Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

30 821 Nationale Veiligheid

35 165 Verkiezingen

Nr. 118

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 12 oktober 2020

Het beschermen van onze verkiezingen tegen ongewenste (digitale) inmenging is van groot belang voor onze democratie. Uw Kamer heeft daarvoor bij motie van de leden Middendorp (VVD) en Asscher (PvdA) aandacht gevraagd.[1] Hoewel zich bij het stemmen geen digitale dreigingen voordoen, kan de dreiging van digitale inmenging bij verkiezingen in diverse vormen voorkomen. Bijvoorbeeld doordat desinformatie wordt verspreid of doordat partijen of kandidaten gehackt worden. In deze brief ga ik in op de uitdagingen rond digitale inmenging omtrent de verkiezingen, zowel bij het verkiezingsproces zelf als in aanloop naar de verkiezingen. Ook noem ik de maatregelen die de overheid neemt om digitale inmenging bij de Tweede Kamerverkiezing van 2021 te voorkomen. Hiermee ga ik in op de motie van de leden Middendorp (VVD) en Asscher (PvdA) en de toezegging naar aanleiding van een vraag van het Eerste Kamerlid Verkerk (ChristenUnie) om een reactie op bedreigingen rondom ICT[2]. Tevens ga ik in op het verzoek van de leden van de vaste commissie voor Binnenlandse Zaken om een kabinetsreactie op de beoordeling van de Europese Commissie over de naleving van de «code of practice» inzake desinformatie en mogelijk aanvullende maatregelen op korte en lange termijn. Bij deze brief bied ik u ook het rapport *«Digitale dreigingen voor onze democratie»* van het Rathenau Instituut aan[3]. In deze brief ga ik in op de volgende zeven uitdagingen die ik zie als het belangrijkste om digitale inmenging in de verkiezingen te voorkomen.

Uitdagingen digitale inmenging Tweede Kamer verkiezingen 2021

- Blijven beperken van digitale risico's voor het verkiezingsproces.

[1] Kamerstuk 35 300 VII, nr.126
[2] Eerste Kamer, T02840
[3] Raadpleegbaar via www.tweedekamer.nl.

kst-30821-118
ISSN 0921 - 7371
's-Gravenhage 2020

- Kwetsbaarheid politieke partijen voor digitale incidenten verminderen.
- Voorkomen dat mis- en desinformatie het democratisch proces ondermijnt.
- Gebrek aan transparantie omtrent digitale campagnes verminderen.
- Informatiepositie over mis- en desinformatie verder ontwikkelen.
- Rekening houden met nieuwe technieken om mis- en desinformatie te verspreiden.
- Weerbaarheid burgers tegen mis- en desinformatie in stand houden.

Blijven beperken digitale risico's voor het verkiezingsproces

Zoals ik meldde in mijn voorgaande brief over desinformatie en verkiezingen is in Nederland het vertrouwen in de betrouwbaarheid van de verkiezingen hoog[4]. Dat is een groot goed en moet behouden blijven. Tijdens onze verkiezingen vindt zowel de stemming als de telling handmatig plaats. De kiezer maakt in het stemhokje zijn keuze bekend met een rood potlood op een papieren stembiljet. De papieren stembiljetten worden vervolgens door de leden van de stembureaus met de hand geteld. Doordat bij dit deel van de verkiezingen geen digitale middelen worden gebruikt, is het niet vatbaar voor digitale inmenging.

