



SENAAT

De bestrijding van de inmenging door buitenlandse mogendheden met het oog op het ondermijnen van de democratische rechtsstaat

INFORMATIEVERSLAG

19 april 2024





De tekst kan worden gedownload op het volgende adres:
<http://www.senaat.be>

Ce texte est également disponible en français.

Secretariaat van de Commissie voor de Democratische Vernieuwing, Burgerschap en Internationale
Aangelegenheden:
comcivitas@senate.be
02/501 71 11

Verantwoordelijke uitgever:

Gert Van der biesen, secretaris-generaal van de Senaat
Natieplein 1, 1009 Brussel

Deze publicatie heeft een informatieve waarde. Aan het redigeren ervan werd de grootste zorg besteed, maar noch de Senaat noch de diensten kunnen aansprakelijk worden gesteld voor de inhoud van de publicatie.

Wettelijk depot: D/2025/3427/2



De bestrijding van de inmenging door buitenlandse mogendheden met het oog op het ondermijnen van de democratische rechtsstaat

INFORMATIEVERSLAG

19 april 2024

Dit verslag werd voorbereid door de Commissie voor de Democratische Vernieuwing, Burgerschap en Internationale Aangelegenheden

Rapporteurs:

de heer Coenegrachts, mevrouw Ryckmans en de heer Freches

Samenstelling van het adviescomité:

Voorzitter: Rodrigue Demeuse

Leden:

N-VA: Andries Gryffroy, Freya Perdaens, Nadia Sminate

Ecolo-Groen: Rodrigue Demeuse, Chris Steenwegen, Farida Tahar

Vlaams Belang: Adeline Blancquaert, Bob De Brabandere, Guy D'haeseleer

PS: Philippe Courard, Latifa Gahouchi, Laurent Léonard

MR: Véronique Durenne, Gregor Freches

CD&V: Kris Poelaert, Orry Van de Wauwer

Open Vld: Steven Coenegrachts, Willem-Frederik Schiltz

PVDA-PTB: László Schonbrodt, Ayse Yigit

Vooruit: Ludwig Vandenhove



BELGISCHE SENAAT

ZITTING 2023-2024

19 april 2024

Dossier nr. 7-344

Informatieverslag ter bestrijding van de inmenging door buitenlandse
mogendheden met het oog op het
ondermijnen van de democratische rechtsstaat

Parlementaire stukken:

7-344/1: Verzoek tot het opstellen van een informatieverslag

7-344/2: Verslag namens het adviescomité

7-344/3: Vaststellingen en aanbevelingen aangenomen door het adviescomité

7-344/4: Hoorzittingen

INHOUD

I. VOORWOORD	7
II. VASTSTELLINGEN	9
I. Wettelijk kader	
II. Algemene bespreking	10
III. AANBEVELINGEN	27
IV. HOORZITTINGEN	37
INFORMATIEVERSLAGEN: https://www.senate.be/informatieverslagen	39



I. VOORWOORD

Illegale buitenlandse inmenging is een verschijnsel van alle tijden en is onlosmakelijk verbonden met de geschiedenis van de internationale betrekkingen. De motieven lopen uiteen en kunnen van economische, militaire, geopolitieke of politieke aard zijn. Maar in de hedendaagse praktijk ligt aan de basis van dit soort buitenlandse inmenging steeds vaker de wens om de grondvesten van een democratische rechtsstaat te ondermijnen.

Een middel dat vaak wordt ingezet bij dergelijke inmenging is desinformatie. Daarom kan dit informatieverlag gezien worden als een logisch vervolg op het verslag over fake news (doc. Senaat, nr. 7-110/1 tot 4). Maar buitenlandse inmenging blijft niet beperkt tot het manipuleren van informatie via de traditionele media en sociale netwerken, of het manipuleren van gegevens op internet. Het gaat ook om het oneigenlijk gebruik van technologie om te destabiliseren, zoals cyberaanvallen, hacking of het gebruik van artificiële intelligentie, *deepfakes*, *spyware*, trollenlegers en *bots*. Buitenlandse inmenging kan ook de vorm aannemen van geheime financiering van politieke partijen, zakenlui of andere. Ten slotte kan ook economische dwang worden uitgeoefend of probeert men het middenveld te destabiliseren bijvoorbeeld via de universiteiten, niet gouvernementele organisaties (ngo), religieuze gemeenschappen of de diaspora.

Via al deze middelen proberen de aanstokers van de inmenging het democratisch debat in de samenleving te verstoren, verkiezingen te vervalsen of te manipuleren en de samenleving te polariseren om de maatschappelijke cohesie te beschadigen en te trachten het land onbestuurbaar te maken.

De doelstelling van dit informatieverlag, namelijk de bestrijding van de inmenging die erop gericht is democratische rechtsstaten te ondermijnen, is dus van groot belang in de huidige politieke context. We moeten erop toezien dat onze verkiezingen vrij en integer blijven, dat de individuele mensenrechten blijvend geëerbiedigd worden, dat de democratische instanties en de landen die de principes van de rechtsstaat in acht nemen, hun taken op een werkbare manier kunnen blijven uitoefenen.

Als de samenleving haar onafhankelijkheid wil bewaren en haar lot in eigen handen wil houden, moet ze dus waakzaam blijven met betrekking tot dergelijke dreigingen. Personen, regeringen, samenlevingen en internationale gemeenschappen moeten samenwerken aan een gecoördineerde aanpak om het beginsel van de democratische rechtsstaat te beschermen tegen buitenlandse inmenging. Om de integriteit van het democratisch proces te waarborgen, dient voor een holistische aanpak te worden gekozen om de weerbaarheid van zowel elke burger als van onze instellingen te versterken. Om inmenging te bestrijden zijn politieke, technologische, juridische, maar ook sociale maatregelen nodig.

Dit informatieverlag wil zijn steentje bijdragen tot dit onderwerp. In het eerste deel wordt een reeks vaststellingen uiteengezet die een stand van zaken van het verschijnsel als dusdanig weergeven. De gevaren en aandachtspunten, zoals uiteengezet door de zesentwintig sprekers tijdens de hoorzittingen, staan er ook in vermeld. In het tweede deel

van het verslag worden aanbevelingen geformuleerd voor alle burgers en overheden. Die aanbevelingen moeten helpen om het verschijnsel, dat zich doorgaans onder de radar ontwikkelt, af te bakenen en efficiënter te bestrijden.

De voorzitter,
Rodrigue DEMEUSE

De rapporteurs,
Steven COENEGRACHTS
Hélène RYCKMANS
Gregor FRECHES



VASTSTELLINGEN

I. WETTELIJK KADER

A. Internationale en Europese regelgeving

1. Het Verdrag van Wenen van 18 april 1961 inzake diplomatiek verkeer geeft expliciet aan, in artikel 41.1, dat buitenlandse diplomaten de plicht hebben om zich niet te mengen in de binnenlandse aangelegenheden van de ontvangende staat¹.
2. Vermeldenswaard is richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van verordening (EU) nr. 910/2014 en richtlijn (EU) 2018/1972 en tot intrekking van richtlijn (EU) 2016/1148 (NIS2-richtlijn). De Europese verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van richtlijn 2000/31/EG (de digitaaldienstenverordening) bevat elementen om desinformatie en informatiemanipulatie aan te pakken. De belangrijkste uitgangspunten zijn transparantie en verantwoording. De verordening moet samen gelezen worden met de praktijkcode 2022 inzake desinformatie².
3. Het Europees Parlement heeft op 10 maart 2022 beslist om een bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie (EU), met inbegrip van desinformatie, en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), in te stellen³.

De werkzaamheden van de commissie ING2 van het Europees Parlement resulteerden onder meer in:

- de resolutie van het Europees Parlement van 1 juni 2023 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2022/2075(INI));
 - de resolutie van het Europees Parlement van 13 juli 2023 over aanbevelingen voor de hervorming van de regels van het Europees Parlement inzake transparantie, integriteit, verantwoordingsplicht en corruptiebestrijding (2023/2034(INI)).
4. De Europese Commissie vaardigde een pakket maatregelen uit ter verdediging van de democratie (COM(2023) (630 final)). Het pakket bevat ook een aanbeveling over de transparantie van de financiering van het politieke leven want één van de grootste gevaren van buitenlandse inmenging is uiteraard de financiering van politieke partijen door landen als Rusland of China. Hierover kunnen evenwel geen maatregelen worden genomen door de EU, omdat dit een nationale bevoegdheid betreft. Er kunnen dus hoogstens Europese aanbevelingen geformuleerd worden op dat vlak⁴.

1. dr. Luca Ferro, assistant professor internationaal recht, Vrije Universiteit Brussel.

