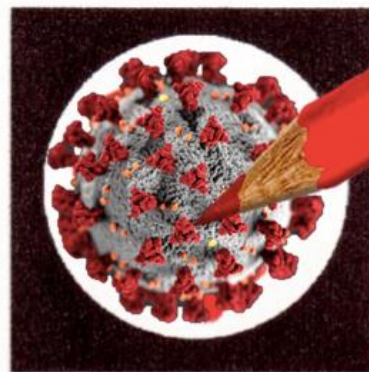




TECH TEGEN CORONA

Verkiezingen maart 2021, desinformatie & COVID-19

Oktober 2020



Met dank aan:

Dr. Majoor. Jaap Hoogenboezem, Bestuurskunde, Universiteit Maastricht
Em. prof. dr. Roel Wieringa, Informatie Systemen, Universiteit Twente

INHOUDSOPGAVE

1	<i>Voorwoord</i>	3
2	<i>Introductie</i>	4
3	<i>Facts & figures</i>	5
3.1	Wereldwijd.....	5
3.2	Europa.....	5
3.3	Nederland	6
4	<i>Privacy en echo-chambers, óók buiten facebook en twitter</i>	7
5	<i>Mogelijke gevolgen voor Nederland in de aanloop naar verkiezingen in maart 2021...</i>	8
6	<i>Wat kan hiertegen worden gedaan: door ondernemers en overheid?</i>	9
6.1	Nederlandse Tech-Ondernemers	9
6.2	Overheid.....	10
7	<i>Referentielijst</i>	12
8	<i>Colofon</i>	14

1 VOORWOORD

[TechTegenCorona](#) is een samenwerkingsverband van academici, uitvinders, > 300 Nederlandse tech-bedrijven, >2000 tech-experts die sinds de start van de COVID-19 crisis oplossingen zoeken voor maatschappelijke dilemma's. Zie ook het [Open Source document](#) met tips voor de 1.5 samenleving.

“Dit advies sluit goed aan bij de behoefte van Defensie, omdat er ook nagedacht wordt over ondermijning en ontwijking. Oorlog wordt al lang niet meer gevoerd met uitsluitend klassieke wapens, nu de beheersing en beïnvloeding van zowel kanalen als de inhoud van informatie een belangrijk doel van de militaire tegenstanders van ons land is geworden.”

~ Dr. Majoor. Hoogenboezem

“Algoritmen en online netwerken grijpen diep in het dagelijks leven van burgers en in openbaar bestuur. De overheid moet zijn rol pakken en burgers faciliteren in het doorzien van desinformatie en het begrijpen van de adviezen van Kunstmatige Intelligentie. Dit vereist geen technisch inzicht maar gezond verstand en nuchterheid. Dit rapport beoogt daarbij een handreiking te zijn”

~ Em. Prof. Dr. Roel Wieringa

“Vrijheid van meningsuiting is één van de belangrijkste kenmerken van de Nederlandse democratie. Daarom moeten wij dat koesteren en bewaken. En alert zijn op buitenlandse bots die kunstmatig tweespalt proberen aan te wakkeren. Dit advies probeert hier een bijdrage aan te leveren”

~ Elisabeth van der Steenhoven, voorzitter TechTegenCorona

Bij het schrijven van dit advies stond het waarborgen van de democratie centraal. TechTegenCorona zal nooit pleiten voor een advies die de vrijheid van meningsuiting inperkt. [Onze uitgangspunten zijn privacy en een non-intrusieve overheid.](#)

2 INTRODUCTIE

Dit advies gaat in op het samenvallen van de COVID-19 pandemie met de Nederlandse Tweede Kamerverkiezingen van maart 2021. Aanleiding voor dit advies is de volgende combinatie van factoren:

