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

1659

Vragen van de leden **Piri** en **Kathmann** (GroenLinks-PvdA) aan de Ministers van Buitenlandse Zaken en van Binnenlandse Zaken en Koninkrijksrelaties over *nieuwssites die al jaren pro-Chinese desinformatie verspreiden* (ingezonden 15 februari 2024).

Antwoord van Staatssecretaris **Van Huffelen** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Ministers van Binnenlandse Zaken en Koninkrijksrelaties en van Economische Zaken en Klimaat (ontvangen 6 mei 2024). Zie ook Aanhangsel Handelingen, vergaderjaar 2023–2024, nr. 1208.

Vraag 1
Bent u bekend met het artikel «Netwerk van nieuwssites verspreidt al jarenlang pro-Chinese desinformatie, ook in Nederland»?[1]

Antwoord 1
Ja

Vraag 2
Was u bekend met het netwerk van nieuwssites die zijn opgezet door het Chinese pr-bedrijf Haimai om desinformatie te verspreiden? Zo nee, moet de Rijksbrede strategie effectieve aanpak van desinformatie worden verbeterd zodat dit soort desinformatiecampagnes eerder aan het licht komen en effectief worden aangepakt?

Antwoord 2
Voor het verschijnen van de artikelen «Netwerk van nieuwssites verspreidt al jarenlang pro-Chinese desinformatie, ook in Nederland» en «NVJ: netwerk pro-Chinese nieuwssites leidt tot desinformatie» was ik niet bekend met dit netwerk van nieuwssites opgericht door het Chinese pr-bedrijf Haimai.
In de brief van 9 november 2023 heeft het kabinet al aangekondigd te onderzoeken of, en zo ja hoe, de Rijksbrede aanpak van desinformatie over

[1] De Volkskrant, 7 februari 2024, «Netwerk van nieuwssites verspreidt al jarenlang pro-Chinese desinformatie, ook in Nederland» (https://www.volkskrant.nl/nieuws-achtergrond/netwerk-van-nieuwssites-verspreidt-al-jarenlang-pro-chinese-desinformatie-ook-in-nederland~b9eac34c/#:~:text=Een%20netwerk%20van%20123%20nieuwssites,die%20kritisch%20staan%20tegenover%20Beijing)

ah-tk-20232024-1659
ISSN 0921 - 7398
's-Gravenhage 2024

de kernprocessen van de democratie versterkt moet worden.[2] Uw Kamer wordt hier dit voorjaar over geïnformeerd in de Voortgangsbrief over deze strategie.

Vraag 3
Kunt u achterhalen hoeveel bezoekers deze nieuwssites per jaar ongeveer hebben?

Antwoord 3
Het onderzoek van Citizen Lab «PAPERWALL: Chinese Website Posing as Local News Outlets Target Global Audiences with Pro-Bejing Content»[3] waarop de artikelen «Netwerk van nieuwssites verspreidt al jarenlang pro-Chinese desinformatie, ook in Nederland» en «NVJ: netwerk pro-Chinese nieuwssites leidt tot desinformatie» gebaseerd zijn, richtte zich o.a. op het bereik van deze websites.
Voor de beantwoording van deze vraag is contact gezocht met de onderzoeker van Citizen Lab. De organisatie onderzocht door middel van verschillende publieke en open source tools, waaronder hypestat.com (een web platform en browserextensie), de bezoekersaantallen van de websites binnen het netwerk. Van alle websites verscheen alleen een aantal generieke Engelstalige websites «wdpp[.]org» of «euleader[.]org», in de statistieken, met een gemiddelde van 50 bezoekers per dag. Dit hoeven geen unieke bezoekers te zijn, dit kan ook dezelfde persoon zijn die de website een aantal keer bezoekt. Dat andere websites, waaronder «nlpress.org» en «greaterdutch.com», niet in de statistieken verschijnen betekent dat hun bereik verwaarloosbaar is.