2. De heer Lutz Güllner, *Head of Strategic Communications, European External Action Service (EEAS)*.

3. De heer Dirk Janvier, afdelingscommissaris, Algemene Dienst inlichting en veiligheid (ADIV).

4. De heer Raphaël Kergueno, *senior policy officer, Transparency International EU*.

B. Nationale regelgeving

5. Volgens de heer Luca Ferro, *assistant professor* internationaal recht aan de Vrije Universiteit Brussel, staat het de nationale regelgever vrij om wetten aan te nemen die bijvoorbeeld de buitenlandse financiering van politieke campagnes aan banden leggen, of die een transparantieplicht opleggen aan lobbyisten naar analogie van de *Foreign Agents Registration Act* in de Verenigde Staten (VS). De spreker stelt dat niets verhindert dat België, al dan niet in EU verband, opteert voor een striktere wetgeving dan wat internationaalrechtelijk van toepassing is, zolang daarmee de geldende internationale voorschriften niet worden overtreden.
6. De organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten omschrijft inmenging als: «de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden» (art. 8, 1^o g))⁵.
7. Volgens de heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen aan de Universiteit Antwerpen, is er nood aan (extra) analyse van de bestaande achterpoortjes en de tekortkomingen van huidige lobbywetten, van bestuurlijke en maatschappelijke kwetsbaarheden, van nationale initiatieven en tegenmaatregelen, van de motieven en doelen van de agressoren en van de effecten van algoritmes.
8. Er werden wetgevende initiatieven genomen, onder meer de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (de BIM-wet), en er werden meer middelen vrijgemaakt. De Veiligheid van de Staat (VSSE) zit op een groeipad richting duizend effectieven en de Algemene Dienst inlichting en veiligheid (ADIV) lanceerde onlangs het *Cyber Command*. De diensten staan er beter voor en dit werpt heel zeker vruchten af: *Qatargate* is hier een mooie illustratie van⁶.
9. Het nieuwe boek II van het Strafwetboek (doc. Kamer, nr. 55 3518/013) bevat een aantal bepalingen die handelingen strafbaar stellen die als buitenlandse inmenging kunnen worden beschouwd. Het betreft de bepalingen van titel 8 «Misdriften tegen de Staat en zijn functioneren», en meer bepaald de artikelen 546 (aanvaarding van buitenlandse steun aan ondermijning van de essentiële nationale belangen), 573 (steun aan de politiek of doelstellingen van de vijand), 574 (aan het wankelen brengen van de trouw aan de Staat) en 596 (verstrekken van foute essentiële informatie) alsook artikel 638 (publieke omkoping).

C. Bevoegdheidsverdeling in België

10. Ten dienste van de afbakening van de materie maakt de VSSE geen gebruik van de term «beïnvloeding». De term «inmenging» is duidelijk gedefinieerd in de wet die de bevoegdheden van de inlichtingendiensten regelt, namelijk de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten⁷.
11. Dezelfde wet bepaalt de opdrachten van de betrokken diensten. De ADIV doet vaststellingen en ontvangt informatie: als deze kaderen binnen hun opdracht, kan een onderzoek worden opgestart. De onderzoeken kunnen ervoor zorgen dat bijvoorbeeld het gerecht wordt ingeschakeld, dat veiligheidsmachtigingen worden ingetrokken, enz. In principe bepaalt de dienst autonoom welke onderzoeken er gevoerd worden zolang ze binnen de opdracht passen. De dienst valt uiteraard onder de controle van het Vast

5. De heer Dirk Janvier, afdelingscommissaris, ADIV.

6. De heer Kristof Clerix, onderzoeksjournalist, Knack.

7. De heer Peter Lanssens, directeur van de Analyse, Veiligheid van de Staat (VSSE).

Comité I dat ten allen tijde inzage kan krijgen in de lopende onderzoeken, deze kan becommentariëren of aanbevelingen doen indien nodig⁸.

12. De Cel voor financiële informatieverwerking (CFI) is een instantie die zich actief bezighoudt met het voorkomen van het witwassen van geld en de financiering van terrorisme. Zij kan bijvoorbeeld haar analisten niet vragen een onderzoek in te stellen op basis van een persartikel. De CFI kan alleen werken op basis van een verslag dat is opgesteld, hetzij door de onderworpen entiteiten, hetzij door de administratieve diensten van de Staat, en tot op zekere hoogte ook door het openbaar ministerie als het gaat om terrorisme. De Cel kan ook optreden in het geval van een verwijzing door een vergelijkbare buitenlandse autoriteit. Er zijn ongeveer honderdzestig van dergelijke eenheden in de wereld⁹.
13. De Gewesten zijn momenteel niet betrokken bij de aanpak van inmenging.
14. De ADIV gaat in principe niet in overleg met gouverneurs¹⁰.
15. Wat de contacten met de politiediensten betreft, is er onder andere een effectieve interactie tussen de VSSE en de lokale politie via de Lokale Taskforces. Hierbij wordt onder meer een beroep gedaan op een *information officer*, die het directe aanspreekpunt voor de burgemeester is. Op die manier wordt er een efficiënte informatiestroom gegarandeerd¹¹.
16. Voor wat betreft de communicatie tussen de verschillende politiediensten onderling, zijn er zeker op het vlak van terrorisme mechanismen in werking waar veel informatie wordt uitgewisseld, ook in de *Agile Taskforce Information Operations* (ATFIO) (die intussen weliswaar is vervangen door andere samenwerkingsverbanden met hetzelfde opzet) bestaat er een samenwerking op dat vlak¹².

De invoering van *information officers* als rechtstreeks aanspreekpunt voor de burgemeester zorgt voor een efficiënte informatiedoorstroom, net als de antiterrorismede-forums¹³: vergaderingen met alle veiligheidspartners op arrondissementsniveau.

II. ALGEMENE BESPREKING

A. Buitenlandse inmenging met het oog op het ondermijnen van de democratische rechtstaat

1) Definitie

17. Een definitie formuleren van «buitenlandse inmenging» is ingewikkeld: het kan gaan om buitenlandse staten, buitenlandse burgers of buitenlandse belangen.

Inmengingsoperaties zijn handelingen die erop gericht zijn buitenlandse belangen te bevorderen door de onrechtmatige inzet van *soft power* om de integriteit van politieke processen en gedragingen te corrumperen. Het begrip *soft power* staat centraal. Bij inmengingsoperaties gaat het niet echt om dwang, maar meer om overtuigingshandelingen die het politieke gedrag beïnvloeden¹⁴.

18. De Noord-Atlantische Verdragsorganisatie (NAVO) hanteert veeleer de term *hybrid interference* waarmee verwezen wordt naar een verzameling van verdoken, niet-

8. De heer Dirk Janvier, afdelingscommissaris, ADIV.

9. De heer Philippe de Koster, voorzitter, Cel voor financiële informatieverwerking (CFI).

10. De heer Dirk Janvier, afdelingscommissaris, ADIV.

11. De heer Peter Lanssens, directeur van de Analyse, VSSE.

12. De heer Dirk Janvier, afdelingscommissaris, ADIV.

13. Jaarrapport van de Veiligheid van de Staat, 2019, blz. 18.

14. Mevrouw Sofia Collignon, *lecturer (assistant professor)*, School of politics and IR, Queen Mary University of London.

militaire middelen met als doel het ondermijnen van de interne cohesie en het versterken van de politieke polarisatie. Het betreft heimelijke manipulatie van de strategische belangen van andere staten. De term *hybrid interference* moet duidelijk onderscheiden worden van *hybrid warfare*, dat als een militaire benadering moet beschouwd worden. Drie instrumenten staan centraal in *hybrid interference*: clandestiene diplomatie, geo-economie en desinformatie¹⁵.

19. Het besluit van het Europees Parlement van 10 maart 2022 over de instelling van een bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (ING2) stelt dat inmenging gaat over kwaadwillende en autoritaire buitenlandse overheids- en niet-overheidsactoren die gebruikmaken van manipulatie van informatie en andere tactieken om zich in democratische processen in de EU te mengen. Het uiteindelijke doel is de Europese democratie te destabiliseren¹⁶.
20. Er zijn gradaties van inmenging, zoals wordt geïllustreerd in het schematisch overzicht in een *Policy Brief* van het *Clingendael Institute* over de Europese initiatieven tegen inmenging. Het schema bevat een trappensysteem dat gaat van transparante beïnvloeding van de publieke opinie tot paramilitaire operaties waarbij mensen worden omgebracht. Dit toont aan dat er een volledig spectrum van vormen van inmenging bestaat. De begrippen moeten dus duidelijk afgebakend worden. Invloed is in alle geval geen synoniem voor inmenging. Er ligt een vage grens tussen legitieme beïnvloeding en ongeoorloofde manipulatie¹⁷.
21. Rechtmatige invloed en onwettige inmenging zijn twee conceptuele polen in een spectrum van soortgelijke activiteiten. Bepalen wat rechtmatig is, is een intrinsiek politieke activiteit¹⁸.
22. Invloed is normaal en maakt deel uit van de diplomatie. Het feit dat andere (private) actoren proberen om onze besluitvormingsprocessen in hun voordeel te beïnvloeden, maakt deel uit van de traditionele manier van zaken of handel doen. Er stelt zich geen probleem zolang dit legitiem gebeurt.

Ongeoorloofde inmenging daarentegen is wel problematisch. Inmenging omvat heimelijke, misleidende, dwingende, corrumperende of andere illegale activiteiten van een buitenlandse statelijke of niet-statale actor die ingaan tegen onze soevereiniteit, waarden en belangen.