- De veelvuldige pogingen tot digitale ontwrichting & desinformatie *voorafgaand* aan verkiezingen in andere Westerse landen, met name de Baltische Staten,
- Het feit dat de pandemie leidt tot een toenemende *afhankelijkheid* van digitale communicatie- & een afname van rechtstreeks menselijk contact (IRL),
- Onderzoeken concluderen dat zowel *COVID-19* alsook toekomstige *vaccins* worden gebruikt om tweespalt te zaaien/versterken,

Het advies gebruikt hierbij twee concepten:

1. *Desinformatie*, het bewust verspreiden van foutieve en/of misleidende informatie ter beïnvloeding van politieke en/of maatschappelijke processen. Dit in tegenstelling tot *misinformatie* dat per ongeluk ontstaat. Het advies gaat ook niet over *fake news*, nu hieronder ook parodie of slechte journalistiek wordt geschaard.
2. *Digitale ontwrichting*, het bewust massaal delen van informatie om tweespalt te veroorzaken in de maatschappij, vaak door middel van bots en buitenlandse trollen. Dit kan, in tegenstelling tot desinformatie, met correcte informatie mits de informatie die wordt gedeeld polariseert.

Deze twee concepten brengen een dilemma met zich mee. Namelijk: hoe verhoudt desinformatie of digitale ontwrichting zich tot de vrijheid van meningsuiting? Waar houdt de vrijheid van meningsuiting op en waar begint desinformatie of digitale ontwrichting? Het strafrecht biedt hierbij weinig soelaas.

Een mogelijke deeloplossing is het identificeren van berichten die door duizenden (buitenlandse) bots worden gedeeld. Dit is echter slechts een aanwijzing - en zegt nog niets over het bericht zelf.

Dit advies begint met de huidige situatie omtrent des- en misinformatie, op basis van recent onderzoek. Vervolgens wordt het belang van privacy en het voorkomen van media-bubbles belicht. Hierna worden de mogelijke effecten van desinformatie op de Nederlandse verkiezingen besproken. Tot slot wordt er gekeken naar oplossingen. Het laatste onderdeel is opgesplitst in twee onderdelen: ondernemers en de overheid.

3 FACTS & FIGURES

3.1 WERELDWIJD

In een onderzoek uit 2018, schat het [Pew Research Centre](#)ⁱ dat 66% van alle tweets met een link naar een externe website zijn gemaakt door bots. Bots zijn vele malen actiever op het internet dan mensen. Zo schat het Pew Research Centre dat de 500 meest actieve bots verantwoordelijk zijn voor 22% van de getweete links, in tegenstelling tot de 500 meest actieve menselijke gebruikers die verantwoordelijk zijn voor 6%. Onderzoek gepubliceerd in [Nature Communications Journal](#)ⁱⁱ liet zien dat 6% van de bots verantwoordelijk is voor 31% procent van de tweets met een link naar een onbetrouwbare bron.

Een onderzoek van [de Computational Propaganda Research Project](#)ⁱⁱⁱ toonde aan dat tools zoals het gebruik van bots en het verspreiden van desinformatie werden gebruikt tijdens verkiezingen. Facebook was hierbij het meest populaire platform.

De periode voorafgaand aan verkiezingen leidt in toenemende mate (sinds 2017/2018) tot een hausse in desinformatie en/of digitale ontwrichting. Zo onthulde [Sophie Zhang](#)^{iv}, een voormalige Facebook-medewerker, een veelvoud aan gecoördineerde campagnes om politieke kandidaten een boost te geven of juist te hinderen. Zij noemde de volgende landen waarin Facebook als platform werd gebruikt om verkiezingen te beïnvloeden: **de VS, Malta, UK, Honduras, Azerbaidjan, Brazilië, Ukraine, Bolivia, Ecuador, Spanje en India**. Sophie Zhang en haar collega's hebben 10,5 miljoen nepaccounts en reacties verwijderd in o.a. Brazilië en de VS in 2018.^v Eén van de bekendste voorbeelden van microtargeting teneinde de uitslag van verkiezingen te beïnvloeden komt van [Cambridge Analytica](#).^{vi}

