Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2022–2023

Aanhangsel van de Handelingen

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

2505

Vragen van de leden **Brekelmans**, **Koerhuis**, **Rajkowski** en **Valstar** (allen VVD) aan de Ministers van Buitenlandse Zaken, van Binnenlandse Zaken en Koninkrijksrelaties, van Defensie en van Infrastructuur en Waterstaat over *het bericht ««Verdachte» Chinese kranen staan ook in Nederlandse havens: zorgen om spionage»* (ingezonden 13 maart 2023).

Antwoord van Minister **Harbers** (Infrastructuur en Waterstaat), mede namens de Ministers van Buitenlandse Zaken, van Binnenlandse Zaken en van Koninkrijksrelaties en van Defensie (ontvangen 8 mei 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2106.

Vraag 1
Bent u bekend met het bericht ««Verdachte» Chinese kranen staan ook in Nederlandse havens: zorgen om spionage»?[1]

Antwoord 1
Ja.

Vraag 2
Hoe beoordeelt u de in het artikel genoemde zorgen dat China op deze manier gevoelige informatie kan vergaren over militaire transporten of activiteiten in havens kan platleggen?

Antwoord 2
Het kabinet neemt de in het artikel genoemde zorgen serieus. Het is essentieel dat onze havens hun belangrijke maritiem-logistieke hub-functie voor onze economie en ten behoeve van het faciliteren van militaire transporten onafhankelijk en veilig kunnen uitoefenen. Er wordt onderzocht in hoeverre de in het artikel genoemde zorgen gelden voor de Nederlandse context, zie ook het antwoord op vragen 3, 4 en 5.
In brede zin heeft het kabinet aandacht voor de invloed van China in Nederlandse- en Europese havens. Hierover is uw Kamer eerder geïnformeerd in de Kamerbrief

[1] Silvan Schoonhoven, ««Verdachte» Chinese kranen staan ook in Nederlandse havens: zorgen om spionage», 10 maart 2023, https://www.telegraaf.nl/nieuws/938215803/verdachte-chinese-kranen-staan-ook-in-nederlandse-havens-zorgen-om-spionage

ah-tk-20222023-2505
ISSN 0921 - 7398
's-Gravenhage 2023

«Reactie rapport «Navigating an uncertain future»» (Kamerstuk 35 207, nr. 62). Daarbij werkt het kabinet doorlopend aan het verhogen van het bewustzijn bij partijen in de sector over de belangrijkste dreigingen (onder meer vanuit China), spionagedoelwitten- en werkwijzen van statelijke actoren en het verhogen van weerbaarheid. De AIVD waarschuwt regelmatig voor de risico's voor het gebruik van hard- en software bij de uitwisseling van gevoelige informatie – met name binnen de vitale infrastructuur – wanneer digitale apparatuur afkomstig is uit landen met een offensief cyberprogramma gericht tegen de Nederlandse belangen. De grootste digitale dreiging gaat uit van China, Rusland en in mindere mate van Iran en Noord-Korea.[2] Hier wordt ook op ingegaan in de Kamerbrief «Aanpak statelijke dreigingen en aanbieding dreigingsbeeld statelijke actoren 2» (Kamerstuk 30 821, nr. 175) en het AIVD-jaarverslag 2022.

Vraag 3, 4 en 5
Is het mogelijk om vanuit de Shanghai Zhenhua Heavy Industries Company Limited (ZPMC)-faciliteiten in China digitale toegang te krijgen tot de kranen, en tot de informatie die zij verwerken, tijdens bijvoorbeeld onderhoud of updates?
Zijn de ZPMC-kranen in de Rotterdamse haven op enigerlei wijze digitaal verbonden met een servicecentrum, controlecentrum of andere faciliteit van ZPMC, dan wel in Nederland, China of een derde land?
Tot wat voor soort informatie kunnen de ZMPC-faciliteiten in China via de ZMPC-kranen in de Rotterdamse haven toegang krijgen?

