Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2024–2025

Aanhangsel van de Handelingen

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

150

Vragen van de leden **Piri** en **Kathmann** (beiden GroenLinks-PvdA) aan de Minister van Buitenlandse Zaken, de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (Koninkrijksrelaties en Digitalisering) en de Minister van Binnenlandse Zaken en Koninkrijksrelaties over *het onderzoek van Trollrensics over desinformatienetwerken tijdens de EU verkiezingen* (ingezonden 12 juli 2024).

Antwoord van Minister **Uitermark** (Binnenlandse Zaken en Koninkrijksrelaties), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en de Ministers van Defensie en van Justitie en Veiligheid (ontvangen 2 oktober 2024).

Vraag 1
Bent u bekend met het onderzoek van Trollrensics over desinformatienetwerken op sociale media met als doel de Europese verkiezingen van 2024 te beïnvloeden?[1]

Antwoord 1
Ja, hiermee zijn we bekend.

Vraag 2
Deelt u de mening dat dergelijke activiteiten een rechtstreekse bedreiging zijn voor de democratische rechtsstaat en daarmee voor de staatsveiligheid? Zo nee, waarom niet?

Antwoord 2
Ja. Heimelijke beïnvloeding ondermijnt onze democratische rechtsstaat en het vertrouwen in onze democratische instituties. Daarmee vormt het een bedreiging voor onze nationale veiligheid. Het is voor het kabinet van groot belang om dreigingen tegen onze samenleving tegen te gaan.

[1] Russisch netwerk op X poogde radicaal-rechts in Europa te versterken | de Volkskrant, 12 juli 2024

ah-tk-20242025-150
ISSN 0921 - 7398
's-Gravenhage 2024

Vraag 3
Beamen de AIVD, MIVD en NCTV de resultaten van het onderzoek volledig? Met hoeveel zekerheid is te zeggen dat in Nederland niet op dezelfde schaal campagnes zijn gevoerd door buitenlandse mogendheden tijdens de verkiezingen van 2024?

Antwoord 3
Onze inlichtingen- en veiligheidsdiensten waarschuwen al langere tijd dat inmengingsactiviteiten van andere landen in toenemende mate een bedreiging vormen.[2] Het netwerk ontdekt door Trollrensics was actief in Frankrijk, Duitsland en Italië. In Nederland werd het niet waargenomen. Dit netwerk past in het normbeeld waarbij Rusland voortdurend probeert westerse beelden besluitvorming te beïnvloeden ten gunste van Rusland, maatschappelijke tegenstellingen probeert aan te wakkeren en te versterken en onderlinge eenheid te ondermijnen. In de openbare jaarverslagen van de AIVD en MIVD is te lezen dat Rusland zijn heimelijke beïnvloedingsactiviteiten vooral op grote Europese landen richt. Dat betekent niet dat er geen risico is voor Nederland op heimelijke beïnvloeding vanuit Rusland. Rusland stelt zich in deze opportunistisch op en is in staat om in te spelen op zich voordoende kansen in kleinere landen. Bovendien kunnen beïnvloedingscampagnes tegen bondgenoten ook indirect gevolgen hebben voor Nederland.

Vraag 4
Hebben de AIVD en MIVD signalen opgevangen dat soortgelijke desinformatiecampagnes in Nederland zijn gevoerd tijdens de verkiezingen van 2024? Zo ja, zijn deze effectief bestreden? Wat was de schaal van deze campagne(s)?

Antwoord 4
De diensten hebben een divers instrumentarium om heimelijke beïnvloeding te onderzoeken en waar nodig de samenleving, instanties en/of personen te alerteren. Het kabinet kan in het openbaar geen mededelingen doen naar waar de inlichtingen- en veiligheidsdiensten al dan niet onderzoek naar doen. Het is voor het werk van de inlichtingen- en veiligheidsdiensten immers van doorslaggevend belang dat zij in het belang van onze nationale veiligheid, geheimhouding en bronbescherming waarborgen. U kunt ervan uitgaan dat de diensten hun wettelijke bevoegdheden kunnen en zullen inzetten om heimelijke beïnvloeding te onderkennen en waar mogelijk, tegen te gaan.