Vraag 4
Bent u in contact met de andere dertig landen waar het netwerk actief is geweest en zo ja, neemt u initiatief om gezamenlijk deze desinformatiecampagne tegen te gaan?

Antwoord 4
Het kabinet staat zowel bilateraal als in multilateraal verband in nauw contact met bevriende landen over de problematiek van buitenlandse inmenging en Foreign Information Manipulation and Interference (FIMI). Dit betreft o.a. uitwisseling van informatie in EU-verband, binnen het NAVO-bondgenootschap en via het Hybrid Centre of Excellence. Via deze weg worden FIMI-campagnes gesignaleerd, vindt uitwisseling plaats over de verschillende verschijningsvormen van FIMI en worden *best practices* gedeeld over het verhogen van de weerbaarheid en responsmogelijkheden.

Vraag 5
Welke poortwachters zijn er die toezicht houden op nieuw aangemaakte websites? In hoeverre is het mogelijk om in een vroeg stadium al te signaleren dat een nieuwe website onderdeel is van een buitenlandse desinformatiecampagne? Speelt het daarbij een rol of een website in het.com,.org of.nl domein wordt geregistreerd?

Antwoord 5
Op het moment dat een domeinnaam wordt geregistreerd in het domeinnaamsysteem (DNS) is nog niet bekend voor welke diensten, bijvoorbeeld email of een website, de domeinnaam gebruikt zal gaan worden. Het is dus bij de registratie van een domeinnaam niet mogelijk om het karakter van de website te duiden. Daarnaast breng het vooraf controleren van inhoud van websites de vrijheid van meningsuiting in gevaar.
Wel zijn er binnen de domeinnaamindustrie afspraken gemaakt t.a.v. het voorkomen van DNS misbruik. Hieronder valt een breed spectrum van misbruik waarbij de domeinnaam zelf onderdeel vormt van het misbruik. Bijvoorbeeld *phishing* m.b.v. domeinnamen die veel lijken op de naam van bestaande gerenommeerde websites (o.a. banken, webwinkels, overheid).

---

[2] Kamerbrief weerbaarheid verkiezingsproces Tweede Kamerverkiezingen 2023 – file (overheid.nl)
[3] PAPERWALL: Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content – The Citizen Lab

Veel domeinnaam- registers en tussenpersonen (*registrars*) maken bij de aanvraag van een domeinnaam een risicoanalyse op basis van de geregistreerde domeinnaam en de gegevens van de aanvrager. Indien er twijfels zijn over de aanvraag kunnen extra verificatiestappen worden verricht om bijvoorbeeld meer te weten te komen over de identiteit van de aanvrager en diens intenties.
Deze methode wordt onder de naam RegCheck toegepast op registraties van.nl domeinnamen. De Stichting Internetdomeinregistratie Nederland (SIDN) die de registratie van.nl verzorgt, geeft op haar website aan dat vorig jaar ruim 8000 domeinnamen i.v.m. DNS-misbruik offline zijn gehaald. Dit systeem richt zich op het voorkomen van DNS misbruik. Desinformatie of meer algemeen ongewenste inhoud van websites valt niet onder de definitie van DNS-misbruik.
Van andere top-level domeinnamen zijn geen gegevens bekend. Wel zijn er recentelijk door ICANN, de internationale organisatie die deze top-level domeinnamen uitgeeft, een aantal contractuele aanpassingen gedaan wat de registers van deze domeinnamen en hun tussenpersonen verplicht meer maatregelen te nemen om DNS misbruik tegen te gaan en sneller en adequaat te reageren op meldingen over misbruik.
Het ligt niet voor de hand om beheerders van domeinnamen een verantwoordelijkheid te geven in de bestrijding van desinformatie. De enige interventie die beheerders van domeinnamen tot hun beschikking hebben is om een domein in het geheel ontoegankelijk te maken. Als een domein tevens wordt gebruikt voor de verspreiding van legale inhoud dan kan het ontoegankelijk maken een disproportionele beperking van de vrijheid van meningsuiting inhouden.