3.2 EUROPA

[De Europese Unie bracht op 19 oktober 2020 een nieuw beleid uit over desinformatie](#). Dit beleid geeft aan dat desinformatie in de EU steeds vaker voorkomt. Het afgelopen jaar richtte de desinformatie zich met name omtrent de COVID-19 crisis. Sinds het begin van crisis ziet de EU een toename van 45% van het gebruik van Twitter Moments, gegroepeerde tweets waarmee de wereldwijde verspreiding van het coronavirus kan worden gevolgd. Volgens Twitter zijn er meer dan 3,4 miljoen verdachte accounts aangepakt die het op gesprekken over COVID-19 hadden gemunt. YouTube heeft meer dan 100.000 video's over het COVID-19 virus getoetst aan eigen regels, 15% daarvan bleek gevaarlijke of misleidende informatie te bevatten en zijn verwijderd.^{vii} Desinformatie bereikt een groot publiek.

Volgens [Newsguard](#) kent Europa meer dan 448,000 mensen die sociale media accounts van QAnon volgen. Of QAnon daadwerkelijk een bron is van desinformatie wordt nog onderzocht. Wél is [geconstateerd dat oude antisemitische complottheorieën](#)^{viii} bij QAnon (opnieuw) opgeld doen (zie ook [nrc.nl](#)^{ix}).^x

In 2018 in [Litouwen](#), werd door de Russische overheid een publieke omroep gehackt die vervolgens desinformatie verspreidde. Litouwen heeft inmiddels een systeem van cyberreservisten opgericht die ingezet kunnen worden in de strijd tegen desinformatie.^{xi}

Tijdens de tweede ronde [van de 2017 verkiezingen](#) in Frankrijk bleek 16.4% van het verkeer op sociale media te zijn gegenereerd door bots.^{xii}

Niet-Engelstalige landen worden minder ‘beschermd’ tegen desinformatie dan Engelstalige landen. [In een onderzoek van EEAS en Avaaz](#) kwam naar voren dat blootstelling van gebruikers aan desinformatie vaker plaatsvond in niet-Engelstalige landen zoals Spanje en Italië. De NGO’s stelden dat dit komt doordat Facebook hier minder actief is in het verifiëren en verwijderen van content. 29% van al de Engelstalige content was niet geverifieerd in tegenstelling tot 68% van de Italiaanse en 70% van de Spaanse content.^{xiii xiv}(zie ook: eu.boell.org).

[EUvsDisinfo](#)^{xv}, een initiatief van [de European External Action Service](#)^{xvi} plaatst regelmatig artikelen, analyses en statistieken met betrekking tot Russische desinformatie campagnes. [Zo stelde EUvsDisinfo](#)^{xvii} dat pro-Kremlin media wederom een verhoging zagen van 1,1 miljard euro in hun budget.

3.3 NEDERLAND

Een in Nederland bekend voorbeeld van desinformatie zijn de berichten rondom het neerhalen van vlucht MH-17. Op 18 en 19 juli 2014 zijn meer dan [65.000 berichten](#) verspreid door een Russische trollenfabriek. Hierin werd Oekraïne beschuldigd van het neerhalen van vlucht MH-17.^{xviii}

[Onderzoek door het datajournalistiek platform Pointer](#) laat zien dat het merendeel van desinformatie in Nederland momenteel gaat over het COVID-19 virus. Zo vonden ze zelf 530 berichten met foutieve informatie over het COVID-19 virus. Deze zijn 12354 keer gedeeld door 3901 verschillende accounts.^{xix}

Ook vindt in Nederland maatschappelijke ontwrichting plaats. Enkele leden van TechTegenCorona wijzen op de [Zwarte Piet](#) discussie waarbij sommige foutieve berichten tienduizenden of honderdduizenden keren werden gedeeld.^{xx} Of deze berichten vanuit het buitenland komen kan niet met zekerheid worden vastgesteld.