Inmenging gebeurt in het voordeel van de politieke, economische, en socio-culturele belangen van de agressor. Transparantie en openbaarheid maken plaats voor heimelijke, misleidende, dwingende of zelfs corrumperende handelingen. Het is een belangrijk gegeven dat de agressor niet altijd een statelijke actor maar evengoed een niet-statale actor kan zijn.

23. Inmenging is problematisch van zodra besluitvormingsprocessen worden beïnvloed en er gepoogd wordt om strategische economische processen te infiltreren en te manipuleren in het voordeel van de agressor en ten nadele van onze maatschappij en democratische waarden¹⁹.

Inmenging maakt deel uit van de geschiedenis van de internationale betrekkingen. In verschillende landen bestaat er een ingeburgerde term om het fenomeen te om-

15. De heer Dirk Janvier, afdelingscommissaris, ADIV.

16. De heer Dirk Janvier, afdelingscommissaris, ADIV.

17. De gradaties worden duidelijk geïllustreerd in een schema met een trappensysteem: zie *Realising the EU Hybrid Toolbox: opportunities and pitfalls* (December 2022, Kenneth Lasoen, *Clingendael Policy Brief*).

18. Prof. Dr. Alexander Mattelaer, *vice dean research*, *Brussels School of Governance*, Vrije Universiteit Brussel.

19. Prof. Dr. Alexander Mattelaer, *vice dean research*, *Brussels School of Governance*, Vrije Universiteit Brussel.

schrijven: «*the silent option*», «*the hidden hand*», «*special projects*», «psychologische oorlogsvoering»; de Russen hebben het bijvoorbeeld over «actieve maatregelen»²⁰.

2) Versterkende rol van artificiële intelligentie

24. Voor wat betreft de mogelijke impact van een tool als *ChatGPT* op vlak van desinformatie, wordt gesteld dat artificiële intelligentie (AI) nu al volop aan zet is. Het *Advanced Impact Media Solutions* (AIMS)-systeem van het hieronder vermeld bedrijf «*Team Jorge*» heeft een AI-component die ervoor zorgt dat de gebruiker van het systeem zelf geen berichten meer hoeft te schrijven in naam van de avatars: een paar steekwoorden en een «toon» (neutraal, negatief, positief) voldoen: het systeem doet de rest. Content wordt dus zeker al automatisch gecreëerd²¹.
25. Volgens de heer Raphaël Glucksmann, voorzitter van de bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie, en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), vormt artificiële intelligentie (AI) een zeer groot probleem voor onze democratieën. Er is nood aan reglementering, alsook aan controle en een vorm van traceerbaarheid. Het grote probleem van het genereren van beelden of klankfragmenten via artificiële intelligentie is dat dit productieproces «achter de schermen» gebeurt: dat is de kern van de problematiek die moet aangepakt worden²². De suggestie vanwege sommige bekende figuren om tijdelijk de ontwikkeling van deze technologie stop te zetten, kan enig nut hebben omdat het ons wijst op de gevaren, maar de heer Glucksmann acht het niet echt waarschijnlijk dat het wetenschappelijk onderzoek op vlak van AI kan worden stopgezet.
26. Volgens de heer Maxime Lebrun, *deputy director - Research & Analysis in The European Centre of Excellence for Countering Hybrid Threats*, is de rode draad in de discussie over artificiële intelligentie het algoritmebeheer. AI is een zelflerend algoritme; het maakt gebruik van technologie om berekeningen te maken en om een groot aantal datasets met elkaar te vergelijken om zo een oplossing te vinden voor een gegeven probleem. De moeilijkheid in verband met beheerskaders voor algoritmen gaat over de keuze van de sector waarin ze van toepassing zijn. De ontwikkeling van artificiële intelligentie zal niet opgeschort worden; deze technologie kan niet verboden worden want dat zou ingaan tegen de loop van de geschiedenis en de ontwikkeling van wetenschap en technologie. Volgens de heer Lebrun, is het voornamelijk een politieke keuze: er moet bepaald worden in welke sectoren de regulering van algoritmebeheersingstechnieken al dan niet wenselijk is. Mag politieke communicatie bijvoorbeeld gebaseerd zijn op algoritmes? Met andere woorden: is het ethisch verantwoord en wenselijk voor het democratische debat dat dit soort van hulpmiddelen gebruikt worden door politieke partijen in de verkiezingsperiode? Overigens is het zo dat het gebruik van artificiële intelligentie in domeinen als de strijd tegen de klimaatopwarming, ruimtelijke ordening of volksgezondheid heel nuttig lijkt en oplossingen kan aanbrengen voor grote problemen waar we tegenwoordig mee geconfronteerd worden.

Volgens de heer Lebrun is het niet de regulering van de inhoud van de boodschappen die van belang is - behalve wanneer die inhoud onwettig is, zoals bij het oproepen tot haat of bij ongeoorloofde content - maar moet men veeleer een reglementair kader overwegen om te voorkomen dat de gebruikte algoritmen het democratisch debat

20. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

21. De heer Kristof Clerix, onderzoeksjournalist, Knack.

22. Ook de Senaat onderzocht eerder al de rol van artificiële intelligentie bij de productie en verspreiding van fake news (doc. Senaat, nr. 7-110).

grondig zouden vervalsen. Dat geldt in het bijzonder voor grote digitale platformen en/of sociale netwerken. Het gaat om een politieke keuze die erop gericht moet zijn te bepalen in welke sectoren het gebruik van algoritmen wenselijk is of aan reglementering dient te worden onderworpen.

3) Uitingen van buitenlandse inmenging

27. De resolutie van het Europees Parlement van 10 oktober 2019 over buitenlandse inmenging in verkiezingen en desinformatie in de nationale en Europese democratische processen (2019/2810(RSP)) schetst een overzicht van de verscheidenheid aan vormen van buitenlandse inmenging en van de mogelijke aandachtspunten.
28. Volgens het Amerikaanse *Federal Bureau of Investigation* (FBI) kunnen inmengingsoperaties zich als volgt manifesteren:
- criminele pogingen om het stemmingsproces te ondermijnen en in illegale campagne-financiering te voorzien;
 - cyberaanvallen op de steminfrastructuur, samen met computerinbraken gericht op onder meer verkozen ambtenaren, verkiezingsuitslagen en verkiezingskandidaten. Tijdens de hoorzittingen werd er door mevrouw Sofia Collignon verwezen naar een specifieke beïnvloedingsoperatie: online desinformatiecampagnes die regelmatig worden gevoerd en bijdragen tot de verspreiding van verkeerde informatie met als doel de verkiezingsuitslag te beïnvloeden of de kwaliteit van het verkiezingsproces in twijfel te trekken²³.

a) Via de reverse OODA-loop

29. Tijdens de hoorzittingen werd o.a. verwezen naar het systeem dat gebaseerd is op inversie op basis van de OODA-loop (*observe–orient–decide–act–cyclus*). Het gaat om een beproefde techniek die vooral wordt gebruikt door piloten om aan targeting te doen.

De «agressor» vertrekt van het eindpunt, dat wil zeggen het gewenste scenario. Van hieruit gaat men aan *reverse engineering* doen en de etappes overlopen van hoe men het doelwit effectief - onbewust - uit eigen beweging kan doen handelen om dat eindresultaat te bewerkstelligen.

De gestelde strategische doelen zijn:

- inlichtingen over het doelwit verkrijgen via spionage, dat wil zeggen meer weten over het doelwit dan het doelwit over zichzelf weet. Hiervoor moet de agressor heel goed de kwetsbaarheden van het doelwit kennen alsook de nodige kanalen om het doelwit te kunnen manipuleren;
- besluitvorming manipuleren over de ganse lijn en
- democratische waarden ondermijnen²⁴.

b) Via in desinformatie gespecialiseerde privé-ondernemingen

30. Het *Pegasus*-project, opgezet door een journalistencollectief, onthulde dat journalisten en mensenrechtenactivisten wereldwijd het slachtoffer waren geworden van de *Pegasus-spyware*, ontwikkeld door de Israëlische *NSO Group*. Ook in België waren er slachtoffers van de software, onder meer Carine Kanimba, dochter van *Hotel Rwanda*-held Paul Rusesabagina, die vermoedelijk door Rwanda werd bespioneerd, en El Mahjoub Maliha, een mensenrechtenactivist afkomstig uit de Westelijke Sahara die

23. Mevrouw Sofia Collignon, *lecturer (assistant professor)*, School of politics and IR, Queen Mary University of London.

er van uit gaat dat hij door Marokko werd gevolgd. De software in kwestie liet toe om vanop afstand de software van smartphones volledig over te nemen en te controleren²⁵.

De heer Kristof Clerix, onderzoeksjournalist bij Knack, suggereert om de inzet van *Pegasus-spyware* in België te vervolgen, transparant te communiceren over de intelligence- en gerechtelijke onderzoeken hieromtrent, en om via Buitenlandse Zaken een duidelijk signaal uit te sturen naar de betrokken landen dat de inzet van dit soort *spyware* in België niet geduld wordt.