Antwoord 3, 4 en 5
Het kabinet vindt het cruciaal dat de fysieke en digitale processen in de haven, waaronder de software op kranen, zo veilig mogelijk zijn ingericht. De havenfaciliteiten (bedrijven die zeeschepen afhandelen) zijn verantwoordelijk voor de beveiliging van computersystemen- en netwerken binnen hun eigen werkgebied.
Of het mogelijk is om vanuit de ZPMC-faciliteiten in China digitale toegang te krijgen tot de kranen, of dat deze op enigerlei wijze verbonden zijn of toegang hebben tot informatie in de Rotterdamse haven, wordt onderzocht in afstemming met het Havenbedrijf Rotterdam. Dit wordt betrokken bij een reeds bestaand interdepartementaal traject waarin aan de hand van een risicoanalyse wordt gekeken naar de te beschermen belangen, dreigingen en weerbaarheid van de Rotterdamse haven, welke risico's hieruit naar voren komen en hoe hier eventueel vervolg aan gegeven moet worden. Dit traject en onderzoek wordt gecoördineerd vanuit het Ministerie van Infrastructuur en Waterstaat en de Nationaal Coördinator Terrorismebestrijding en Veiligheid, in samenwerking met de Ministeries van Defensie, Economische Zaken en Klimaat en Buitenlandse Zaken. Naar verwachting wordt het onderzoek in het najaar van 2023 afgerond.

Vraag 6
Valt het gebruik van de ZPMC-kranen in de Rotterdamse haven onder enige vorm van veiligheidsscreening of toetsing? Zo ja, welke? Zo nee, waarom niet?

Antwoord 6
Op basis van de Havenbeveiligingswet (Hbw) moeten de risico's van radio en telecommunicatiesystemen, inclusief computersystemen en netwerken worden meegenomen in de risicobeoordelingen van havenfaciliteiten. In de beveiligingsplannen van de havenfaciliteiten worden de mitigerende maatregelen beschreven om risico's af te dekken.
De havenmeester van de haven van Rotterdam is als Havenbeveiligingsfunctionaris (Port Security Officer) verantwoordelijk voor de uitvoering en naleving van de Hbw door havenfaciliteiten in de haven. Deze taak voert de havenmeester uit in mandaat van de burgemeester als autoriteit voor havenveiligheid. Vanuit deze verantwoordelijkheid toetst de havenmeester de risicobeoordelingen van de havenfaciliteiten en houdt hij toezicht op de uitvoering

[2] Jaarverslagen AIVD 2019, 2021 en 2022 (p. 29 en 32–33). Zie ook *Dreigingsbeeld Statelijke Actoren 2, publicatie AIVD, MIVD en NCTV, november 2022, p. 5 en 34.*

van de beveiligingsplannen van de havenfaciliteiten. De Inspectie Leefomgeving en Transport (ILT) houdt tweedelijns toezicht op de uitvoering en naleving van de Hbw door de burgemeester. De beoordeling van deze werkwijze wordt betrokken bij het lopende onderzoek waar in het antwoord op de vragen 3, 4 en 5 naar wordt verwezen.

Vraag 7
Zijn de ZPMC-kranen verbonden met het Chinese logistieke dataplatform Logink, of komt informatie over wat zij doen op enigerlei andere wijze terecht bij Logink?

Antwoord 7
Het is op dit moment nog niet duidelijk of ZPMC-kranen verbonden zijn met Logink en/of informatie over activiteiten van de kranen terecht kan komen bij Logink. Dit vereist nader onderzoek. Zie antwoord op vraag 3, 4 en 5.

Vraag 8
In hoeverre werkt de Rotterdamse haven samen met Logink, en kunt u schetsen welke data op welke wijze wordt gedeeld?

Antwoord 8
Het Havenbedrijf Rotterdam heeft geen samenwerking noch data-uitwisseling met Logink. Ook het Port Community Systeem «Portbase» werkt niet samen met Logink en er wordt geen data gedeeld.