Ook in Nederland ziet men [de verspreiding van complottheorieën](#) over onder andere QAnon en de schadelijkheid van 5G-netwerken.^{xxi} Zo vonden er [25 brandstichtingen](#) plaats bij 5G zendmasten om de verspreiding van het COVID-19 virus wegens 5G te voorkomen.^{xxii}

[QAnon](#) laat een lastig dilemma zien binnen de bestrijding van desinformatie. Desinformatie is het bewust verspreiden van foutieve en/of misleidende informatie ter beïnvloeding van politieke en/of maatschappelijke processen. Deze definitie wordt gehanteerd door het gros van [academici](#)^{xxiii} alsook [de Nederlandse overheid](#).^{xxiv} Of QAnon onder deze definitie valt is lastig te bepalen. Aanhangers van deze theorieën geloven immers zelf dat dit echt is en dat zij correcte informatie verspreiden. Bij de bestrijding van desinformatie moet dan ook voorzichtig worden opgetreden om niet de vrijheid van meningsuiting in te perken.



In de afgelopen tijd heeft Defensie (de landmacht) vier veelvoorkomende *narratives* geïdentificeerd:

1. Virus-narratief:
Met meer-of minder- wetenschappelijk onderzoek worden de COVID-19 maatregelen bekritiseerd, met name de anderhalve-meter maatregelen.
2. Rusland vs. EU:
Rusland wordt gepositioneerd als verlosser t.o.v. de EU. Dergelijke berichten krijgen opvallend veel retweets van anonieme accounts.
3. 5G-Narratief:
Volgens dit narratief zijn mensen vatbaarder voor COVID-19 door 5G-straling omdat deze straling het immuunsysteem aantast en het virus zelfs verspreidt.
4. Vaccinatie-narratief:
Dit narratief trekt de veiligheid van vaccins in het algemeen in twijfel. Het narratief richt zich voornamelijk op de gezondheidsrisico's van vaccins en een onverantwoorde, te snelle ontwikkeling van vaccins. Het narratief is ontstaan uit de theorie dat Bill Gates een vaccin zou gebruiken om de wereldbevolking te beïnvloeden.

4 PRIVACY EN ECHO-CHAMBERS, ÓÓK BUITEN FACEBOOK EN TWITTER.

Eén van de redenen waarom desinformatie voet aan de grond krijgt, zijn zogenaamde “echo-chambers” of “filter-bubbles”. Bij dit fenomeen wordt (ten onrechte) veelal aan Facebook, Twitter en Instagram gedacht. Dit fenomeen manifesteert zich juist ook op het ‘reguliere’ internet - hetgeen van belang is voor ambtenaren, politici, veiligheidsdiensten en beleidsmakers.

Ambtenaren, politici, veiligheidsdiensten, beleidsmakers en burgers gebruiken continu zoekmachines om informatie te vinden op het internet. Hierbij wordt vaak gebruik gemaakt van bekende zoekmachines die zoektermen opslaan en toevoegen aan een persoonlijk profiel, o.a. op basis van cookies of het IP-adres. Zo wordt bij de traditionele zoekmachines (zoals Google) bij elke zoekopdracht ongemerkt een extra puzzelstukje aan de totale puzzel toegevoegd. Er ontstaat een persoonlijk profiel waar, per gebruiker, toekomstige resultaten op worden gebaseerd.

Op basis van dit profiel is het heel eenvoudig om een gebruiker geraffineerd te manipuleren. Een algoritme kan bepaalde resultaten juist als eerste tonen, of deze juist *niet* bovenaan weergeven. Bijvoorbeeld voor commerciële doeleinden zoals target-advertising. Het gevolg is dat een persoon - ambtenaar, politicus of burger- steeds meer in een ‘bubble’ terechtkomt.

Om deze reden is het zinvol om zoekmachines te gebruiken die zoektermen *niet* opslaan.