Vraag 6
Worden deze websites nader onderzocht om dergelijke nepsites voortaan sneller te detecteren?

Antwoord 6
«Nepsites» als zodanig is geen bestaand fenomeen. Het gaat hier om websites die misleidende informatie bevatten. Het vooraf controleren van de inhoud van een website brengt vrijheid van meningsuiting in gevaar. Daarnaast is het bestempelen van desinformatie als zodanig en factchecken geen taak van overheden. Dit ligt bij factcheckers en onderzoeksjournalistiek. Want vrijheid van meningsuiting en persvrijheid blijven centraal staan. Wanneer blijkt dat de inhoud van, bijvoorbeeld een website, de nationale veiligheid, volksgezondheid, maatschappelijke en/of economische stabiliteit in gevaar brengt, kan de overheid wel optreden en desinformatie tegenspreken.

Vraag 7
Zijn de critici van de Chinese overheid die door de desinformatiecampagne worden geïmpliceerd op de hoogte gesteld dat zij genoemd worden? Worden er maatregelen genomen om hen waar nodig hulp te bieden?

Antwoord 7
Buitenlandse Zaken staat in contact met mensenrechtenverdedigers en (vertegenwoordigers van) de Chinese diaspora in Nederland. Onder andere via deze weg komen signalen binnen wanneer er sprake is van negatieve gevolgen van desinformatie, intimidatie via familie in China of bedreiging. Personen in Nederland die te maken krijgen met strafbare feiten kunnen altijd aangifte of melding doen bij de politie.

Vraag 8
Welke mogelijkheden heeft u om zulke desinformatiecampagnes tegen te gaan? Biedt de Digital Service Act (DSA) voldoende instrumenten om dit soort desinformatiecampagnes tegen te gaan?

Antwoord 8
De Digital Services Act (DSA) is onder meer van toepassing op hostingdiensten en online platforms voor zover die diensten worden aangeboden aan afnemers in de Unie. Een hostingdienst is een dienst die op verzoek van een afnemer informatie opslaat. Een online platform is een hostingdienst die informatie op verzoek van afnemers informatie opslaat en verspreidt bij het

publiek. De websites die worden beschreven in de berichtgeving van de Volkskrant lijken hier niet aan te voldoen omdat de websites werden gebruikt door de eigenaren om zelf informatie te verspreiden. Er vindt geen opslag en/of verspreiding van informatie plaats op verzoek van afnemers van de dienst. Zodoende is de DSA waarschijnlijk niet van toepassing op deze websites.
De websites maakten geen gebruik van online platforms, zoals sociale media, om hun content te verspreiden. Daarom zijn de systeemrisico-analyses die zeer grote online platforms als Facebook, Instagram en TikTok jaarlijks moeten verrichten, waarbij ze ook aandacht moeten hebben voor de verspreiding van dit soort desinformatie, in dit geval niet relevant.
In het voorjaar wordt de Kamer geïnformeerd over de voortgang van de aanpak desinformatie. Hierin worden nieuwe acties voorgesteld om de negatieve impact van desinformatie tegen te gaan.

Vraag 9
Kunt u achterhalen of deze nieuwswebsites ook tegen betaling gepromoot zijn op sociale media, en zo ja, hoe groot het bereik van deze posts is geweest en, waar relevant, in het geval van betaalde promotie en advertenties, hoeveel platforms als Facebook en X daaraan verdiend hebben?