Het project *Story Killers* - een internationaal project van een journalistencollectief dat ertoe strekt die organisaties en bedrijven te onderzoeken die gespecialiseerd zijn in het manipuleren van de publieke opinie en het verspreiden van valse informatie - heeft op zijn beurt aangetoond, dat operaties die vroeger enkel door landen werden opgezet, nu ook voor en door particulieren/bedrijven worden georganiseerd:

- *Team Jorge* bijvoorbeeld is een privéspeler, weliswaar met roots in het Israëlische leger; het kan ingeschakeld worden voor éénieder die geld op tafel legt;
- *NSO Group*, het bedrijf achter *Pegasus*, werkte daarentegen enkel samen met overheden²⁶.

c) Via politieke actoren

31. Inmenging kan ook de vorm aannemen van maatschappelijke subversie en ongeoorloofde pogingen, via mandatarissen of hoge functionarissen of drukingsgroepen, om druk uit te oefenen op de besluitvorming en de wetgeving²⁷.

d) Via verenigingen en instellingen

32. Een bekend voorbeeld is het Confuciusinstituut dat gefinancierd wordt door de Chinese overheid. Via activiteiten op universiteiten probeert het een gunstiger beeld van China te projecteren en tegelijk te infiltreren in de kenniseconomie waarbij het aast op de resultaten van R&D en/of leningen verstrekt onder bepaalde voorwaarden²⁸.

e) Via kerken en religieuze groeperingen

33. De VSSE onderzoekt in het kader van haar wettelijke opdracht met betrekking tot inmenging bijvoorbeeld ook mogelijke vormen van ongeoorloofde, bedrieglijke of clandestiene beïnvloeding via kerken en religieuze groeperingen. In het kader van de oorlog in Oekraïne bijvoorbeeld werd in verschillende Europese landen vastgesteld dat Rusland invloed probeert uit te oefenen via de Russisch Orthodoxe kerk. Daarnaast wordt in de procedure die in België wordt aangewend voor de erkenning van een eredienst of een levensbeschouwing, het advies van de VSSE en van andere veiligheidspartners gevraagd. Een van de aspecten die de VSSE nakijkt is het risico op inmenging, volgens de definitie in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Een andere partner die wordt bevraagd is de CFI, dewelke onderzoek kan voeren naar mogelijke financiering uit een derde land²⁹.

f) Via «influencers» of bekende personen

34. Een andere mogelijke manier van inmenging in de aangelegenheden van een derde land is rekrutering, plaatsing of het dwingen, op korte of lange termijn, van individuen op strategische posities (*social engineering*, omkoping, chantage of intimidatie)³⁰.

25. De heer Kristof Clerix, onderzoeksjournalist, Knack.

26. De heer Kristof Clerix, onderzoeksjournalist, Knack.

27. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

28. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

29. De heer Peter Lanssens, directeur van de Analyse, VSSE.

30. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

g) Via cyberaanvallen

35. Op vlak van tactieken en technieken kan er sprake zijn van cyberintrusie (sabotage) of acquisitie van kritieke (cyber)infrastructuur voor spionage of dwang. Een voorbeeld hiervan is het gebruik van communicatietechnologie van Chinese makelij waarbij het risico bestaat dat China de communicatielijnen gaat beheersen. De VSSE heeft hier in ieder geval al voor gewaarschuwd³¹.

h) Via economische dwang

36. Op financieel vlak komt inmenging er op neer om financiële afhankelijkheid te creëren van het doelwit via strategische investeringen, schenkingen aan belangengroepen of politieke partijen of onderzoeksfinanciering. Wat dit laatste betreft, kan worden verwezen naar de praktijken van het hogervermelde Confuciusinstituut³².

4) Risico's voor de democratie

37. Buitenlandse invloeden manifesteren zich niet enkel in het politiek systeem maar kunnen ook gericht zijn op de rechterlijke macht³³.
38. Het is een uitdaging om te bepalen hoe met binnenlandse actoren moet worden omgegaan in de context van beïnvloedingsoperaties: het kan namelijk zo zijn dat een binnenlandse actor de belangen van een buitenlandse mogendheid verdedigt omdat er affiniteit aan zet is en dat er geen sprake is van een doelbewuste demarche: hoe bepaal je of waar leg je de grens tussen wie dader en wie slachtoffer is en waar het buitenlandse belang zich manifesteert³⁴?
39. De verspreiding van desinformatie over kandidaten heeft gevolgen voor de verkiezingen:
- we kunnen namelijk met zekerheid zeggen - hoewel het moeilijk is om in elk specifiek geval na te gaan welke bron er aan de oorsprong ligt en welke buitenlandse invloed er wordt nagestreefd - dat het de bedoeling is om de verkiezingsuitslag te beïnvloeden aangezien kandidaten die grote kanshebber zijn om de verkiezingen te winnen meer kans lopen om het doelwit van desinformatie te zijn;
 - we weten dat de georkestreerde pogingen om desinformatie over politieke actoren te verspreiden de kandidaten in gevaar kunnen brengen³⁵.
40. De inmenging door «partnerlanden» vormt een bijzonder probleem. De behandeling van flagrante inmenging door landen waarmee België nauwe betrekkingen onderhoudt - en de aanwezigheid van een grote diaspora is daar vaak niet vreemd aan - vereist bijzondere voorzorgsmaatregelen om een juiste kosten-batenverhouding te handhaven. De Belgische overheid gaat in dergelijke gevallen dan ook voorzichtig en beredeneerd te werk, met name door de kwestie buiten de media om te behandelen en door, indien nodig, de voorkeur te geven aan uitzetting boven vervolging van de betrokkenen. De banden met landen als Marokko en Turkije zijn in deze context goede voorbeelden. De kwestie van inmenging kan in dezen niet *ex nihilo* worden behandeld, maar moet gekaderd worden rekening houdend met de context van de bestaande betrekkingen met de desbetreffende partners³⁶.
41. Ten gevolge van - of samengaan met - een brutaal klimaat van informatieverbreiding, is er de impliciete insinuatie of zelfs expliciete aanmoediging van een gewelddadige eschatologie in het discours, in de parlementaire debatten en in de sociale protesten. Deze gewelddadige ondertoon zoekt aansluiting bij een discours dat elke vorm van

31. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

32. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

33. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

34. Mevrouw Sofia Collignon, lecturer (assistant professor), *School of politics and IR, Queen Mary University of London*.

35. Mevrouw Sofia Collignon, lecturer (assistant professor), *School of politics and IR, Queen Mary University of London*.

36. De heer Michel Liégeois, professor, *Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain*.



politieke dialoog uitsluit. Het herhaaldelijk beledigen tijdens het parlementair debat en diaboliseren van tegenstanders leveren voedingsbodem voor radicalisering en voor fysiek en politiek geweld dat een rechtstreekse bedreiging vormt voor een vreedzaam parlementair debat en een verdraagzame politieke dialoog³⁷.

42. Een onderzoek over de kandidaten voor de Britse verkiezingen van 2019 toonde aan dat de doelwitten van desinformatie herleid konden worden tot bepaalde groepen: kandidaten van zwarte en Aziatische minderheidsgroepen waren significant vaker het doelwit. Dit betekent dus dat desinformatiecampagnes kunnen worden ingezet als een georganiseerde poging om de vertegenwoordiging van bepaalde personen met bepaalde kenmerken te ondermijnen³⁸.
43. Onderzoek wees ook uit dat kandidaten die het slachtoffer zijn van desinformatie de oorzaak hiervan bij hun tegenstanders leggen, ook al geven ze toe dat ze eigenlijk niet echt weten wie aan de oorsprong ligt van de desinformatie. En zelfs als dit nog technisch kan worden nagetrokken, blijft het sneeuwbal effect ervan moeilijk te stoppen. Het is bewezen dat desinformatie tot andere vormen van intimidatie en geweld kan leiden. Het is ook geweten dat ingrepen op kleinere schaal door het sneeuwbal effect heel grote gevolgen kunnen hebben³⁹.

B. Belangrijkste actoren

1) «Positieve» actoren die pogingen tot inmenging proberen tegen te gaan en te voorkomen

a) Internationaal

44. *Transparency International* (TI) is een wereldwijde beweging die zich inzet tegen corruptie. TI is aanwezig in 126 landen. De instelling werkt rond verschillende thema's. Het kantoor in Brussel werkt vooral rond en met de Europese instellingen. Hierbij doet TI aanbevelingen aan de EU-instellingen om hun politieke integriteit te optimaliseren⁴⁰.
45. Op het niveau van de EU werd binnen het Europees Parlement de hoger vermelde Bijzondere Commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2) opgericht. Deze commissie formuleerde op 13 juli 2023 de eerder vermelde resolutie 2023/2034 (INI) die precieze aanbevelingen bevat met oplossingen voor vormen van kwaadwillige buitenlandse inmenging. Ze stelde ook regels op om belangenconflicten te voorkomen, de transparantie te verbeteren en om buitenlandse inmenging en corruptie te voorkomen, te ontmoedigen en op te sporen.
46. De benadering van de problematiek van inmenging kan niet ruim genoeg zijn omdat ze impact heeft op alle lagen van de samenleving. De omschrijvingen die gehanteerd worden binnen de EU en de Noord-Atlantische Verdragsorganisatie (NAVO) kunnen hier tot leidraad dienen⁴¹.
47. Disruptie en reglementering kunnen ingezet worden om bepaalde situaties een halt toe te roepen, ook al is dat niet eenvoudig.