5 MOGELIJKE GEVOLGEN VOOR NEDERLAND IN DE AANLOOP NAAR VERKIEZINGEN IN MAART 2021

In Nederland vallen ongelukkigerwijs deze herfst twee elementen samen: de ‘reguliere’ COVID-19 (en/of anti-vaccinatie) desinformatie én de desinformatie-hausse voorafgaand aan verkiezingen, zoals beschreven in de vorig paragraaf.

Immers; de ervaring uit andere landen (waaronder de Baltische staten, de VS, het VK (Brexit)) leert dat verkiezingen vaak een moment zijn waar buitenlandse actoren proberen tweespalt in de samenleving aan te wakkeren. Dit wordt ook bevestigd door recente analyses van o.a. de [European External Action Service^{xxv}](#), met als gevolg een [European Action Plan against desinformation^{xxvi}](#).

Het gevaar dat Nederland doelwit wordt van pogingen tot digitale ontwrichting neemt toe, zoals ook door [de Nederlandse overheid is geconstateerd^{xxvii}](#) [Kolonel Hans van Dalen \(Defensie\) stelt dan ook:](#) “Als gevolg van disruptieve informatietechnologie erodeert de democratie en neemt het vertrouwen in bestaande politieke, financiële, economische, juridische en zelfs maatschappelijke instituties af.”^{xxviii} Verder is er een afname van menselijke interactie i.v.m. COVID-19 & een toenemende digitalisering. Dit vergemakkelijkt digitale polarisatie.

Hierin kunnen drie mogelijke gevaren worden onderscheiden:

1. De verspreiding van des- en misinformatie kan resulteren in afnemend vertrouwen van de bevolking in de overheid en/of toenemende animositeit tussen bevolkingsgroepen. Een dergelijke polarisering is onwenselijk en maakt een land kwetsbaar.
2. Desinformatie over COVID-19 kan leiden tot zowel afname in testbereidheid alsook tot vaccinatie. Deze zijn beiden gevaarlijk voor de volksgezondheid.
3. Desinformatie kan leiden tot geweld. Bijvoorbeeld de [brandstichting van 5G masten^{xxix}](#).

6 WAT KAN HIERTEGEN WORDEN GEDAAN: DOOR ONDERNEMERS EN OVERHEID?

Om het democratisch proces te waarborgen tijdens de verkiezingen van 2021 is het zinvol om desinformatie van meerdere kanten te bestrijden. [De Nederlandse overheid heeft de belangrijkste stap al gezet](#): het onderwerp agenderen, bespreekbaar maken én mediawijsheid bij jongeren en volwassenen stimuleren.

Het gevaar van desinformatie en misinformatie ten tijde van COVID-19 én aankomende verkiezingen is dermate groot dat een ‘whole-of-government’ aanpak benodigd, tezamen met academici, burgers en tech-ondernemers. Om een paar voorbeelden te noemen:

De Nederlandse overheid kan lessons learned overnemen van de Baltische starten, inclusief het beleid om desinformatie binnen 24 uur te ontcrachten.

Kunstmatige Intelligentie kan worden gebruikt voor herkenning van [deepfakes](#).^{xxx} [Microsoft](#) heeft recentelijk een tool ontwikkeld dat een ‘echtheids- score’ geeft aan video’s.

Verder bestaat er een meldpunt voor desinformatie voor online bedrijven (zoals Google, Facebook, Twitter en Mozilla) in de Europese Unie. De platforms werken samen [met de nationale contactpunten](#) voor desinformatie en factcheckers, om te helpen bij de doeltreffende bestrijding van desinformatie.^{xxxi} Dit stimuleert een holistische aanpak tegen desinformatie.

6.1 NEDERLANDSE TECH-ONDERNEMERS

- Voor cloud-providers in Nederland geldt: [het notice-and-takedown-beleid](#)^{xxxii} (NTD) naleven (zie ook: [mijnonlineidentiteit.nl](#)^{xxxiii}). Dit beleid wordt al gebruikt omtrent [copyright in de EU](#).^{xxxiv} Het NTD beleid leent zich bij uitstek voor de strijd tegen desinformatie.