Bij het optellen van de uitslagen gebruiken gemeenten, hoofdstembureaus en het centraal stembureau de nieuwe versie van de programmatuur die de Kiesraad beschikbaar stelt. Voor het gebruik van deze programmatuur krijgen gemeenten instructies over de manier hoe zij deze moeten gebruiken. Onderdelen daarvan zijn het vier-ogen-principe en het online publiceren van de processen-verbaal van alle stembureaus en de berekende totalen op gemeentelijk niveau. Zoals op 12 december 2019 aan uw Kamer is gemeld, worden de instructies voor het gebruik van de ondersteunende programmatuur voor de aankomende verkiezingen opnieuw tegen het licht gehouden.[5]

Gemeenten vervullen een centrale rol in het verkiezingsproces. Zij organiseren de verkiezingen, tellen de stemmen en geven deze door aan het hoofdstembureau. Met de Vereniging Nederlandse Gemeenten (VNG) is afgesproken dat de Informatiebeveiligingsdienst (IBD) van de VNG het centrale meldpunt is voor risico's en kwetsbaarheden rond het verkiezingsproces bij gemeenten. Ook kan de IBD op verzoek van gemeenten een ondersteunende rol vervullen bij het analyseren van processen en procedures en het adviseren over mogelijke aanvullende maatregelen.

Kwetsbaarheid politieke partijen voor digitale incidenten verminderen

Zoals ook de Staatscommissie Parlementair Stelsel beschreef in haar eindrapport (Kamerstuk 34 430, nr. 9), zijn personen en instituties die een rol spelen in het democratisch proces een potentieel doelwit voor kwaadwillenden om bijvoorbeeld informatie te ontvreemden, of desinformatie over te verspreiden. Om de dreiging van cybercrime, cyberspionage en cybersabotage effectief te bestrijden, moeten personen en organisaties, en dus ook politieke partijen, weten en begrijpen wat deze dreigingen inhouden en welke risico's dat oplevert. Het is immers ieders eigen verantwoordelijkheid om zich veilig in het digitale domein te bewegen. Daar waar incidenten zich voordoen rond huidige Kamerleden

[4] Kamerstuk 30 821, nr. 51
[5] Kamerstuk 35 165, nr. 19

kan melding gedaan worden bij de beveiligingsambtenaar (BVA) van de Tweede Kamer.
Waar dat moet en kan, levert de rijksoverheid ondersteuning. Bijvoorbeeld door politieke partijen voorlichting te geven, onder meer op basis van bestaande adviezen en kennisproducten van het Nationaal Cyber Security Centrum (NCSC). Hoewel politieke partijen geen doelgroep van het NCSC zijn, kunnen zij altijd een vrijwillige melding doen bij ernstige incidenten.

Voorkomen dat mis- en desinformatie het democratisch proces ondermijnt

Het is van belang dat burgers zich in aanloop naar de verkiezingen goed kunnen informeren over het verkiezingsproces zelf, politieke partijen en hun standpunten en de kandidaten die deelnemen aan de verkiezingen. Mis- en desinformatie kunnen ervoor zorgen dat burgers de stembusgang wordt belemmerd, omdat ze bijvoorbeeld onjuiste informatie over het verkiezingsproces krijgen of dat hun stemgedrag wordt beïnvloed door misleidende informatie over partijen en kandidaten.

Aard van de dreiging

Zoals eerder gemeld in de kabinetsreactie op de mededeling van de Europese Commissie over desinformatie over COVID-19[6] is het bij het tegengaan van de verspreiding van misleidende informatie belangrijk om onderscheid te maken tussen mis- en desinformatie. Desinformatie is het doelbewust, veelal heimelijk, verspreiden van misleidende informatie, met het doel om schade toe te brengen aan het publieke debat, democratische processen, de open economie of nationale veiligheid. Bij misinformatie ontbreekt een dergelijke kwade intentie en wordt onbedoeld onjuiste of misleidende informatie verspreid. Het inzetten van desinformatie is veelal een middel van statelijke en daaraan gelieerde actoren om het vertrouwen in onze democratie te ondermijnen. Deze informatie kan daarna ook onbewust verder verspreid worden door anderen.