Antwoord 9
Artikel 39 van de DSA verplicht aangewezen zeer grote online platforms, waartoe ook grote sociale media bedrijven horen, om de advertenties die op hun dienst worden getoond in een doorzoekbaar register vast te leggen. In dat register moet, naast de inhoud van de reclame, onder meer informatie worden opgenomen over de natuurlijke of rechtspersoon namens wie de reclame wordt getoond en de natuurlijke of rechtspersoon die voor de reclame heeft betaald. Ook de periode waarin de advertentie werd getoond en bepaalde demografische gegevens over het publiek moeten in het register worden opgenomen.
Vanuit de advertentiebibliotheek van X en Meta (Facebook) is geen aanwijzing gevonden dat de websites of HaiMai van sociale media gebruik hebben gemaakt om hun content te verspreiden. Dit is bevestigd door CitizenLab, dat de oorspronkelijke analyse deed en daar uitgebreid naar heeft gekeken. Daarnaast gaf de organisatie aan dat er ook geen officiële sociale media accounts zijn die kunnen worden gelinkt aan een van de websites uit het netwerk.

Vraag 10
Deelt u de mening dat de huidige gedragscode desinformatie als officiële gedragscode onder de Digital Services Act nu te weinig specifieke, vage tekst en kernprestatie-indicatoren bevat op het gebied van aanbevelingsalgoritmes? Zo ja, bent u het eens dat de gedragscode in combinatie met de DSA op het punt van desinformatie en aanbevelingssystemen in de praktijk niet te handhaven is? Zo ja, bent u van mening dat de gedragscode desinformatie op dat punt moet worden aangepast?

Antwoord 10
Op dit moment is de huidige gedragscode desinformatie nog geen officiële gedragscode onder de DSA. Daardoor zijn de onderdelen van de DSA die aansluiting bij, en naleving van, de gedragscode stimuleren nog niet van toepassing. Naar mijn weten is de Europese Commissie bezig om de omzetting naar een gedragscode onder de DSA voor te bereiden. Het is daarom te vroeg om uitspraken te doen over de effectiviteit van de gedragscode.

Vraag 11
Staat u open voor het aannemen van meer effectieve maatregelen tegen aanbevelingssystemen, bijvoorbeeld het verbieden van algoritmen gebaseerd op interactie, waarvan we weten dat ze in de praktijk desinformatie in de hand werken? En dat de verplichte niet-gepersonaliseerde aanbevelingssystemen in Artikel 29 DSA altijd de standaard zijn in plaats van gepersonaliseerde aanbevelingssystemen? Zou u hiervoor willen pleiten in de Europese Unie (EU)?

Antwoord 11
Ik ga ervan uit dat de vragenstellers doelen op artikel 38 DSA en niet artikel 29 DSA. Artikel 38 DSA bepaalt dat zeer grote online platformen ook altijd een optie voor een aanbevelingssysteem moeten aanbieden dat niet gebaseerd is op profilering.
De DSA is pas recent volledig van toepassing geworden. Het is nog te vroeg om te concluderen dat de verplichtingen die daarmee zijn geïntroduceerd onvoldoende effectief zijn. Bovendien wil ik erop wijzen dat aanbevelingsalgoritmes niet alleen risico's kennen, maar ook nuttig kunnen zijn. Ze helpen gebruikers bijvoorbeeld om in de enorme hoeveelheid informatie op het internet de voor hen meest interessante informatie te vinden. Daarom ben ik nog niet bereid om te stellen dat de norm van artikel 38 DSA bredere toepassing moet krijgen. Hierbij speelt ook mee dat de invloed van aanbevelingsalgoritmes ook betrokken moet worden in de systeemrisicoanalyses waar grote platforms toe verplicht zijn (zie antwoord 12).
Ten slotte is het van belang op te merken dat de DSA een rechtstreeks werkende verordening is die voorziet in maximumharmonisatie.