Vraag 9 en 10
Klopt het dat Logink gratis ter beschikking wordt gesteld, en dat het zo lastig is voor eventuele Westerse alternatieven om succesvol te zijn op bijvoorbeeld de Europese markt?
Deelt u de analyse dat via het gratis ter beschikking stellen van Logink China een dominante positie kan krijgen over datastromen rond internationale handel?

Antwoord 9 en 10
Voor zover bekend wordt Logink gratis beschikbaar gesteld aan lokale, Chinese partijen in China. Het is met name een supply chain visibility platform voor Chinese klanten, gericht op Chinese handelsstromen.
Om handel en transport te ondersteunen ontwikkelen de meeste landen handelsfacilitatieplatformen die fungeren als centraal punt voor scheepsgerelateerde meldingen (Maritime Single Window) voor handel en transport. Er is een uitgebreid landschap van systemen waarbij voor elk van de platformen veiligheid en integriteit van de systemen hoge prioriteit heeft. In dit landschap is het lastig een groot marktaandeel wereldwijd te bemachtigen. Daarbij is de neutraliteit van de platformen van belang voor de betrokken marktpartijen.
In Nederland wordt het handelsfacilitatieplatform grotendeels gevormd door een samenwerking tussen belangrijke overheidssystemen (zoals de Douane) en de Port Community Systemen (PCS) van de mainports, zoals Portbase voor de havens van Rotterdam en Amsterdam en Cargonaut voor Schiphol. Met de ontwikkeling van de Basis Data Infrastructuur (BDI), een publiek-privaat initiatief, wordt ingezet om de samenwerking tussen deze platformen verder te intensiveren en gebruik verder te stimuleren.

Vraag 11
Hoe verhoudt zich deze staatsgesteunde gratis levering van Logink tot de verordening buitenlandse subsidies, en welke mogelijkheden zijn er eventueel om tegen Logink maatregelen te nemen?

Antwoord 11
De verordening buitenlandse subsidies biedt mogelijkheden om in te grijpen indien er sprake is van overheidssteun uit derde landen aan bedrijven die de concurrentie op de interne markt verstoort. Daarmee draagt de verordening buitenlandse subsidies bij aan de economische veiligheid. De verordening is per 12 januari van dit jaar in werking getreden. De Europese Commissie kan vanaf 12 juli 2023 op basis van de «ex-officio» bevoegdheid ambtshalve

onderzoeken starten. De meldplicht bij overnames en aanbestedingen geldt vanaf 12 oktober 2023.
De verordening buitenlandse subsidies bevat drie componenten, waarvan in dit geval mogelijk het ambtshalve onderzoek relevant is. Op basis van deze ambtshalve (ex-officio) bevoegdheid kan de Commissie achteraf subsidies onderzoeken in alle marktsituaties, waar er sprake is van concurrentieverstoring. Dit kan zij doen op basis van signalen uit de markt.
De Commissie is de toezichthouder voor deze verordening en het is dan ook aan haar om te besluiten om over te gaan tot een onderzoek als er sprake is van concurrentieverstoring op de interne markt. De mogelijke concurrentieverstoring op de interne markt vormt de aanleiding voor een dergelijk onderzoek van de Commissie. Mogelijke maatregelen die de Commissie kan opleggen zijn herstelmaatregelen of het aangaan van verbintenissen met ondernemingen op basis waarvan de verstoring verholpen wordt.

Vraag 12
Welke Westerse alternatieven zijn beschikbaar op bijvoorbeeld de Europese Markt, en welke mogelijkheden zijn er eventueel om Westerse alternatieven te stimuleren?