Er zijn geen aanwijzingen dat er bij eerdere verkiezingen in Nederland door statelijk actoren grootschalige desinformatiecampagnes hebben plaatsgevonden. Desalniettemin is blijvende waakzaamheid geboden. Onder andere uit het jaarverslag van de AIVD blijkt dat er sprake is van voortdurende (online) Russische beïnvloedingsactiviteiten op West-Europese sociale media.[7]

Strategie tegen mis- en desinformatie

Om de schadelijke effecten van mis- en desinformatie tegen te gaan, heb ik een strategie opgesteld[8]. Doelstelling van het beleid is de stabiliteit en kwaliteit van onze democratische rechtsorde en onze open samenleving te beschermen, met inbegrip van de vrijheid van meningsuiting en pers. De strategie tegen desinformatie kent drie actielijnen: preventie, informatiepositie verstevigen en (indien nodig) reactie en wordt doorlopend ingezet, dus ook richting de verkiezingen.
Een van de handelingsopties van de overheid in het geval de nationale veiligheid of de politieke, economische of maatschappelijke stabiliteit in het geding is, is het actief tegenspreken van misleidende informatie. Dit is in sommige gevallen dan ook gebeurd tijdens de COVID-19-crisis. Ook in het licht van de verkiezingen zou het kunnen voorkomen dat misleidende informatie over het verkiezingsproces actief wordt tegengesproken.

---

[6] Kamerstuk 22 112, nr. 2896
[7] Kamerstuk 30 977, nr. 156
[8] Kamerstuk 30 821, nr. 91

Bijvoorbeeld waar het gaat om onjuiste informatie over de sluitingstijden van stemlokalen of de wijze van stemmen.
De overheid heeft ook juridische handvatten bij het optreden tegen mis- en desinformatie. Het instituut voor informatierecht (IViR) concludeert dat de wetgeving omtrent het verspreiden van desinformatie verschillende wetgevingsgebieden doorkruist. Rond het verkiezingsproces is volgens de onderzoekers artikel 127 Sr. het meest relevant. Dit artikel gaat over het plegen van een bedrieglijke handeling, waardoor een stem van onwaarde wordt of een stem wordt uitgebracht op een ander dan de bedoelde persoon. Verder kunnen er bij misleidende informatie over campagnes, partijen of kandidaten juridische aangrijpingspunten zijn in het civielrecht, of als er sprake is van een strafbaar feit als smaad of laster.
De betrokken departementen, diensten en lokale overheden gebruiken bij (dreigende) incidenten rond beïnvloeding door statelijke actoren een divers instrumentarium. Dit instrumentarium loopt uiteen van monitoren en informeren tot maatregelen in het kader van de openbare orde en veiligheid en inzet van diplomatieke middelen (waaronder aanspreken, toegang tot Nederland weigeren, reizen naar Nederland ontmoedigen, en – in ultimo – persona non grata verklaren van diplomaten). Deze instrumenten worden ingezet wanneer dat nodig, gewenst, haalbaar en effectief wordt geacht.

Gebrek aan transparantie omtrent digitale campagnes verminderen

In aanloop naar de verkiezingen moet het voor burgers duidelijk zijn wie de afzender is van een politieke advertentie en waarom zij deze te zien krijgen. Met deze informatie kunnen burgers zelf deze beter advertenties op waarde schatten. Politieke advertenties kunnen een middel zijn om desinformatie te verspreiden. Meer transparantie maakt het voor kwaadwillenden lastiger hun identiteit te verhullen. Daarnaast moeten politieke advertenties ook voor iedereen openbaar zijn zodat ze onderdeel kunnen worden van het publieke debat. Zo kan het ook duidelijk worden welke boodschappen aan verschillende groepen burgers zijn gericht.

Europese gedragscode tegen desinformatie

Via de Europese gedragscode tegen desinformatie hebben verschillende internetdiensten zich gecommitteerd de verspreiding van desinformatie te adresseren, onder andere door transparantie van politieke advertenties te vergroten. Een aantal internetdiensten staat inmiddels echter geen politieke advertenties meer toe op hun platforms. De belangrijkste internetdiensten die nog wel politieke advertenties aanbieden hebben maatregelen genomen om de transparantie van politieke advertenties te vergroten. Bijgevoegd is een overzicht van de maatregelen van internetdiensten op dit gebied[9].
Op 10 september publiceerde de Europese Commissie haar evaluatie van de gedragscode[10]. Ik ben het met de Europese Commissie eens dat deze gedragscode een goede eerste stap van de bedrijven is om hun verantwoordelijkheid te nemen. Maar dit is nog niet genoeg. De evaluaties van de gedragscode wijzen op een grote informatie asymmetrie: de informatie die momenteel door internetdiensten wordt verstrekt als gevolg van de gedragscode is onvoldoende voor overheden, academici, burgers en andere belanghebbenden om de inspanningen van de platforms goed en