Vraag 12
Deelt u de mening van de Nederlandse Vereniging van Journalisten (NVJ) dat er nieuwe Europese wetgeving moet komen die bij grote techbedrijven afdwingt dat dit soort desinformatie-websites geen aandacht krijgen via social media-algoritmes?[4]

Antwoord 12
De DSA voorziet in een verplichting voor zeer grote online platforms, waaronder een aantal grote sociale netwerken als Facebook, TikTok en Instagram, om systeemrisico's te analyseren en beperken (artikel 34 en 25). Ook de verspreiding van sommige vormen van desinformatie kan een systeemrisico vormen. Te denken valt aan desinformatie die verkiezingen kan beïnvloeden, of negatieve effecten heeft voor de volksgezondheid of op minderjarigen. Als dergelijke risico's bestaan dan kunnen er diverse maatregelen worden genomen, waaronder aanpassingen aan aanbevelingssystemen (artikel 35).
Identificatie en bestrijding van desinformatie is echter niet eenvoudig. Naarmate de methodes daarvoor beter worden kunnen zeer grote platformen die overwegen wanneer zij ter uitvoering van de DSA maatregelen moeten nemen ter bestrijding van systeemrisico's. Of zeer grote online platforms met hun maatregelen voldoen aan hun verplichtingen onder artikel 35, wordt gecontroleerd en gehandhaafd door de Europese Commissie. De komende jaren moet blijken in hoeverre dit systeem voldoende is. Tot die tijd acht ik verdere wetgeving niet nodig.

Vraag 13
Deelt u de mening dat het zorgelijk is dat niet alleen Rusland[5], maar ook China actief inzet op desinformatiecampagnes om de publieke opinie te beïnvloeden?

Antwoord 13
Ja. Desinformatiecampagnes zijn een onderdeel van de bredere, ambitieuzere Chinese inspanningen op het gebied van FIMI. Chinese FIMI-activiteiten richten zich op het manipuleren van het media- en informatiesysteem binnen en buiten Europa, o.a. om een positief beeld te creëren van het eigen autoritaire bestuursmodel.[6]

Vraag 14
Heeft u informatie dat China en Rusland hierin gezamenlijk optrekken? Zo ja, op welke manier? Op welke manier trekt u samen met de EU, Verenigde Staten (VS) en andere bondgenoten op om deze ondermijning te bestrijden?

---

[4] Villamedia, 7 februari 2024, «NVJ: netwerk pro-Chinese nieuwssites leidt tot desinformatie» (https://www.villamedia.nl/artikel/nvj-netwerk-pro-chinese-nieuwssites-leidt-tot-desinformatie)
[5] Aanhangsel Handelingen II, vergaderjaar 2023–2024, Zaaknummer 2024Z01501
[6] Zie o.a. Daniel Mattingly, Trevor Incerti, Changwook Ju, Colin Moreshead, Seiki Tanaka en Hikaru Yamagishi: «Chinese State Media Persuades a Global Audience that the «China Model» is Superior: Evidence from a 19-Country Experiment», *American Journal of Political Science*

Antwoord 14
Er zijn voorbeelden beschikbaar waarbij Chinese mediabedrijven Russische desinformatie actief verspreiden.[7] Ook na de inval in Oekraïne deelden Chinese staatsmedia op grote schaal Russische narratieven en desinformatie.[8] dat China in het recente verleden heeft geleerd van Russische tactieken en technieken voor de verspreiding van desinformatie.[9] Zoals genoemd onder vraag 4, werkt Nederland in meerdere kaders samen met gelijkgezinde landen om ervaring en geleerde lessen te delen en onze aanpak af te stemmen. Dat is echter een zaak van lange adem en meerdere sporen, zoals in deze beantwoording geschetst.

[7] Elian Peltier, Adam Satarino, Lynsey Chutnel, «How Putin became a hero on African TV,» The New York Times, April 2023, https://www.nytimes.com/2023/04/13/world/africa/russia-africa-disinformation.html
[8] Allen-Ebrahimian, Bethany (2023). «How China Trolls Flooded Twitter.» Foreign Policy. July 30. https:// foreignpolicy.com/2023/07/30/china-propaganda-twitter-russia/
[9] Emulating Russia, China Is Improving Its Ability to Operate in the Gray Zone, The Diplomat, 1 juni 2023