Op digitaal vlak kunnen er bijvoorbeeld verschillende tools ingezet worden. Daarnaast is er ook de hogervermelde digitale dienstenverordening en de aangescherpte praktijkcode 2022 inzake desinformatie. Het gaat om een zelfreguleringscode voor alle

37. De heer Maxime Lebrun, *deputy director - Research & Analysis, The European Centre of Excellence for Countering Hybrid Threats*.

38. Mevrouw Sofia Collignon, *lecturer (assistant professor), School of politics and IR, Queen Mary University of London*.

39. Mevrouw Sofia Collignon, *lecturer (assistant professor), School of politics and IR, Queen Mary University of London*.

40. De heer Raphaël Kergueno, *senior policy officer, Transparency International EU*.

41. De heer Dirk Janvier, *afdelingscommissaris, ADIV*.

grote platforms die streeft naar een evenwicht tussen een concrete aanpak van informatiemanipulatie en desinformatie, en de vrijheid van meningsuiting.

b) In België

48. Op Belgisch niveau kan onder meer verwezen worden naar de Veiligheid van de Staat (VSSE), de Algemene Dienst inlichting en veiligheid (ADIV), de federale gerechtelijke politie (FGP) en in het bijzonder de Centrale Dienst voor de bestrijding van corruptie (CDBC), het Coördinatieorgaan voor de dreigingsanalyse (OCAD), de Cel voor financiële informatieverwerking (CFI) en het Centrum voor cybersecurity België (CCB).
49. De heer Alexander Mattelaer, *vice dean research, Brussels School of Governance* aan de Vrije Universiteit Brussel, stelt dat het recent operationeel verklaarde *Cyber Command* van de Belgische Defensie zich onder meer toelegt op het detecteren van digitale beïnvloedingsoperaties en eventuele pogingen van buitenlandse overheden om verkiezingen te manipuleren via sociale media. Het is verre van ondenkbaar dat er in de toekomst meldingen worden gedaan van georkestreerde desinformatiecampagnes met als doel de verkiezingsresultaten te manipuleren. Dit maakt het noodzakelijk om na te denken over de te volgen procedures en over de vraag hoe de eigen strategische communicatiecapaciteit versterkt kan worden in de gevallen dat de bevindingen van onze eigen overheden actief gecontesteerd worden door buitenlandse actoren.
50. Het huidige digitale tijdperk, houdt in dat er rekening moet worden gehouden met (legitieme en niet legitieme) invloeden uit allerhande hoeken. Het verminderen van de impact van vijandige invloeden op de bevolking is dan ook van cruciaal belang. De inlichtingendiensten verrichten belangrijk werk op het vlak van detectie en sensibilisering van de verschillende actoren rond de dreigingen gelinkt aan inmenging. In het kader van de Strategie Terrorisme Extremisme en Radicalisering (TER) volgt het OCAD met belangstelling de educatieve initiatieven van de deelstaten op het vlak van mediageletterdheid⁴³.
51. Volgens de heer Eric Kalajzic, directeur van het Studiecentrum voor Veiligheid en Defensie aan het Koninklijk Hoger Instituut voor defensie (KHID) moet er een strategie gevolgd worden waarin onder meer ingezet wordt op de ontwikkeling van een veiligheids- en inlichtingencultuur. Terwijl de Angelsaksische wereld zich meestal bewust is van de veiligheidsproblemen en van het nut van inlichtingen, stelt onze open, liberale samenleving zich echter weigerachtiger op tegenover verplichtingen uit veiligheidsoverwegingen. Meer nog, onze leiders weten vaak niet wat ze van hun inlichtingendiensten mogen eisen en verwachten.

Men moet dus opleidingscampagnes in de federale overheidsdiensten (FOD), de overheidsadministraties, de privéondernemingen en onder de burgers organiseren en herhalen, om tot een mentaliteitswijziging te kunnen komen. Ook de ministers en hun adviseurs moeten worden opgeleid. Op Europees niveau is er in alle geval de jongste jaren sprake van enige bewustwording, de hogervermelde commissie ING2 van het Europees Parlement en de totstandkoming van de «*hybrid toolbox*» van de EU ter bestrijding van informatiemanipulatie en buitenlandse inmenging zijn hier het bewijs van.
52. De heer Philippe de Koster, Voorzitter van de Cel voor Financiële Informatieverwerking (CFI), houdt een pleidooi voor een zo nauwkeurig mogelijke afbakening en definitie van het nationaal defensiebeleid en -strategie. Enkel de wetgever kan hiervan de regels vastleggen, de CFI is niet aan zet. Zo ging het ook in Frankrijk: in november 2022 kondigde president Macron de grote lijnen aan van de Franse nationale defensie-strategie. Kort samengevat betreft het de bescherming van de democratische verworvenheden en

43. De heer Gert Vercauteren, directeur a.i., Coördinatieorgaan voor de dreigingsanalyse (OCAD).

het voorkomen dat buitenlandse spelers invloed uitoefenen of zich inmengen. Het werkterrein van de inlichtingendiensten - en dus ook van de Franse tegenhanger van de CFI, de *Traitement du renseignement et action contre les circuits financiers clandestins* (Tracfin) - is daarmee duidelijk afgebakend. Op basis hiervan kan Tracfin bijvoorbeeld informatie opvragen over betalingsverkeer tussen België en Frankrijk wanneer het vermoeden bestaat dat de Belgische rekeningen in kwestie uitsluitend worden gebruikt om de Franse (economische) infrastructuur te destabiliseren.

53. Het uitgangspunt van de aanbevelingen die de heer Etienne Soula, *research analyst* aan de *Alliance for Securing Democracy*, wenst te formuleren, is het belang van een eensgezinde reactie van de democratische landen. België staat niet alleen: de heer Soula verwijst naar de hoger vermelde resolutie van het Europees Parlement van 9 maart 2022 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2020/2268(INI)), waaruit blijkt dat dit de hele EU aangaat. Alle partners van België worden immers rechtstreeks getroffen door gevallen van inmenging. Het gaat om een gemeenschappelijke uitdaging voor alle democratieën: de voorbeelden van inmenging komen overal vandaan en de omvang van het probleem overstijgt de grenzen van één land of zelfs één continent.
54. Op het gebied van inmenging zijn er specifieke uitdagingen op het niveau van de federale gerechtelijke politie (FGP). De FGP is namelijk een potentieel doelwit voor inmenging, omdat ze als onderzoeksdienst bevoegd is om bepaalde onderzoeken naar corruptie uit te voeren en daarnaast belast is met het verlenen van de nodige bescherming als politietaak. Hierdoor kan ze in het bezit zijn van gevoelige informatie die relevant kan zijn voor buitenlandse - zowel private als publieke - actoren⁴⁴.

2) «Strategische» actoren die als toegangskanaal voor inmenging kunnen dienen

55. Er wordt niet alleen vertrouwd op de traditionele kanalen van beleidsvorming, maar er wordt tevens gebruik gemaakt van denktanks die innovatieve ideeën en benaderingen ontwikkelen. Daarnaast wordt er invloed uitgeoefend via activistische groeperingen, soms via «nuttige idioten» die onbewust bepaalde politieke agenda's bevorderen. Het valt echter op dat critici van deze benaderingen vaak geconfronteerd worden met intimidatie en tegenmaatregelen, wat de vrije uitwisseling van ideeën en open debat kan belemmeren⁴⁵.
56. Beïnvloedingsoperaties via sociale media mikken vaak op (politieke) kwesties die haat zaaien en shockeren omdat dergelijke kwesties makkelijker gedeeld worden op sociale media. De uitdaging bestaat erin om te weten hoe er mee om te gaan als ze worden ingezet om te pleiten voor een bepaalde zaak of om de discussie aan te zwengelen in verkiezingstijden⁴⁶.
57. Met de komst van de *large language models* (LLM's), is het perfect mogelijk dat we in de nabije toekomst worden overspoeld met desinformatie afkomstig van allerlei chatbots⁴⁷.
58. De heer Raphaël Glucksmann, voorzitter van de bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie met inbegrip van desinformatie en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), stond stil bij de praktijken van *TikTok*. Volgens hem moet *TikTok* aantonen dat het niet toestaat dat onze gegevens worden gebruikt ten behoeve van de Chinese Communistische Partij. Dit is nodig omdat *TikTok* nu eenmaal geen privébedrijf is als een ander. In China is er namelijk een nationale veiligheidswet

44. De heer Eric Snoeck, directeur-generaal federale gerechtelijke politie, Centrale Dienst voor de bestrijding van de corruptie (CDBC).

45. De heer Kenneth Lasoen, lector *intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

46. Mevrouw Sofia Collignon, *lecturer (assistant professor)*, School of politics and IR, Queen Mary University of London.

47. De heer Guy De Pauw, CEO en medeoprichter, *Textgain*.

van kracht die grote Chinese groepen of bedrijven verplicht - ook als ze in de privésector actief zijn - om zich onder het gezag te scharen van de Chinese Communistische Partij en alle voor-de-Chinese-nationale-veiligheid-interessante informatie door te spelen. Dat vormt een enorm probleem. De heer Glucksmann wil evenwel niet gezegd hebben dat *TikTok* volledig verboden moet worden, maar wel dat het veeleer dient te bewijzen dat het de gegevens in kwestie niet aan de Chinese nationale veiligheidsdiensten doorgeeft.