[9] Raadpleegbaar via www.tweedekamer.nl.
[10] SWD(2020) 180. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement, zie: https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

publiekelijk te onderzoeken of om verdere kennis en inzichten te krijgen die nodig is om het beleid tegen mis- en desinformatie effectiever te maken.
Ik ben van mening dat de Europese gedragscode tegen desinformatie moet worden verbeterd. In de gedragscode moeten minimale transparantie- en rapportagestandaarden en gemeenschappelijke definities van sleutelconcepten (zoals politieke advertenties) worden vastgelegd, en gebruikers moeten toegang hebben tot een objectieve beroepsprocedure tegen beslissingen over de moderatie van hun berichten. De naleving van een dergelijke nieuwe gedragscode moet worden gecontroleerd, bijvoorbeeld via onafhankelijke audits. Momenteel zijn er geen gevolgen voor de ondertekenaars voor het niet naleven van hun toezeggingen. Ik ben daarom van mening dat de Europese Commissie moet zorgen voor een rechtsgrond om ondertekenaars aansprakelijk te stellen voor niet-naleving van hun toezeggingen, en deelname aan de nieuwe gedragscode verplicht te stellen voor bepaalde platformen, zonder daarbij een barrière te creëren voor innovatie en het MKB. De nieuwe gedragscode moet daarom een vorm van co-regulering worden, waarbij internetdiensten, het maatschappelijk middenveld en deskundigen met de juiste technische expertise betrokken moeten zijn bij de formulering.
Deze positie breng ik ook over aan de Europese Commissie en andere lidstaten ter overweging voor het komende Europese Democratie Actieplan en het Digital Service Act Package welke naar verwachting eind 2020 zullen verschijnen. Zo heb ik bovenstaande positie ook overgebracht tijdens mijn recente gesprek met Eurocommissaris Jourová.

Andere ontwikkelingen transparantie politieke advertenties

Op nationaal niveau werk ik aan een Wet op de politieke partijen (Wpp). Daarin krijgen transparantieregels een plek, die de controleerbaarheid voor de kiezer van verkiezingscampagnes moeten waarborgen en vergroten, misleiding voorkomen en duidelijkheid geven over wie een advertentie heeft betaald.[11] Regulering hiervan heeft tot doel de campagnes voor kiezers inzichtelijk te maken. Het is van belang dat hier een balans komt tussen transparantie en het beperken van de administratieve lasten.
Zowel Europese als nationale wetgeving zijn nog niet gereed voor de Tweede Kamerverkiezingen van 2021. Daarom blijf ik in de tussentijd de internetdiensten aanspreken op hun verantwoordelijkheid en hen verzoeken meer transparantie te bieden zoals ik ook in een gesprek op 25 juni jl. heb gedaan. Meer structurele monitoring zoals de Europese Commissie in haar evaluatie[12] voorstelt kan daarbij helpen. De maandelijkse monitoring[13] van de maatregelen van de internetdiensten m.b.t. COVID-19 desinformatie die is opgestart n.a.v. de recente mededeling van de Europese Commissie[14] kan daarvoor een voorbeeld zijn.