Vraag 5
Draagt Nederland als wereldwijde *host* van online diensten, waaronder servers die gebruikt worden in Russische desinformatiecampagnes zoals recent bevestigd door de AIVD[3], een bijzondere verantwoordelijkheid in het bestrijden van desinformatie? Zo ja, hoe kan hier effectief tegen worden opgetreden met respect voor de privacy van onschuldige internetgebruikers?

Antwoord 5
Aanbieders van hostingdiensten (inclusief online platformen) hebben bepaalde verantwoordelijkheden voor de informatie die zij hosten, die nader beschreven staan in de Digitaledienstenverordening (DSA). Dit betekent onder andere dat wanneer desinformatie de vorm heeft van illegale inhoud de DSA diverse bepalingen bevat die aanbieders van hostingdiensten een verantwoordelijkheid geven in de bestrijding daarvan. Artikel 6 DSA bepaalt dat aanbieders van hostingdiensten in beginsel niet aansprakelijk zijn voor informatie die gebruikers op hun servers plaatsen en opslaan. Zodra zij er echter kennis van krijgen dat ze illegale inhoud hosten, dan zijn ze verplicht om prompt te handelen en die inhoud te verwijderen of de toegang ertoe te blokkeren. Doen ze dat niet, dan kan de Europese Commissie, als toezichthouder van de DSA, ze wél aansprakelijk stellen voor die illegale inhoud. De DSA verplicht hen ook om meldingen van illegale inhoud mogelijk te maken en verduidelijkt dat dergelijke meldingen leiden tot kennis in de zin van artikel 6

[2] AIVD, MIVD en NCTV – Dreigingsbeeld Statelijke Actoren 2 (2022)
[3] Nederland en VS verstoren Russische digitale beïnvloedingsoperatie | Nieuwsbericht | AIVD, 9 juli 2024

(artikel 16, derde lid). Daarmee is er niet alleen een verplichting maar ook een prikkel om dat soort meldingen op te volgen.
Een puur hostingsbedrijf kan veelal niet ingrijpen op het niveau van specifieke inhoud van internetgebruikers, maar wel op het niveau van een hele server of website. Bijvoorbeeld door die ontoegankelijk te maken. Ingrepen door hostingbedrijven zijn daardoor over het algemeen minder proportioneel dan ingrepen door de website-eigenaar of de dienst die op de servers van het hostingbedrijf draait.
Niet alle desinformatie is illegaal. Niettemin kan het schadelijk zijn. Voor die gevallen bevat de DSA verplichtingen voor zeer grote online platformen. Zeer grote online platformen zoals X moeten daardoor in aanvulling op de verplichtingen waar alle aanbieders van hostingdiensten aan dienen te voldoen, verantwoordelijkheid nemen tegen desinformatiecampagnes, bijvoorbeeld in de vorm van niet-authentieke manipulatie van die diensten, op hun platformen. Dit probleem moet Europa-breed en bij de bron worden aangepakt. Artikel 34 en 35 van de DSA, die betrekking hebben op risicobeoordeling en risicobeperking, verplichten sociale media platforms als X of Facebook om maatregelen te nemen tegen gecoördineerd niet-authentiek gedrag en desinformatiecampagnes. Het is de Europese Commissie die hierop toezicht houdt vanuit de Digital Services Act (DSA). Meer informatie over de wijze waarop de Europese Commissie dit heeft ingevuld rondom de Europese Parlementsverkiezing is te vinden in het recentelijk gepubliceerde rapport hierover.[4]

Vraag 6
Zijn er nog andere voorbeelden bekend waar Nederland een faciliterende rol speelde in beïnvloedingscampagnes gericht op andere landen? Hoe wordt dit ondervangen?