Bij de Notice-and-takedown-policy staat centraal dat:

- Er *actief* gezocht moet worden naar desinformatie.
 - Wanneer desinformatie wordt ontdekt en het strafrechtelijk verboden is het per direct wordt verwijderd. Snelle verwijdering sluit verdere verspreiding uit waardoor zo min mogelijk mensen worden beïnvloed.
 - De gebruiker die het bericht deelt, krijgt een melding dat de post is verwijderd en de reden hiervoor.
- Het stimuleren van het benoemen van desinformatie in de ‘fair-use-policy’ van websites en platfora. Dit wordt al geïmplementeerd bij sites als [Nu.nl](#)^{xxxv} waarin hun reactieplatform onwaarheden zoals het ontkennen van klimaatverandering verbiedt en verwijderd.

- Voor kleinere tech-bedrijven, tech-experts en de burgers blijkt er geen plek te zijn waar **desinformatie kan worden gemeld**. Grotere bedrijven/vitale sectoren zijn aangesloten bij een CERT/CSIRTS, dit is echter niet noodzakelijkerwijs een plek waar desinformatie kan worden gesignaleerd. Het zou de moeite waard zijn een plek te creëren waar de bevolking en grotere en kleinere tech/cyber bedrijven desinformatie kunnen signaleren. Soortgelijke meldpunten bestaan al voor andere zaken zoals kinderporno. Deze initiatieven zijn opgericht door burgers, los van de overheid.

Dit meldpunt zou burgers inzicht kunnen geven welke berichten zijn ‘gemanipuleerd’ (zoals deep fakes) danwel door een groot aantal buitenlandse bots worden gepusht. Het is *niet* de bedoeling om via dit meldpunt berichten te laten verwijderen. Dit zou de vrijheid van meningsuiting aantasten. Inmiddels heeft **een netwerk van tech experts zich bereid verklaard een dergelijk meldpunt op te zetten**. Hierbij staan transparantie en vrijheid van meningsuiting centraal. De meldingen worden gewogen door een Raad van Advies, hierin zullen ook ‘corona-tegenstanders’ plaatsnemen. Berichten die aantoonbaar zijn gemanipuleerd én als enig doel hebben om tweespalt te zaaien worden met een uitleg op de website gepubliceerd. In de uitleg staat hoeveel buitenlandse bots het bericht hebben gedeeld danwel de manier waarop beelden zijn gemanipuleerd. Het doel is het bevorderen van mediawijsheid.

- Platfora zoals Facebook, Instagram, Twitter en TikTok enz. beschikken allen over rapporteerfuncties; het zou de moeite waard zijn om burgers en bedrijven aan te moedigen om desinformatie actief te rapporteren.

6.2 OVERHEID

De Nederlandse overheid spant zich al jarenlang in tegen desinformatie, zie ook de Kamerbrieven d.d. [10 juli 2020](#)^{xxxvi} en [13 mei 2020](#)^{xxxvii}. Onderstaande adviezen zijn een vervolg hierop.

- Zélf in woord en daad het goede voorbeeld geven door zo transparant en accuraat mogelijk te communiceren. Nu Nederland de volgende COVID-19 fase ingaat is het wenselijk om -waar mogelijk- achterliggende onderzoeken & cijfers publiek te maken. Juist door gebrek aan transparantie en eenduidigheid neemt de ruimte voor desinformatie en complotten toe.
- Politici, ministers, Tweede en Eerste Kamerleden horen ook het goede voorbeeld te geven. Zo zouden zij een pact kunnen sluiten met burgers/kiezers waarin zij beloven geen ‘deep fakes’ te gebruiken, geen onwaarachtige montages te zenden en geen (bewezen) desinformatie te verspreiden. Vanzelfsprekend roept dit de vraag op hoe een dergelijk pact zich verhoudt tot vrijheid van meningsuiting; het is beslist de moeite waard om deze afweging *gezamenlijk* te maken - politici én kiezers.
- Desinformatie als gevaar benoemen en uitleggen. Nederlandse bevolking informeren over de manieren waarop desinformatie kan worden herkend alsook de gevaren van echo-chambers.
 - Deze informatie kan het beste worden verstrekt op plekken waar desinformatie het meest wordt verspreid, namelijk sociale media.
 - Mediawijsheid op scholen stimuleren en daar ruimschoots budget voor vrijmaken.

