonden met Noord-Amerika, Frankrijk, Spanje, België Ierland, IJsland, Denemarken en Noorwegen. Groot-Brittannië heeft een groot aantal kabels omdat het immers voor een groot deel afhankelijk is van connectiviteit via zeekabels. België is over zee enkel verbonden met Nederland en Groot-Brittannië. Zoals eerder vermeld is Denemarken verbonden met Nederland, verder heeft zij zeekabelverbindingen naar Noorwegen, Zweden, Duitsland, IJsland en Groot-Brittannië. Noorwegen heeft verder nog een zeekabelverbinding met Ierland. Zweden heeft gezien haar ligging alleen verbindingen via de Oostzee waardoor zij een zeekabelverbinding heeft met Estland, Letland, Litouwen, Polen en Finland. Een actueel overzicht van alle zeekabels is online te raadplegen[3].
Een enkele kabel kan tientallen terabits/s zo niet honderden terabits/s verzenden. Het is niet te zeggen hoeveel data daarvan data betreft van Nederlandse instellingen of bedrijven dan wel buitenlandse entiteiten. Wel kan gesteld worden dat verkeer over (Trans-Atlantische)zeekabels internationaal verkeer is en dat veel data dat al dan niet via Nederland gestuurd wordt, ook onderweg is naar andere landen.

Vraag 3
Deelt u de mening dat het zorgen voor de integriteit van deze data een vitaal nationaal belang is, ook op het moment dat deze data zich in een kabel bevinden die buiten de Nederlandse territoriale wateren ligt?

Antwoord 3
Zoals vermeld in het antwoord op vraag 1 vormen statelijke dreigingen een risico voor de veiligheid van zeekabels[4]. Zeekabels die data transporteren vormen een belangrijk onderdeel van de mondiale digitale ruimte. Zoals aangegeven in het *Cybersecuritybeeld Nederland 2021* zijn al onze digitale processen, waaronder vitale processen, sterk verweven en afhankelijk van deze mondiale digitale ruimte. Wanneer statelijke actoren op grote schaal onderzeese kabels aftappen voor inlichtingenvergaring of – ten tijde van conflicten – die kabels saboteren schendt dat de integriteit en exclusiviteit van data met mogelijk grote gevolgen voor het functioneren van digitale processen waaronder vitale processen[5]. Wanneer vitale processen worden aangetast kan dat gevolgen hebben voor de Nederlandse nationale veiligheid. Om die reden vindt het Kabinet, zoals aangegeven in de brief Veiligheid van zeekabels van 2 juli 2021, het belangrijk dat zeekabels veilig zijn en volgt de ontwikkelingen rond de veiligheid van zeekabels, zowel binnen als buiten de territoriale wateren, nauwlettend. In dat kader staat de veiligheid van zeekabels ook internationaal op de agenda bij de NAVO en de EU[6].

Vraag 4
Welke risico's zijn er voor de positie van Nederland als Europese data hub indien Nederland de integriteit van deze data niet kan beschermen?

Antwoord 4
De bescherming van data is geen uitdaging die zich beperkt tot Nederland en ook zeker niet tot zeekabels. Datastromen gaan via kabels over land door internet exchanges, datacenters en zeekabels en kunnen hiermee ook andere landen en continenten doorkruisen. Op het gebied van regulering van data gaat er de komende tijd met de uitwerking van de Digital Governance Act (DGA) en de Data Act (DA) in Europa veel veranderen juist ook om op het gebied van integriteit meer waarborgen te hebben. Deze regulering is namelijk gericht op het versterken van de governance van de interne markt voor data, op het beter delen en beschikbaar maken van data, en op het creëren van waarborgen voor beschermde data in de internationale context.

---

[3] Zie: https://www.submarinecablemap.com/.
[4] . Zie Dreigingsbeeld Statelijke Actoren, Kamerstuk 30 821, nr. 124 Bijlage 968015, 04 februari 2021.
[5] CSBN 2021, Kamerstuk 26 643, nr. 767, Bijlage CSBN 2021, 28 juni 2021
[6] Kamerbrief Veiligheid van zeekabels, Kamerstuk 26 643, nr 770, 02 juli 2021

Vraag 5
Betekent de inschatting dat «mogelijk datakabels worden afgetapt» dat er geen goed zicht is op de vraag of dit daadwerkelijk gebeurt?

Antwoord 5
Om operationele redenen kunnen we hierop geen nadere toelichting geven.

Vraag 6
Maken verdachte scheepsbewegingen in de regel onderdeel uit van diepzeewater onderzoeksinstituut GUGI of gebeurt het ook buiten dat verband?

Antwoord 6
Verdachte scheepsbewegingen gebeuren ook buiten dit verband.

Vraag 7
Welke maatregelen vinden er op dit moment plaats om datakabels te beschermen?