Antwoord 6
Nederland is een belangrijk knooppunt in mondiale digitale netwerken en infrastructuur. Het is voor veel statelijke actoren aantrekkelijk om misbruik te maken van Nederlandse ICT-infrastructuur, omdat deze van hoge kwaliteit is en eenvoudig is in te zetten. De AIVD, MIVD en NCTV waarschuwen daarom al langer voor het risico van misbruik van Nederlandse infrastructuur door statelijke actoren.[5] Het is een belangrijke bevoegdheid en tegelijkertijd een taak van de AIVD en de MIVD om heimelijke beïnvloeding te onderkennen en tegen te gaan. Ook als de beïnvloeding in een ander land plaatsvindt en gebruik maakt van Nederlandse infrastructuur. Op 9 juli jl. is uw Kamer geïnformeerd over de verstoring van een Russische digitale beïnvloedingsoperatie, gericht op de beïnvloeding van het publieke debat in de Verenigde Staten van Amerika. Bij deze beïnvloedingsoperatie werd gebruik gemaakt van een server in Nederland. De MIVD rapporteerde in 2022 over routers die door de Russische militaire inlichtingendienst (*Glavnoje Razvedyvatelnoje Oepravlenije*, GROe) gebruikt worden als aanvalsinfrastructuur en de verstoring van dat netwerk.[6] In 2023 zag de MIVD dat Russische actoren gebruik blijven maken van gehackte infrastructuur van onschuldige gebruikers ten behoeve van digitale spionage-, sabotage- en beïnvloedingsactiviteiten.[7]
Het is van belang om de Nederlandse ICT-infrastructuur in generieke zin weerbaarder te maken tegen misbruik, daarom zet het kabinet in op de uitvoering van de Nederlandse Cybersecurity Strategie.[8]

Vraag 7
Doet de regering uws inziens voldoende om desinformatiecampagnes in Nederland als ook beïnvloedingscampagnes die gehost worden vanuit Nederland tegen te gaan?

---

[4] European Board for Digital Services publishes post-election report on the EU elections | Shaping Europe's digital future (europa.eu)
[5] AIVD, MIVD en NCTV – Dreigingsbeeld Statelijke Actoren 2 (2022)
[6] MIVD jaarverslag 2022, p.13.
[7] MIVD jaarverslag 2023, p. 12.
[8] Https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028

Antwoord 7
Het kabinet heeft in de Voortgangsbrief Rijksbrede strategie desinformatie, die in juni aan de Tweede Kamer is verzonden, beschreven wat zij deed en welke nieuwe acties zij voornemens zijn te ondernemen. Deze acties zijn onder andere gericht op het versterken van de weerbaarheid van burgers tegen desinformatie.[9]
Zie verder het antwoord op vraag 5.

Vraag 8
Zijn er tijdens de Europese verkiezingen in 2024 aanvullende maatregelen genomen om desinformatienetwerken tegen te gaan? Zo ja, welke en bleken deze effectief? Zo nee, waarom niet?