- Een vergaande intensivering van media-onderwijs voor volwassenen.
- Bevolking op de hoogte brengen van privacy-vriendelijke zoekmachines.
- Een Rijksbrede inzet tegen digitale ontwrichting met o.a. de volgende componenten:
 - Betrokkenheid van een breed scala aan actoren uit de samenleving, waaronder jongeren.
 - Debunken van schadelijke desinformatie op o.a. Facebook, Instagram , Reddit enz. op grond van (verifieerbare) argumenten.
 - Aan burgers, bedrijven, wetenschappers en betrokkenen tips & tools geven om desinformatie tegen te gaan.
- De Nederlandse Krijgsmacht heeft in de afgelopen jaren expertise opgebouwd omtrent desinformatie tijdens uitzendingen. Het is beslist de moeite waard om deze expertise in te zetten in de strijd tegen digitale ontwrichting door buitenlandse actoren. Zie ook <https://www.militairespectator.nl/militaire-spectator-2020-09>
- [Politieke partijen zouden nog transparanter kunnen zijn over politieke advertenties.](#)^{xxxviii}
 Politieke partijen zouden elke variatie van een advertentie die zij versturen op hun website kunnen publiceren.

Tot slot: er bestaat geen silver bullet tegen desinformatie. De beste afweer is een weerbare bevolking met een hoge media-wijsheid die zélf in staat is om afwegingen te maken. Burgers, bedrijven, wetenschappers, journalisten en de overheid kunnen allen hieraan bijdragen.