Antwoord 7
Zoals de Minister van Defensie eerder aan uw Kamer tijdens het Commissiedebat over de NAVO-top op 7 juni jl. heeft aangegeven, houdt ook de Noord-Atlantische Verdragsorganisatie (NAVO) de ontwikkelingen rond de veiligheid van zeekabels in de gaten. Ook in het onderwaterdomein geldt dat het versterken van de bondgenootschappelijke afschrikking en verdediging van belang is. Daarnaast is er onlangs in VN-verband door de United Nations Group of Governmental Experts (UNGGE) bij consensus de aanbeveling vastgesteld dat staten geen actie mogen ondernemen die opzettelijk kritieke infrastructuur beschadigt of anderszins het gebruik van kritieke infrastructuur schaadt, zoals infrastructuur tussen verschillende staten die essentieel is voor de algemene beschikbaarheid of integriteit van het internet.
Zeekabels die zijn aan te merken als onderdeel van openbare elektronische communicatienetwerken en -diensten moeten voldoen aan de gestelde zorgplichten in de Telecommunicatiewet (Tw).[7]
Gezien het grensoverschrijdende karakter van de zeekabels en de data die erover getransporteerd wordt, is Europese en internationale samenwerking essentieel.

Vraag 8
Zijn er afspraken gemaakt met de eigenaren van de kabels om elke storing te melden?

Antwoord 8
Aanbieders van openbare elektronische communicatienetwerken en -diensten op grond van artikel 11a.2, eerste lid Tw een meldplicht van incidenten. Dat betekent dat zij incidenten waarbij er sprake is van een inbreuk op de veiligheid of een verlies van integriteit, waardoor de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in belangrijke mate worden onderbroken, moeten melden bij toezichthouder Agentschap Telecom. Andere Europese lidstaten kennen een soortgelijke meldplicht.

Vraag 9
Wordt elke melding van een storing onderzocht en geattribueerd?

Antwoord 9
Agentschap Telecom beoordeelt meldingen die binnen komen op basis van de hiervoor genoemde Tw. Bij voldoende aanleiding kan een melding leiden tot de start van een onderzoek. In Nederland zijn geen incidenten met zeekabels gemeld.

---

[7] Een nadere verkenning is nodig naar of alle zeekabels zijn aan te merken als onderdeel van een openbaar communicatienetwerk en of bij het aanbieden van telecommunicatiediensten en transmissiediensten over een zeekabel altijd sprake is van een openbare elektronische communicatiedienst in de zin van de Tw. In de Kamerbrief van 2 juli 2021 Veiligheid van zeekabels is nader ingegaan op de regulering van de veiligheid van zeekabels, zie Kamerstukken 26 643, nr. 770.

Vraag 10
Welke instanties hebben mogelijk een rol bij het onderzoeken van incidenten? Spelen ook civiele elementen zoals de kustwacht, Nationaal Cyber Security Centrum (NCSC) of andere diensten een rol?

Vraag 10
Welke instanties hebben mogelijk een rol bij het onderzoeken van incidenten? Spelen ook civiele elementen zoals de kustwacht, Nationaal Cyber Security Centrum (NCSC) of andere diensten een rol?

Antwoord 11
Zoals eerder genoemd zijn hebben aanbieders van openbare elektronische communicatienetwerken en -diensten op grond van artikel 11a.2, eerste lid Tw een meldplicht van incidenten. Dat betekent dat zij incidenten waarbij er sprake is van een inbreuk op de veiligheid of een verlies van integriteit waardoor de continuïteit van openbare elektronische communicatienetwerken en openbare elektronische communicatiediensten in belangrijke mate worden onderbroken moeten melden bij toezichthouder Agentschap Telecom. In Nederland zijn geen incidenten gemeld bij het Agentschap Telecom op dit vlak.
Ook dienen aanbieders op grond van artikel 11.3 Tw technische en organisatorische maatregelen te treffen ten behoeve van de veiligheid en beveiliging van de door hen aangeboden netwerken en diensten in het belang van de bescherming van de persoonsgegevens en de bescherming van de persoonlijke levenssfeer van abonnees en gebruikers. Indien een inbreuk op die beveiliging zich voordoet heeft de aanbieder van een openbare elektronische communicatiedienst op grond van artikel 11.3a Tw de verplichting die inbreuk, onverwijld nadat hij die inbreuk heeft geconstateerd, te melden bij de Autoriteit Persoonsgegevens. Bij de Autoriteit Persoonsgegevens zijn geen meldingen bekend op dit vlak.

Vraag 12
Zijn bedrijven die eigenaar of beheerder zijn van de datakabels verplicht om detectiesystemen te hebben die het kunnen signaleren als een derde partij onder zee aan hun kabel zit?

Antwoord 12
Een aanbieder van openbare elektronische communicatienetwerken en -diensten moeten op basis van artikel 11a.1 van de Tw passende technische en organisatorische maatregelen nemen voor het beheersen van de risico's voor de veiligheid en integriteit van hun netwerken en diensten. Detectie kan daar een onderdeel van zijn, net zoals andere maatregelen zoals sterke encryptie.