Antwoord 8
Ja, er zijn maatregelen genomen in aanvulling op reeds bestaande maatregelen, zowel in samenwerking op Europees niveau, als aanvullende maatregelen op nationaal niveau.
De Europese Dienst voor extern optreden (EDEO) heeft netwerken van statelijke actoren tijdens de Europese verkiezingen beter in beeld gebracht door deze te identificeren en hierover artikelen te publiceren op de website EUvsDisinfo.[10]
De Europese Commissie heeft met enkele van de sociale media platformen, NGO's en nationale toezichthouders, waaronder de ACM, een zogenoemde «stresstest» gevoerd. Hierbij testte de Commissie samen met de platformen of zij klaar waren voor heimelijke verkiezingsbeïnvloeding, zoals desinformatienetwerken, op hun platform en hoe daarmee om te gaan.[11] Verder heeft de Commissie richtsnoeren gepubliceerd voor aanbieders van zeer grote onlineplatforms en zeer grote onlinezoekmachines (VLOPS en VLOSE) inzake de beperking van systeemrisico's voor verkiezingsprocessen.[12] Sinds de inwerkingtreding van de DSA is de ACM in Nederland aangewezen als digitaledienstencoördinator. Bij de afgelopen EP-verkiezing was de ACM betrokken bij onder andere de verkiezingstafel.
Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) werkt samen met andere EU-lidstaten via mechanismen zoals het Rapid Alert System (RAS), de voor de verkiezingen ingestelde geïntegreerde regeling politieke crisisrespons (IPCR) en het European Cooperation Network on Elections (ECNE) om informatie en acties te coördineren en de weerbaarheid te vergroten.
Op nationaal niveau neemt het Ministerie van BZK tijdens de verkiezingen standaard extra maatregelen om de effecten van desinformatienetwerken te verminderen.[13] Dit gaat op de eerste plaats om begrijpelijke en transparante communicatie over het verkiezingsproces en de stemprocedure. Als burgers weten hoe het verkiezingsproces werkt, zijn ze minder vatbaar voor desinformatie over dit onderwerp. Daarnaast organiseerde het Ministerie BZK wederom een verkiezingstafels voor vertegenwoordigers van de gemeenten, de Kiesraad en alle veiligheidspartners (Politie, OM, ACM en betrokken ministeries), waar mogelijke risico's worden besproken die ondermijnend zijn voor het verkiezingsproces. Verder organiseerde het ministerie een webinar voor gemeenteambtenaren waar specifiek is ingegaan op het tegengaan van desinformatie.
Tot slot kan het Ministerie van BZK in bijzondere gevallen haar trusted flagger status inzetten, waardoor meldingen door sociale media platformen met prioriteit worden behandeld. De sociale mediabedrijven maken hierbij altijd hun eigen onafhankelijke afweging of er sprake is van een overtreding van de gebruikersvoorwaarden en dus of actie gerechtvaardigd is. Het ministerie heeft geen bevoegdheid bepaalde content te laten verwijderen. Deze status is voor de EP-verkiezing eenmalig ingezet bij het platform X om een algemene waarschuwing te geven dat er wellicht valse berichten worden verspreid over het verkiezingsproces. Uw Kamer wordt hierover nader geïnformeerd in de

[9] Kamerstukken II 2023–2024, 30 821, nr. 230
[10] European elections Archives - EUvsDisinfo
[11] Commission stress tests platforms' election readiness under the Digital Services Act | Shaping Europe's digital future (europa.eu)
[12] EUR-Lex - 52024XC03014 - EN - EUR-Lex (europa.eu)
[13] Kamerstukken II 2023–2024, 35 165, nr. 64

evaluatie van de EP-verkiezingen. De Minister van BZK streeft ernaar deze evaluatie begin november aan uw Kamer toe te sturen.
Uit rapporten van de onder de DSA opgerichte Europese digitaledienstenraad en de EDMO (het factcheckers consortium) Task Force blijkt dat er, ondanks pogingen van desinformatienetwerken, geen grote of structurele problemen zijn geweest bij de Europese verkiezingen.[14] Ook de nieuwe, onder de DSA opgerichte, Europese digitaledienstenraad concludeert op dit moment dat er geen grootschalige of systemische incidenten hebben plaatsgevonden waardoor het verloop van de Europese verkiezingen is verstoord.[15]

Vraag 9
Biedt de bestaande Europese wet- en regelgeving, met name via de Digital Services Act, voldoende mogelijkheden om op te treden tegen desinformatiecampagnes? Welke nationale en Europese maatregelen zijn er verder nog nodig om desinformatie effectief te bestrijden?