3) «Aanvallers»

59. De «agressor» poogt om de *situational awareness* van het doelwit te verstoren. Er wordt druk uitgeoefend op het doelwit om een gunstige uitkomst voor de agressor te bewerkstelligen. Men poogt om de perceptie van het doelwit te manipuleren, zodanig dat het doelwit besluiten neemt in het voordeel van de initiator (dat wil zeggen de agressor) van de inmengingsoperatie⁴⁸.

60. Buitenlandse inmenging is niet langer uitsluitend het werk van Staten die al dan niet slechte bedoelingen hebben, maar soms ook, en in de toekomst waarschijnlijk vaker, van niet-gouvernementele actoren: misdaad- en maffiaorganisaties, grote economische en financiële groepen, en andere groeperingen. Die ontwikkeling vergt een aanpassing van de middelen en strategieën ter bestrijding van inmenging en ongetwijfeld ook van de wetgeving.

Het wordt nog ingewikkelder wanneer men ziet dat sommige niet-gouvernementele actoren als onderaannemers optreden van mogelijkheden die zelf niet op het voorplan treden. Het is bijna de regel geworden in cyberspace dat offensieve inmengingsoperaties worden toevertrouwd aan private actoren, die tegen een vergoeding de acties uitvoeren van de aanbestedende mogelijkheid⁴⁹.

61. De term «agressor» kan doelbewust gebruikt worden in deze context, zeker wanneer de agressie uitgaat van autocratische regimes. In dat laatste geval gaat het namelijk om agressie waarin er een vorm van oorlog wordt uitgevochten tussen de open democratische maatschappij en autocratische regimes, gericht tegen onze waarden, onze manier van leven en onze manier van aan politiek doen⁵⁰.

62. Tijdens de hoorzittingen werd de *modus operandi* toegelicht van het Spaans bedrijf Eliminalia. Die zit als volgt in elkaar: een klant vraagt bijvoorbeeld om een ongunstig artikel van het internet te verwijderen. Het team van *Eliminalia* copy-pastet het geviseerde artikel op het platform van een *fakenews*-leverancier waarbij de publicatiedatum wordt geantidateerd waardoor het er op lijkt dat het gekopieerde artikel al eerder verscheen. *Eliminalia* ontkracht vervolgens het oorspronkelijk artikel op grond van plagiaat en verzoekt de internetzoekmachines dan ook om het oorspronkelijke artikel uit de zoekbestanden te verwijderen. Dergelijke - eenvoudige - interventie leverde resultaten op in tal van gevallen. De wetgeving wordt hier dus misbruikt om informatie met een *public interest* gehalte *offline* te kunnen halen⁵¹.

63. Er werd in de hoorzittingen ook verwezen naar het *Pegasus*-project (hoger vermeld) waarin een journalistencollectief onthulde dat journalisten en mensenrechtenactivisten wereldwijd het slachtoffer waren geworden van de *Pegasus-spyware*, ontwikkeld door de Israëlische *NSO Group*. Ook in België waren er slachtoffers. De software in kwestie liet toe om vanop afstand de software van smartphones volledig over te nemen en te controleren⁵².

48. De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

49. De heer Michel Liégeois, professor, *Institut de sciences politiques Louvain-Europe (ISPOLE)*, UCLouvain.

50. De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

51. De heer Kristof Clerix, onderzoeksjournalist, Knack.

52. De heer Kristof Clerix, onderzoeksjournalist, Knack.

C. Geïdentificeerde gevallen van inmenging

64. Tijdens de hoorzittingen werden een aantal landen vernoemd als bronnen van inmenging: Turkije, Qatar (met name sinds *Qatargate* dat het Europees Parlement aanzette tot het uitvaardigen van hogervermelde resolutie 2023/2034(INI)), Marokko (*Marocgate* in verband met de Westelijke Sahara), Congo, Rwanda⁵³.

China en Rusland kwamen ook uitvoerig aan bod.

Daarnaast werden ook de Verenigde Staten geciteerd, wat aantoont dat inmenging dus ook van westerse landen kan komen.

65. Om een strategisch gunstige voedingsbodem te garanderen voor haar invloedssfeer, richt China zich bijvoorbeeld op het «winnen van harten en geesten», niet alleen onder de Europese elite, maar ook onder de lokale bevolking. Het probeert om politici, zowel op regerings- als op oppositieniveau, zowel op nationaal als Europees niveau te beïnvloeden. Het richt zich op lokale politici - via «subnationale diplomatie» - en coöpteert opiniemakers, journalisten en leden van denktanks. China investeerde voorts in Europese media en probeert om via digitale mediaplatforms - *Facebook*, *Twitter*, *TikTok*, enz. - specifieke narratieven tot stand te brengen. Ze heeft onderzoekscentra en instellingen voor hoger onderwijs in Europa benaderd met het oog op een mogelijke transfer van belangrijke en nieuwe technologieën bevorderlijk voor het militair potentieel⁵⁴.
66. Het conflict met Oekraïne heeft de aandacht acuut gevestigd op de doctrine van de «hybride oorlogsvoering» aangestuurd vanuit Rusland. Het gaat hier om niet-militaire wapens die moeten helpen om een potentiële vijand te destabiliseren, om verdeeldheid te zaaien of om bepaalde kritieke en gevoelige sectoren van de tegenstander lam te leggen. Een belangrijke component van deze hybride oorlogsvoering is de strategie van beïnvloeding en manipulatie. Rusland voert al sinds jaren complexe *Information Operations* (IO)-campagnes om de publieke opinie te beïnvloeden en de westerse politieke en maatschappelijke consensus te ondergraven⁵⁵.
67. De *European External Action Service* (EEAS) runt het project *EUvsDisinfo*, dat zich in het bijzonder richt op Russische desinformatie. Het zoomt in op de gebruikte narratieven, probeert feiten te onthullen en het bewustzijn daaromtrent te verhogen⁵⁶.

D. Getroffen maatregelen

1) Op nationaal niveau

68. Volgens de heer Luca Ferro, *assistant professor* internationaal recht aan de Vrije Universiteit Brussel, zijn veel van de juridische criteria gerelateerd aan buitenlandse inmenging vaag en niet volledig uitgekristalliseerd. Ieder soeverein land, inclusief België, kan expliciet positie innemen: het is volgens de heer Luca Ferro dan ook nuttig dat België dat doet. Hij verwijst naar het Belgisch initiatief - pionier in zijn soort - met betrekking tot het opnemen van het misdrijf van ecocide in het vernieuwde Strafwetboek. Hiermee geeft België vorm aan de interpretatie van het internationaal recht. Op vergelijkbare wijze moet dit ook gebeuren voor het fenomeen van buitenlandse inmenging.

Een ander voorbeeld op dat vlak is de casus van de toepassing van het internationaal recht in *cyberspace*, bron voor heel wat discussiemateriaal onder rechtsgeleerden.

53. De heer Kristof Clerix, onderzoeksjournalist, Knack.

54. Mevrouw Ivana Karásková, *European China Policy Fellow*, Mercator Institute for China Studies.

55. De heer Gert Vercauteren, directeur a.i., OCAD.

56. De heer Lutz Güllner, *Head of Strategic Communications*, EEAS.

Hier heeft België nog geen positie ingenomen; Frankrijk, Nederland, Duitsland en Italië daarentegen wel. Volgens de heer Luca Ferro kan België ook op dat vlak het internationaal kader mee vorm geven en een concrete bijdrage leveren aan het debat.

69. Tijdens de verkiezingen van 2019 hebben de VSSE en de ADIV de partijvoorzitters geïnformeerd over de risico's van inmenging in het verkiezingsproces. Ook voor de nakende verkiezingen wil de VSSE hier op inzetten⁵⁷.

Voor de verkiezingen van 2019 stelde de VSSE in samenwerking met de ADIV en het Centrum voor cybersecurity België (CCB) een specifieke brochure op («Veilig online tijdens de verkiezingscampagne»). Er werd toen trouwens ook een *Joint Intelligence Task Force* (JITF) opgericht om na te gaan of er al dan niet sprake was van inmenging.