Vraag 13
Als de verplichtingen uit bovenstaande vragen niet bestaan, kunt u dan aangeven of er landen binnen de NAVO of de EU zijn die een dergelijke verplichting wel hebben?

Antwoord 13
Zie antwoord vraag 12.

Vraag 14
Welke capaciteiten heeft de Nederlandse marine om Nederlandse datakabels te monitoren en te beschermen, en in hoeverre worden deze capaciteiten daarvoor ingezet?

Antwoord 14
De Koninklijke Marine heeft op dit moment geen capaciteiten om Nederlands datakabels te monitoren en te beschermen. De Koninklijke Marine beschikt wel over capaciteiten (als fregatten, onderzeeboten en NH90 helikopters) voor indirecte datakabel bescherming en kan daarmee oppervlakte eenheden en onderzeeboten detecteren, volgen en eventueel neutraliseren.

Vraag 15
Welke meerwaarde bieden onderzeeboten bij het beschermen van datakabels?

Antwoord 15
Datakabels, of in bredere zin onderzeese infrastructuur, kunnen worden bedreigd door onderzeeboten die speciaal zijn toegerust voor dit doel. Op deze manier kan een potentiele tegenstander die over zulke onderzeeboten beschikt, onopgemerkt en dus ongehinderd zijn doel bereiken. Deze heimelijke wijze van het bedrijven van offensieve seabed warfare vormt een actuele en reële dreiging. Een effectief middel voor het bestrijden van onderzeeboten, zijn eigen onderzeeboten. Dit is een kerntaak van de huidige en toekomstige onderzeeboten van de Koninklijke Marine. De meerwaarde van onze eigen onderzeeboten is onder andere het kunnen detecteren, monitoren en eventueel neutraliseren van onderzeeboten gericht op seabed warfare. De wetenschap alleen al van mogelijke inzet van onderzeeboten dwingt de opponent zijn eigen eenheden te beschermen, waardoor hij zijn heimelijke capaciteiten minder makkelijk kan inzetten.

Vraag 16
Welke meerwaarde biedt een gespecialiseerd monitoringsschip zoals de Britse marine gaat kopen als aangekondigd in de Britse defensievisie «Defence in a Competitive Age»?

Antwoord 16
Over de concrete meerwaarde van het genoemde monitoringsschip kan ik u op dit moment niets toelichten omdat ik geen zicht heb op de volledige capaciteit hiervan.

Vraag 17
In hoeverre zijn Nederlandse datakabels straks minder beveiligd dan de Britse als Nederland niet over een dergelijk schip beschikt?

Antwoord 17
Hierop kan ik u geen concreet antwoord geven omdat ik op dit moment geen volledig zicht heb op de capaciteit van de Britten op dit vlak. Wel kan ik aangeven dat de beveiliging van de fysieke zeekabels en de data die hierover getransporteerd wordt altijd een internationale aangelegenheid zal zijn. We zijn hierover in gesprek binnen het bondgenootschap.

Vraag 18
Welk risico's voor sabotage van de kabels zijn er? Kunt u hierbij ook ingaan op de mogelijkheid dat verdachte Russische activiteiten niet alleen dienen voor het aftappen van gegevens, maar ook dienen als verkenning voor mogelijke latere sabotage, of dienen om apparatuur te plaatsen die eventueel in een later stadium de kabels kan saboteren?

Antwoord 18
Er is een dreiging tegen onderzeese kabels en andere zeebodem-gebonden infrastructuur. Over de precieze aard van deze potentiele dreiging kunnen we om operationele redenen niet in gaan.

Vraag 19
Welke risico's en kwetsbaarheden brengen bovengenoemde mogelijke Russische voorbereidingshandelingen met zich mee voor de geopolitieke en militaire positie van Nederland en de NAVO in het geval van een gewapend conflict of een escalatie van spanningen door middel van hybride middelen?

Antwoord 19
In de huidige gemondialiseerde samenleving, waarin het economische en maatschappelijke belang van met name internetverkeer steeds verder toeneemt, is het essentieel dat de veiligheid van zeekabels gegarandeerd blijft. De NAVO houdt de ontwikkelingen rond de veiligheid van zeekabels in de gaten. Zeekabels spelen thans ook een rol bij de civiele en militaire communicatie tussen NAVO-bondgenoten. De bondgenootschappelijke afschrikking en verdediging is daarom ook in het onderwaterdomein van

groot belang. Sinds 2014 heeft de NAVO de bondgenootschappelijke afschrikking en verdediging versterkt. De NAVO heeft in dit kader de beschikking over zowel militaire als niet-militaire capaciteiten en middelen om uitdagingen en dreigingen te adresseren in de vijf operationele domeinen van het bondgenootschap, die naast zee ook land, lucht, de ruimte en cyber betreffen.

Vraag 20
Kunt u bovenstaande vragen afzonderlijk beantwoorden?

Antwoord 20
Ja.