Antwoord 9
Ja, de desinformatiecampagnes zoals omschreven in het onderzoek van Trollrensics, vonden plaats op X. Dit platform geldt als een zeer grote online platform en valt sinds augustus 2023 onder de DSA. De DSA bevat verschillende bepalingen over inhoudsmoderatie door aanbieders van online tussenhandeldiensten. Volgens de definitie van het begrip «inhoudsmoderatie» (artikel 3, onderdeel t, van de DSA) gaat het dan om zowel illegale inhoud als om informatie die in strijd is met de algemene voorwaarden die de aanbieder toepast, bijvoorbeeld omdat hij deze onwenselijk of schadelijk acht. Desinformatie kan zowel de vorm aannemen van illegale inhoud als schadelijke inhoud. In het geval van het laatste, kan desinformatie en andere schadelijke inhoud vallen onder contractuele beperkingen die in de algemene voorwaarden opgenomen zijn. Daarnaast kan desinformatie ook vallen onder zogenaamde «systeemrisico» zoals beschreven in artikel 34 van de verordening. Tegen dergelijke schadelijke inhoud moeten aanbieders van zeer grote online platforms en zeer grote onlinezoekmachines maatregelen treffen om deze te beperken.
Aanbieders van zeer grote online platforms en zeer grote onlinezoekmachines moeten daarom, bij de beoordeling van systeemrisico's, bijzondere aandacht besteden aan de manier waarop hun diensten (kunnen) worden gebruikt om misleidende of bedrieglijke inhoud, met inbegrip van desinformatie en gecoördineerde desinformatiecampagnes, te verspreiden of versterken. Het is vervolgens aan de Europese Commissie als bevoegde toezichthouder om toezicht te houden op zeer grote online platformen en onlinezoekmachines. Bij het treffen van maatregelen moeten platformen de rechten van burgers beschermen, zoals het recht op privacy en de vrijheid van meningsuiting. Daarnaast is uw Kamer recentelijk geïnformeerd over de nieuwe maatregelen die wij nemen in de Rijksbrede strategie voor de effectieve aanpak van desinformatie.[16] Het Ministerie van BZK heeft opdracht gegeven tot een brede verkenning waarin wordt onderzocht hoe de kwaliteit van het open publieke debat beter kan worden gewaarborgd. Daarbij wordt onderzocht welke kwetsbaarheden het open publieke debat kent, waaronder de wijze waarop desinformatie de Nederlandse democratische rechtsstaat kan ondermijnen en welke interventies het open publieke debat beter kunnen beschermen. Over dit onderzoek en de eerste resultaten wordt uw Kamer eind 2024 geïnformeerd.

Vraag 10
Doen grote online platforms volgens u voldoende om desinformatiecampagnes op hun kanalen te bestrijden? Zo ja, waaruit blijkt dat? Zo niet, van welke online platforms verwacht u meer actie en is de Digital Services Act, onder andere, voldoende uitgerust om hen hiertoe te dwingen?

---

[14] European Board for Digital Services publishes post-election report on the EU elections | Shaping Europe's digital future (europa.eu) en FINAL REPORT – Results and outcomes of a community-wide effort – EDMO
[15] European Board for Digital Services publishes post-election report on the EU elections | Shaping Europe's digital future (europa.eu)
[16] Kamerstukken II 2023–2024, 30 821, nr. 230

Antwoord 10
De DSA verplicht zeer grote online platforms en zoekmachines om tenminste jaarlijks een risicobeoordeling te verrichten om te onderzoeken of hun diensten vatbaar zijn voor systeemrisico's. De verspreiding van desinformatie kan zo'n systeemrisico vormen. Indien dergelijke systeemrisico's aanwezig zijn, moeten aanbieders van zeer grote online platforms en zeer grote onlinezoekmachines maatregelen treffen om deze te beperken. Dergelijke maatregelen kunnen de aanpassing van hun diensten, online-interfaces, algemene voorwaarden inhoudsmoderatieprocedures, algoritmische systemen of aanbevelingssystemen omvatten.
Het is nu nog te vroeg om volledig te kunnen vaststellen of zeer grote online platforms en zoekmachines voldoende maatregelen nemen om systeemrisico's, waaronder de verspreiding van desinformatie, te mitigeren. Dat oordeel is in de eerste plaats aan de Europese Commissie als bevoegde toezichthouder. In het geval van niet-naleving van de bepalingen door zeer grote online platformen en zeer grote onlinezoekmachines kan de Europese Commissie handhavingsmaatregelen. Zo kan de Europese Commissie bijvoorbeeld een maximale boete opleggen tot 6% van de wereldwijde omzet van een zeer groot online platform.
De Europese Commissie is voortvarend gestart met het toezicht, ook op de verplichtingen van artikel 34 en 35 DSA. Op 18 december 2023 is ze een formele procedure gestart tegen X. Onder meer omdat ze twijfelt aan de doeltreffendheid van de maatregelen die X neemt ter bestrijding van desinformatie. Deze procedure loopt nog. Op 12 juli j.l. heeft de Europese Commissie zijn voorlopige bevindingen naar X gestuurd.[17] Daarnaast is ze een formele procedure gestart tegen Meta. De systeemrisico-analyses van Meta, de risico's van desinformatie, en de maatregelen die Meta daartoe heeft genomen zijn onderdeel van die procedure.[18] Wij volgen de voortgang van deze procedures en ondersteunen de Europese Commissie waar nodig in haar rol als toezichthouder op de naleving van de DSA.