Antwoord 12
EU-lidstaten hebben over het algemeen het faciliteren van handel op eigen wijze en met eigen platformen ingericht. De meeste Lidstaten met grote handelsstromen in de EU hebben Port Community Systemen (PCS) om transport en logistiek te ondersteunen en data uitwisseling tussen alle partijen in de logistiek en met overheden mogelijk en makkelijk te maken. Op deze wijze kan de logistiek veiliger, efficiënter en duurzamer opereren. In Nederland hebben de mainports daarvoor de platformen Cargonaut (Schiphol) en Portbase (havens van Amsterdam en Rotterdam) ontwikkeld. Portbase is een non-profit organisatie.

Vraag 13
In hoeverre zijn de ZPMC-kranen ook actief in de delen van de Rotterdamse haven die worden gebruikt voor militair transport van Noord-Atlantische Verdragsorganisatie (NAVO)-partners, en zijn deze delen van de haven ook verbonden met Logink?

Antwoord 13
Havenbedrijf Rotterdam heeft navraag gedaan bij de bedrijven in de haven en bevestigt dat ZPMC-kranen niet actief zijn in delen van de Rotterdamse haven die gewoonlijk worden gebruikt voor militair transport van NAVO-partners. Deze delen zijn ook niet verbonden met Logink.

Vraag 14
In hoeverre zijn de ZMPC-kranen ook actief in de haven van Vlissingen in de delen die worden gebruikt voor militair transport van NAVO-partners?

Antwoord 14
Havenbedrijf North Sea Port heeft navraag gedaan bij de bedrijven in de haven en bevestigt dat ZPMC-kranen niet actief zijn in de haven van Vlissingen.

Vraag 15
Bent u het eens met de leden van de VVD-fractie dat gevoelige informatie over militair transport van NAVO-partners goed moet worden beschermd?

Antwoord 15
Ja, daarover ben ik het eens met de VVD-fractie.

Vraag 16
Overweegt u daarom nadere maatregelen te nemen? Zo ja, welke? Zo nee, waarom niet?

Antwoord 16
Indien het interdepartementale onderzoek uitwijst dat aanvullende maatregelen nodig zijn om informatie over militaire transporten te beschermen, dan zullen deze in overleg met de betreffende havens waar nodig worden toegepast. Daarbij zullen per oktober 2024 twee nieuwe EU-richtlijnen in Nederlandse wetgeving zijn geïmplementeerd die gericht zijn op de verbetering van de digitale en fysieke weerbaarheid van bedrijven en organisaties, respectievelijk de *Network and Information Security (NIS2) Directive* en de *Critical Entities Resilience (CER) Directive.* De NIS2 en de CER bieden de nodige wettelijke kaders voor het versterken en waarborgen van de digitale en fysieke weerbaarheid van onze havens en haven-logistieke ketens.
De Europese Commissie heeft daarnaast in maart 2023 aangekondigd de European Maritime Security Strategy (EUMSS) uit 2014 te willen actualiseren. De strategie beoogt de EU maritieme belangen te beschermen tegen dreigingen door moedwillig handelen in het maritieme domein. In de actualisatie is ook specifieke aandacht voor het belang van het mitigeren van risico's van strategische afhankelijkheden als gevolg van buitenlandse investeringen in EU maritieme logistieke infrastructuur, met name zeehavens. Nederland heeft hier nadrukkelijk aandacht voor gevraagd. Hierover is de Kamer op 21 april 2023 middels een aanbiedingsbrief informatie over nieuwe voorstellen Europese Commissie geïnformeerd.[3]

Vraag 17
Kunt u deze vragen beantwoorden voorafgaand aan het Commissiedebat over China van 5 april?

Antwoord 17
De vragen vereisten zorgvuldig onderzoek in samenwerking met de sector en verdere interdepartementale afstemming. Om deze reden kon niet binnen de gebruikelijke termijn geantwoord worden. Op 3 april is met een uitstelbrief aan Uw Kamer uitstel gevraagd voor de beantwoording van de Kamervragen.

[3] Aanbiedingsbrief informatie over nieuwe voorstellen Europese Commissie (21 april 2023), fiche 1: Mededeling hernieuwde Maritieme Veiligheidsstrategie EU