7 REFERENTIELIJST

- ⁱ <https://www.pewresearch.org/internet/2018/04/09/bots-in-the-tweetsphere/>
- ⁱⁱ <https://www.nature.com/articles/s41467-018-06930-7.pdf>
- ⁱⁱⁱ <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>
- ^{iv} <https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo>
- ^v <https://www.buzzfeednews.com/article/craigsilverman/facebook-ignore-political-manipulation-whistleblower-memo>
- ^{vi} <https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie>
- ^{vii} https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response/fighting-disinformation/tackling-coronavirus-disinformation_nl#resultaten-van-de-samenwerking-met-platforms
- ^{viii} <https://www.theatlantic.com/politics/archive/2020/08/conspiracy-theory-rule-them-all/615550/>
- ^{ix} <https://www.nrc.nl/nieuws/2020/09/14/qanon-springt-van-web-over-op-de-echte-wereld-a4011964>
- ^x <https://www.euronews.com/2020/07/30/qanon-theories-are-merging-with-european-conspiracies-report>
- ^{xi} <https://www.groene.nl/artikel/de-elfen-tegen-de-trollen>
- ^{xii} <https://www.rathenau.nl/nl/digitale-samenleving/digitalisering-van-het-nieuws/desinformatie-zo-werken-bots-nederland>
- ^{xiii} https://secure.avaaz.org/campaign/en/facebook_coronavirus_misinformation/
- ^{xiv} <https://eu.boell.org/en/2020/05/06/disinfo-reaches-epidemic-proportions-and-needs-serious-eu-response>
- ^{xv} <https://euvsdisinfo.eu/about/>
- ^{xvi} https://eeas.europa.eu/headquarters/headquarters-homepage/area/foreign-affairs_en
- ^{xvii} <https://euvsdisinfo.eu/figure-of-the-week-1-11-billion-euros/>
- ^{xviii} <https://www.groene.nl/artikel/nepnieuws-uit-sint-petersburg>
- ^{xix} <https://nos.nl/artikel/2344875-zeker-vijftig-accounts-verspreidden-nepnieuws-over-corona-in-nederland.html>
- ^{xx} <https://www.nu.nl/weekend/5523026/zo-wordt-nepnieuws-ingezet-bij-zwartepietendiscussie.html>
- ^{xxi} <https://www.nrc.nl/nieuws/2020/04/19/nana-denkt-dat-de-overheid-ons-uitdunt-met-5g-tijdens-corona-a3997217>
- ^{xxii} <https://www.apparata.nl/nieuws/5g-zendmasten-nederland-brand-36809#:~:text=Tot%20dusver%20zijn%20er%20volgens,een%20snelweg%20vlam%20hebben%20gevat.>
- ^{xxiii} <http://informationr.net/ir/18-1/paper573.html#.X3Lf52gzY2z>
- ^{xxiv} <https://www.rijksoverheid.nl/onderwerpen/desinformatie-nepnieuws>
- ^{xxv} https://eeas.europa.eu/topics/countering-disinformation_en
- ^{xxvi} https://ec.europa.eu/commission/sites/beta-political/files/factsheet_disinfo_elex_140619_final.pdf
- ^{xxvii} <https://www.rijksoverheid.nl/onderwerpen/desinformatie-nepnieuws/aanpak-desinformatie-en-nepnieuws>
- ^{xxviii} <https://www.militairespectator.nl/thema/operaties/artikel/mind-war>
- ^{xxix} <https://nos.nl/artikel/2330187-waarom-worden-door-heel-nederland-zendmasten-in-brand-gestoken.html>
- ^{xxx} <https://www.betterinternetforkids.eu/web/portal/practice/awareness/detail?articleId=5398982#:~:text=De%20epfakes%20are%20computer%2Dcreated%20artificial,action%20that%20never%20actually%20happened.&text=Deepfakes%20are%20fake%20videos%20created,machine%20learning%20and%20face%20swapping>
- ^{xxxi} https://ec.europa.eu/netherlands/news/eu-voert-de-strijd-op-tegen-fakenews_nl
- ^{xxxii} <https://noticeandakedowncode.nl/>
- ^{xxxiii} <https://www.mijnonlineidentiteit.nl/notice-and-takedown-procedure>
- ^{xxxiv} <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790#017.001>
- ^{xxxv} <https://www.nu.nl/nujij/5204540/nujij-huisregels.html>
- ^{xxxvi} https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2020Z13820&did=2020D29348
- ^{xxxvii} <https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2020Z08631&did=2020D18454>
- ^{xxxviii} <https://www.nrc.nl/nieuws/2020/07/24/online-politieke-advertenties-zo-houden-we-het-democratisch-a4006901>

^{xxxix} <https://fd.nl/opinie/1350025/maak-onze-verkiezingen-weerbaar-tegen-digitale-inmenging>

^{xxxx} <https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52020JC0008>

Dank aan:

Dr. Majoor Jaap Hoogenboezem, Bestuurskunde, Universiteit Maastricht
Em. prof. dr. Roel Wieringa, Informatie Systemen, Universiteit Twente

De bijdragen van TechTegenCorona leden zijn gebundeld door o.a.:

Elisabeth van der Steenhoven, voorzitter TechTegenCorona
Finn Visser, junior beleidsmedewerker TechTegenCorona
Daniëlle van Biezen, beleidsmedewerker TechTegenCorona
Hanna van Vuuren, beleidsmedewerker TechTegenCorona
Huib van Doorn, junior beleidsmedewerker TechTegenCorona

[TechTegenCorona.nl](https://www.techtegencorona.nl)



De documenten van TechTegenCorona zijn vrij van copyright, zie ook het Open Source documenten met adviezen over de 1.5 samenleving. Wil jij ook -op basis van vrijwilligheid- bijdragen aan het oplossen van hedendaagse dilemma's? En ben je bereid de Code of Conduct te ondertekenen m.b.t. Good Governance and Digital Do -No-Harm? Sluit je aan bij [TechTegenCorona.nl](https://www.techtegencorona.nl)