Vraag 11
Welke stappen gaat u nemen om samen met uw ambtsgenoten in de EU op te treden tegen deze vorm van buitenlandse verkiezingsbeïnvloeding? Bepleit u samen met hen een gezamenlijke boodschap richting de nieuwe Europese Commissie?

Antwoord 11
Het hoofdlijnenakkoord omschrijft dat de overheid zich inzet om de maatschappij weerbaar te maken tegen desinformatie. Dit belang dragen we ook in de EU uit. Het kabinet staat in EU verband in nauw contact met andere landen waar het buitenlandse beïnvloeding betreft. Concrete voorbeelden hiervan zijn het Europese Rapid Alert System (RAS) en het European cooperation network on elections (ECNE). In deze gremia zijn onder andere signalen over desinformatie, maatregelen om hiermee om te gaan en de laatste wetenschappelijke inzichten uitgewisseld. Leden van de Europese lidstaten doen mee om de negatieve impact van desinformatie zo effectief mogelijk aan te pakken en van elkaar te leren. Via deze wegen worden ook FIMI-campagnes[19] gesignaleerd, vindt uitwisseling plaats over de verschillende verschijningsvormen van FIMI en worden best practices gedeeld over het verhogen van de weerbaarheid en responsmogelijkheden. Waar nodig wordt gekeken naar een gezamenlijke reactie. Nederland participeert actief, o.a. door via het Rapid Alert System vertaalde versies van de Rijksbrede Strategie en de Kamerbrief Weerbaarheid Verkiezingsproces te delen.
De nieuwe Europese Commissie zal op het onderwerp desinformatie nieuwe stappen willen zetten. Dat blijkt uit de politieke richtlijnen van de herkozen Commissievoorzitter.[20] Het is nu aan de Commissie om binnen hun mandaat

[17] https://digital-strategy.ec.europa.eu/en/news/commission-sends-preliminary-findings-x-breach-digital-services-act.
[18] https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2664.
[19] Dit is de term die binnen de EU gebruikt wordt voor ongewenste buitenlandse inmenging in de informatieruimte, een specifiek aandachtsgebied binnen desinformatie. Een FIMI-campagne maakt vaak onderdeel uit van een bredere hybride campagne.
[20] President-elect Ursula von der Leyen - European Commission (europa.eu)

met nieuwe voorstellen te komen. Uw Kamer wordt hier te zijner tijd over geïnformeerd.

Vraag 12
Wat is de stand van zaken van de motie van de leden Piri en Paternotte over het in de Europese Raad pleiten voor onderzoek naar buitenlandse inmenging in de Europese Parlementsverkiezingen?[21]

Antwoord 12
Deze motie is uitgevoerd. De Minister-President heeft tijdens de informele Europese Raad van 17 juni 2024 zijn zorgen overgebracht over mogelijke buitenlandse inmenging in de EP-verkiezingen.[22] De Minister-President gaf daarbij aan dat een onderzoek wenselijk is als er indicaties van inmenging zijn. Een dergelijk onderzoek op Europees niveau zou in de eerste plaats aan het EP zijn, in samenwerking met de Belgische autoriteiten.

Vraag 13
Kunt u de vragen afzonderlijk van elkaar beantwoorden?

Antwoord 13
Ja.

[21] Kamerstuk 21 501-20, nr. 2093
[22] Zie ook het verslag van de informele Europese Raad van 17 juni 2023, file (overheid.nl)