70. Het Vast Comité I besloot begin 2019 om een onderzoek te voeren naar de manier waarop de Belgische inlichtingendiensten reageerden (inwinnen van informatie, waarschuwingen, internationale samenwerking, mogelijke belemmeringen, enz.) op mogelijke inmenging van buitenlandse diensten of landen in de Belgische verkiezingen⁵⁸. Het besluit was dat er geen grote structurele onregelmatigheden waren vastgesteld, alleen enkele minder belangrijke individuele gevallen van beïnvloeding en/of inmenging in het verkiezingsproces.
71. Volgens de heer Tanguy Struye de Swielande, professor aan het *Institut de sciences politiques Louvain-Europe* (ISPOLE) van de *UCLouvain*, beschikken we enerzijds over een nationale veiligheidsstrategie. Anderzijds weet niemand wat die strategie werkelijk inhoudt en stuurt niemand ze aan. Ze bevat heel waardevolle concepten zoals de behoefte aan veerkracht - die van het grootste belang is bij inmenging - en het idee van een *whole society approach* om inmenging te bestrijden. Het probleem is echter dat de aanpak te gefragmenteerd is: er is absoluut geen samenhang of samenwerking met betrekking tot de uitvoering van het plan.
72. In Nederland werden er een aantal initiatieven genomen, onder meer de wetswijziging die diasporaspionage verbiedt en de oprichting van een meldpunt waar leden van diasporagemeenschappen die zich geïntimideerd voelen dit kenbaar kunnen maken. Deze initiatieven laten zien dat de Nederlandse overheid inmenging in diasporagemeenschappen uitermate serieus neemt en probeert om er iets aan te doen. Ze hebben ook een symbolische waarde omdat het handelingsperspectief soms beperkt lijkt⁵⁹.
73. Een ander initiatief dat Nederland al geruime tijd neemt, is het bevorderen van nauw contact tussen bepaalde ministeries en de grotere migrantengemeenschappen. Op die manier kan de overheid in de mate van het mogelijke de vinger aan de pols houden van wat er binnen de gemeenschappen speelt, en detecteren welke delen van de gemeenschappen te maken hebben met intimidatie. Dit kan mogelijk steun en bescherming bieden⁶⁰.
74. Het Verenigd Koninkrijk erkent dat inmenging een belangrijk probleem is en verschillende voorstellen tot aanpassing van de wetgeving werden of worden er besproken:
- er werd een amendement ingediend om de *National Security Bill* te koppelen aan de *Online Safety Bill*; het *Foreign Influence Registration Scheme* (FIRS) werd opgenomen in de *National Security Bill*;

57. De heer Peter Lanssens, directeur van de Analyse, VSSE.

58. Vast Comité I: Activiteitenverslag 2020, blz. 22 e.v.

59. De heer Christopher Houtkamp, *senior research fellow - head Connected Security programme, Clingendael - the Netherlands Institute of International Relations*.

60. De heer Christopher Houtkamp, *senior research fellow - head Connected Security programme, Clingendael - the Netherlands Institute of International Relations*.

- het strafbaar feit van buitenlandse inmenging (*Foreign Interference Offence*) werd toegevoegd aan de lijst van prioritaire misdrijven in de *Online Safety Bill*;
- de strafbaarstelling van buitenlandse inmenging is vastgelegd met inbegrip van de aan-de-staat-gelinkte desinformatie (*state-linked disinformation*);
- wordt strafbaar gesteld: de gedraging waarbij voor, namens of met de bedoeling een buitenlandse mogendheid te bevoordelen, inbreuk wordt gemaakt op de rechten van het Verenigd Koninkrijk; de gedraging die de democratische instellingen in diskrediet brengt, die de deelname van de burgers aan de instellingen manipuleert en die de veiligheid van de belangen van het Verenigd Koninkrijk ondermijnt;
- het strafbare feit omvat de gedraging waarbij een valse of misleidende voorstelling van de zaken wordt gegeven, met inbegrip van het gebruik van informatie die juist is maar op een misleidende manier wordt gepresenteerd of waarbij de identiteit van een persoon verkeerd wordt voorgesteld⁶¹.

2) Op Europees niveau

75. De Europese Unie heeft een aantal aanbevelingen geformuleerd en procedures voorgesteld.

Er zijn onder meer:

- de resolutie van het Europees Parlement van 13 juli 2023 over aanbevelingen voor de hervorming van de regels van het Europees Parlement inzake transparantie, integriteit, verantwoordingsplicht en corruptiebestrijding (2023/2034(INI));
- de resolutie van het Europees Parlement van 1 juni 2023 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2022/2075(INI));
- de *cybersecurity*-strategie en de richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van verordening (EU) nr. 910/2014 en richtlijn (EU) 2018/1972 en tot intrekking van richtlijn (EU) 2016/1148 (NIS2-richtlijn);
- het «strategisch kompas voor veiligheid en defensie» (Raad van de Europese Unie, 21 maart 2022, 7371/22);
- de resolutie van het Europees Parlement van 10 oktober 2019 over buitenlandse inmenging in verkiezingen en desinformatie in de nationale en Europese democratische processen (2019/2810(RSP));
- de *East Stratcom Task Force* van de Europese Dienst voor extern optreden (EEAS);
- het gezamenlijk kader voor de bestrijding van hybride bedreigingen (JOIN(2016) 18 final);
- de EU *Cyber Diplomacy Toolbox* (CDT);
- de EU-regels ter versterking van de democratie (onder andere integriteit van de verkiezingen, transparantie en gerichte politieke reclame, partijfinanciering, kiesrechten).

76. Er is ook het *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE), een autonome, netwerkgebaseerde internationale organisatie voor de bestrijding van hybride bedreigingen.

61. Mevrouw Sofia Collignon, *lecturer (assistant professor)*, School of politics and IR, Queen Mary University of London.

77. Er is duidelijk een wil om de transparantie te moderniseren en operationeel te maken door lobbyregisters aan te maken, en door de melding van contacten tussen verkozen vertegenwoordigers en verschillende drukkingsgroepen verplicht te maken en beter te controleren. In dit verband moet worden opgemerkt dat het transparantieregister vereist dat elke structuur, met inbegrip van niet gouvernementele organisaties (ngo) die financiering ontvangt - en die dus geen commerciële entiteit is - al haar financieringsbronnen moet vermelden⁶².
78. Ook de aandacht voor de veiligheidsaspecten van nieuwe Europese regelgeving is van groot belang:
- de recente digitaledienstenverordening (hoger vermeld) legt bijvoorbeeld verplichtingen op inzake de transparantie van algoritmes waarop sociale media berusten en de nood aan mechanismen om manifest schadelijke content te rapporteren. De hamvraag is of deze nieuwe regelgeving al te ver of net niet ver genoeg gaat;
 - een ander voorbeeld betreft de nieuwe NIS2-richtlijn (hogervermeld) met betrekking tot *cybersecurity* van netwerken en informatiesystemen en het voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van verordening (EU) 2019/1020 (COM(2022)454 final, de zogenaamde *Cyber Resilience Act*). De inzet voor de interne markt is het minimaliseren van de dreiging van buitenlandse inmenging, terwijl tegelijkertijd wordt vastgehouden aan open standaarden en competitieve marktwerking⁶³.

3) Evaluatie en limieten van de genomen maatregelen

79. Door de aanzienlijke toename van de middelen voor de inlichtingendiensten en de geleidelijke afname van de terroristische dreiging zijn in de afgelopen jaren de benodigde middelen vrijgemaakt om inmenging te bestrijden. Bovendien is de coördinatie tussen de civiele en de militaire tak van de inlichtingendiensten verbeterd. Vanuit dit oogpunt is de situatie over het algemeen bevredigend, met name in vergelijking met zo'n vijftien jaar geleden⁶⁴.
80. De toewijzing van (cyber)aanvallen is moeilijk: het toewijzen van een individuele gebeurtenis is relatief eenvoudig, maar wanneer items organisch worden gedeeld, wordt het zeer moeilijk om ze te traceren. In het beste geval is het misschien mogelijk om de oorsprong van dit soort desinformatie te achterhalen, maar hoe ga je om met de organische verspreiding ervan⁶⁵?
81. Inmengingsoperaties werken op het cognitief niveau en zijn niet onmiddellijk gelijk te stellen aan dwanghandelingen. Net omdat ze zich op het cognitief niveau afspelen, is het ook moeilijk om de doeltreffendheid ervan direct te beoordelen⁶⁶.

62. De heer Raphaël Kergueno, *senior policy officer*, Transparency International EU.

63. Prof. dr. Alexander Mattelaer, *vice dean research*, Brussels School of Governance, Vrije Universiteit Brussel.

64. De heer Michel Liégeois, *professor*, Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain.

65. Mevrouw Sofia Collignon, *lecturer (assistant professor)*, School of politics and IR, Queen Mary University of London.

66. Mevrouw Sofia Collignon, *lecturer (assistant professor)*, School of politics and IR, Queen Mary University of London.



AANBEVELINGEN

I. WAARSCHUWINGS- EN RISICOBEPERKINGSSTRATEGIEËN ONTWIKKELEN EN IMPLEMENTEREN

A. Voorlichting/bewustmaking

1. Om zich tegen inmenging te beschermen, is het nodig dat men blijft inzetten op bewustmaking rond de risico's van inmenging op alle niveaus van elke organisatie. Een cruciale stap hierbij is het ontwikkelen door alle leden van de organisatie, ongeacht hun functie, niveau of graad, van «situationeel bewustzijn»: daarbij moet worden onderzocht wie manipuleert, met welke methoden en via welke actoren, alsook hoe dit fenomeen en zijn impact gemeten kunnen worden.

2. Voor de bescherming van onze democratische systemen tegen inmenging is zowel een gespecialiseerd optreden van performante inlichtingen- en veiligheidsdiensten nodig als een leerproces rond de cultuur van risico's op inmenging en de bescherming die georganiseerd moet worden.