Informatiepositie over mis- en desinformatie verder ontwikkelen

Overheden dienen een goede informatiepositie te hebben over de aanwezigheid van mis- en desinformatie zodat zij weten of er sprake is van een dreiging die een reactie van de overheid vereist. Hiervoor is het

[11] Kamerstuk 35 300 VII, nr. 123
[12] SWD(2020) 180. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement, zie: https://ec.europa.eu/digital-single-market/en/news/assessment-code-practice-disinformation-achievements-and-areas-further-improvement
[13] https://ec.europa.eu/digital-single-market/en/news/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme
[14] Kamerstuk 22 112, nr. 2896

belangrijk informatie te delen binnen de overheid maar ook binnen internationale verbanden waardoor een gedeeld normbeeld kan ontstaan. In Nederland staan de betrokken ministeries en diensten doorlopend in nauw contact om informatie over en signalen van mogelijke desinformatieactiviteiten te delen, te duiden en daarop zo nodig te acteren. Ook in aanloop naar de verkiezingen zullen informatie en signalen bij elkaar gebracht worden. Op internationaal vlak versterken we onze informatiepositie door deel te nemen aan internationale samenwerkingsverbanden om kennis en *best practices* uit te wisselen en eventuele signalen rondom mis- en desinformatie te delen. In de bijlage is een overzicht toegevoegd van internationale samenwerkingsverbanden waar we als Nederland aan deelnemen[15].
Ook academici, media en fact-checkers spelen een belangrijke rol in het signaleren en duiden van mis- en desinformatie. Recent heeft de Europese Commissie het European Digital Media Observatory (EDMO) gelanceerd, waarin samenwerking tussen een onafhankelijke gemeenschap van fact-checkers, wetenschappers en andere stakeholders wordt gefaciliteerd. Een ontwikkeling die ik van harte aanmoedig, zeker omdat desinformatie niet aan grenzen gebonden is. Onderdeel van het EDMO worden ook nationale of multinationale *hubs* voor onderzoek naar digitale media, waarin academici, onafhankelijke fact-checkers, mediaorganisaties en andere relevante organisaties deelnemen. De aanbesteding van de Europese Commissie voor de eerste nationale of multinationale hubs staat tot november 2020 open. Naar verwachting zijn vanwege de aanbestedingstermijnen de *hubs* nog niet operationeel voor de Tweede Kamerverkiezingen in 2021.

Rekening houden met nieuwe technieken om mis- en desinformatie te verspreiden

Technologische ontwikkeling staat niet stil, ook niet voor de technieken waarmee mis- en desinformatie verspreid kan worden. Zoals eerder aangekondigd heb ik een verkenning laten uitvoeren naar de impact van verschillende technieken en de betekenis daarvan voor de aanpak van desinformatie. Bijgevoegd bij deze brief is het eindrapport van het Rathenau Instituut «*Digitale dreigingen voor de democratie*». Het onderzoek geeft een overzicht van de technologische ontwikkelingen die de komende jaren een rol kunnen gaan spelen bij de productie en verspreiding van desinformatie. Tot de mogelijkheden behoren onder andere technologieën als tekstsynthese, *voice cloning*, *deepfakes*, micro-targeting en chatbots. De onderzoekers concluderen dat met name *deepfake* technologie en *psychographing*, een geavanceerde vorm van microtargeting, in de toekomst ingezet kunnen worden ingezet door kwaadwillende actoren om het publieke debat en het democratische proces heimelijk te beïnvloeden. Ik verwacht niet dat deze technologieën bij de komende Tweede Kamerverkiezingen al een grote rol zullen spelen. Het onderzoek van het Rathenau Instituut laat echter het aanhoudende belang van het adresseren van mis- en desinformatie zien. Het zal naar verwachting in de toekomst alleen maar lastiger worden om echt van nep te onderscheiden.

Aanbevelingen Rathenau Instituut

Ik deel de conclusie van de onderzoekers dat met name de internetdiensten een verantwoordelijkheid hebben om te voorkomen dat deze technologieën ingezet worden om desinformatie te verspreiden. De overheid kan daarbij de bedrijven wel aansporen om maatregelen te nemen zoals het investeren in detectie van *deepfakes*. Ik neem deze en de

[15] Raadpleegbaar via www.tweedekamer.nl.

andere aanbevelingen van het Rathenau instituut gericht op de internetdiensten mee bij bovenstaande inbreng voor het Europese Democratie Actieplan en de Digitale Service Act Package. De beschreven nieuwe technologieën zouden een plek kunnen krijgen in een verbeterde gedragscode waarbij de ondertekenaars zich committeren te investeren in bijvoorbeeld *deepfake* detectie middelen. Ik zal de onderzoekers vragen hun bevindingen te presenteren aan de internetdiensten en andere relevante partijen om ook bij hen meer bewustwording te creëren. Tevens wordt in het rapport benadrukt dat investeren in fact-checkers en mediawijsheid van belang is. Op dit gebied ondersteunen zowel het kabinet als de EU al verschillende initiatieven en dat zullen we voortzetten.

Weerbaarheid burgers tegen mis- en desinformatie in stand houden

Voor een gezond publiek debat is het belangrijk dat burgers weerbaar zijn tegen de invloed van mis- en desinformatie. Burgers nemen dan zelf verantwoordelijkheid voor het op waarde schatten van berichten. Zoals aangegeven door het Rathenau Instituut zal het naar verwachting alleen maar lastiger worden voor burgers om onderscheid te maken tussen echt en nep. De overheid reikt burgers daarom middelen aan waarmee zij dit kunnen (blijven) doen, bijvoorbeeld door het stimuleren van mediawijsheid. Het creëren van bewustwording en meer mediawijsheid is een uitdaging die niet alleen bij verkiezingen speelt.

Eerder heb ik uw Kamer geschreven geen aanleiding te zien om de campagne die ik op verzoek van uw Kamer in 2019 rond de verkiezingen heb uitgevoerd, voort te zetten.[16] Om mediawijsheid te onderhouden en bevorderen zet het kabinet in op andere middelen, zoals de meerjarige subsidie die ik in samenwerking met mijn collega voor Basis-, Voortgezet Onderwijs en Media, heb verleend aan Netwerk Mediawijsheid om beroepsopleidingen te ondersteunen in vakgebieden die een bijdrage kunnen leveren aan het adresseren en bespreekbaar maken van desinformatie, zoals zorg, onderwijs en media.[17]

Daarnaast heeft ook het maatschappelijk middenveld een belangrijke rol om burgers te helpen om informatie op waarde te schatten. Zo heb ik onlangs via het Startup in Residence InterGov programma bijgedragen aan de ontwikkeling van een digitale tool waarmee gebruikers de betrouwbaarheid van online nieuwsartikelen kunnen beoordelen en inzien. Daarnaast zijn er ook andere technologische oplossingen beschikbaar voor burgers, bijvoorbeeld browser *plugins*, waarmee inzichtelijk wordt voor burgers welke politieke campagnes advertenties op hen gericht worden of websites waar je kunt controleren of een sociale media account een bot is.[18]

Digitale inmenging tegengaan met alle betrokkenen

Uit bovenstaande uitdagingen en maatregelen kan geconcludeerd worden dat gezien de veelzijdigheid van digitale inmenging er verschillende expertises nodig zijn om onze verkiezingen hiertegen te kunnen beschermen. Daarom zal ik over bovenstaande uitdagingen besloten thematafels organiseren, waarbij ik naast relevante ministeries ook toezichthouders, het maatschappelijk middenveld, politieke partijen en internetdiensten uitnodig. Het doel van deze tafels is het creëren van

---

[16] Kamerstuk 30 821, nr. 91.
[17] Kamerstuk 30 821, nr. 91
[18] Zie bijvoorbeeld het overzicht van de Rand Corporation via https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html

bewustzijn over digitale inmenging en het uitwisselen van informatie tussen de betrokken organisaties. Door de capaciteiten en expertise van deze organisaties te betrekken bij de voorbereiding op de verkiezingen en deze organisaties op hun respectievelijke verantwoordelijkheden te wijzen kunnen we het goede functioneren van onze democratie blijven waarborgen.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
K.H. Ollongren