3. In plaats van te vertrouwen op het controleren van feiten (*factchecking*) of het ophelderen ervan (*debunking*) alleen, is het nodig om in te zetten op een bredere mentaliteitswijziging. De aanpak moet zich ook richten op het bevorderen van kritisch denken, mediageletterdheid en weerbaarheid tegen desinformatie waarbij een belangrijke rol voor het onderwijs is weggelegd, als een effectieve manier om inmengingscampagnes te counteren.

4. De maatschappelijke weerbaarheid tegen inmenging stoelt op het eigen gedrag. Men kan hierbij denken aan meerdere groepen personen of instellingen.

a) Men kan in het bijzonder denken aan politieke mandatarissen en openbare ambten. Transparantie aan de dag leggen omtrent financiële belangen, het openbaar maken van eventuele belangenconflicten, deontologische codes en transparantieregisters dragen allemaal bij tot die verhoogde weerbaarheid.

b) In het licht van het belang van kennisveiligheid, is het belangrijk initiatieven op te starten om de universiteiten te beschermen tegen inmenging.

c) Het is belangrijk om bewustmakingscampagnes op te zetten gericht op journalisten, mensenrechtenactivisten en andere potentiële doelwitten van *spyware*-aanvallen.

Deze campagnes hebben tot doel hen te informeren over de risico's van digitale spionage en hen praktische tips aan te reiken om hun online veiligheid te vergroten, zoals het gebruik van *end-to-end* encryptie, het regelmatig updaten van *software* en het vermijden van verdachte links en bijlagen.

d) Opleidingscampagnes moeten regelmatig plaatsvinden binnen overheidsinstanties, privébedrijven en ook bij burgers om een mentaliteitsverandering te bewerkstelligen. Hieronder vallen ook ministers en adviseurs.

e) Er is nood aan educatieve programma's in de scholen, die zich richten op het omgaan met informatie en het ontwikkelen van een kritische geest, speciaal gericht op jongeren, aangezien zij een belangrijke doelgroep zijn van de socialenetwerk-platforms.

5. Het is nodig om concrete stappen, zoals frequente veiligheidsbriefings tijdens interacties met buitenlandse partners, systematisch te implementeren, om verbeteringen te bevorderen.

6. Hiervoor moet de communicatie tussen de Veiligheid van de Staat (VSSE) en de academische, wetenschappelijke en politieke actoren worden versterkt.

a) Wat betreft de academische en onderzoekssectoren, moeten de *Académie de recherche et d'enseignement supérieur* (ARES) en de Vlaamse Interuniversitaire Raad (VLIR) evenals de instellingen voor onderzoek en voor het hoger onderwijs, de volgende maatregelen operationeel maken:

- de versterking van de *cybersecurity* binnen de instellingen ondersteunen;
- een adviesbureau op federaal niveau oprichten dat de informatie van de verschillende overheidsdiensten kan samenbrengen om universiteiten te adviseren over de risico's van bepaalde samenwerkingsverbanden.

b) Wat de politieke mandatarissen betreft, zou de VSSE aan het begin van elke zittingsperiode een briefing moeten organiseren om hen bewust te maken van de mogelijke gevaren voor de veiligheid en de risico's van inmenging, zoals ook werd voorgesteld voor de Europese parlementsleden, en dat op alle bevoegdheidsniveaus (met inbegrip van het lokale niveau).

B. Communicatie

7. Wij bevelen aan dat overheden en socialemediabedrijven samenwerken om educatieve programma's op te zetten die mensen helpen kritischer te zijn ten opzichte van de veelheid aan informatie en om de bronnen te verifiëren voordat ze deze delen.

8. Vooral tijdens verkiezingstijden, dient er een gedragscode te worden ingevoerd voor politieke partijen en kandidaten.

9. Men zou kunnen overwegen om de bijdrage van burgers aan het identificeren van risico's op interferentie te organiseren, vergelijkbaar met het systeem van burgermeldingen via het e-mailadres «verdacht@safeonweb.be».

10. Wij bevelen aan om, naar het voorbeeld van wat in Nederland werd gedaan, in België een contactpunt op te richten tussen specifieke overheidsdiensten en de verenigingen van de diaspora. Dergelijk contactpunt kan bewustmakingsprogramma's en programma's voor media- en informatiegeletterdheid op maat ontwikkelen voor diasporagemeenschappen en minderheden in ons land om hen weerbaarder te maken. Dit zal de overheid in staat stellen om goed geïnformeerd te blijven over de situatie binnen deze gemeenschappen, en om intimidatie, bedreigingen en inmenging effectiever te detecteren en aan te pakken. Dit initiatief dient als een bron van steun en bescherming voor de betrokken gemeenschappen.

11. Om de impact van externe beïnvloeding tegen te gaan, moet de overheid op de bestaande platforms bijdragen aan de transparantie en het vertrouwen door dialoog, debat en discussie met burgers aan te moedigen.

12. Als het erom gaat buitenlandse inmenging aan het licht te brengen, kunnen de pers en de informatieve media waardevolle bondgenoten zijn in hun rol van klokkenluiders, op voorwaarde dat ze de aansprakelijkheidsclausules naleven.

C. Onderzoek

13. Bij organische verspreiding van desinformatie-items moet men in de eerste plaats altijd de oorsprong zien te achterhalen. Het traceren van het spoor naar de eigenlijke bron is erg belangrijk, des te meer als later blijkt dat ze afkomstig zijn van buitenlandse staatsactoren.

Wij bevelen aan dat hierbij middelen worden uitgetrokken voor extra studies betreffende de detectie, analyse en weerbaarheid om het fenomeen nog beter in kaart te brengen. Deze middelen moeten zowel aan de betrokken veiligheidsdiensten als aan de universiteiten worden toegekend.

Om beter beschermd te zijn tegen potentiële bedreigingen is een tweeledige aanpak vereist. Allereerst moeten technologische investeringen plaatsvinden voor verbeterde veiligheid. Daarnaast is een cultuuromslag nodig waarbij België zich bewust wordt van zijn kwetsbaarheid.

In dit opzicht moeten we in de eerste plaats de hiaten dichten en de bestaande lacunes in de huidige wetgeving over lobbying aanpakken. We moeten eveneens de administratieve en maatschappelijke kwetsbaarheden, de nationale initiatieven en tegenmaatregelen, de motieven en doelstellingen van de agressors, en de effecten van algoritmes analyseren.

14. Het inzetten op de continue ontwikkeling van detectietechnieken van teksten die door *bots* geschreven werden en van door artificiële intelligentie gegenereerde beelden, is essentieel. Wij bevelen aan dat de federale overheid hier in overleg met de Gewesten permanent middelen en mensen op inzet.

15. Het doelgericht onderzoeken van potentiële actoren op het gebied van inmenging, of het nu gaat om landen waarvan al vastgesteld is dat er sprake is van inmenging (Rusland, China, Turkije, Qatar, Marokko, Israël), bedrijven (*TikTok*) of diasporagemeenschappen, is van groot belang. Het helpt de overheid bij het verkrijgen van een dieper inzicht in hun kennis en mogelijke handelingsmogelijkheden.

16. Er moet een onderzoek komen naar het ontwikkelen van eventuele duidelijke richtlijnen en criteria om onderscheid te maken tussen binnenlandse actoren die bewust handelen in lijn met buitenlandse belangen en diegenen die simpelweg hun affiniteit uiten. Dit kan onder andere worden bereikt door een nauwe samenwerking tussen nationale veiligheidsinstanties en inlichtingendiensten om te bepalen of er sprake is van een daadwerkelijke intentie om buitenlandse belangen te dienen.

D. Repressieve maatregelen

17. Het verder ontwikkelen van onze nationale cybercapaciteit vormt een belangrijk aandachtspunt. Wij bevelen aan om de bestaande investeringen verder op te drijven. Daarnaast moet men ook de samenwerking met partnerlanden versterken om cybergerelateerde opleidingen te voorzien en expertise uit te wisselen.

18. Om de impact van buitenlandse informatieoperaties te beperken, moet een vergelijkbaar initiatief als dat van de Europese Unie (EU) gevolgd worden om specifieke buitenlandse propagandakanalen te weren. Dit perkt hun bereik en invloed in.

19. Op microniveau bestaat een effectieve aanpak van buitenlandse inmenging via internet uit het systematisch identificeren, analyseren en proactief aanpakken van dergelijke uitingen. Dit omvat: het verwijderen van misleidende content, het ontkrachten van valse informatie en het proactief communiceren van feitelijke informatie over het belang van democratie en mensenrechten om de verspreiding van inmenging te verminderen.

II. TRANSPARANTIE

A. Sociale media

20. Wij raden aan dat een mechanisme op Europees niveau ontwikkeld wordt met betrekking tot een striktere regelgeving en transparantie-eisen voor *online content*, die gerelateerd is aan politieke kwesties. Dit houdt in dat platforms socialemedia-accounts en advertenties moeten identificeren die betrokken zijn bij beïnvloedingsoperaties.

B. Politici

21. Een wachtlijd bij het aanwerven van politici, topambtenaren en andere leidinggevenden door buitenlandse (overheids)bedrijven, gecombineerd met strengere transparantieregels en de openbaarmaking van deze samenwerkingsverbanden vormt een effectieve maatregel om te voorkomen dat politieke, economische en culturele elites worden beïnvloed door buitenlandse belangen.

22. Inmenging gedijt in de schemerzone, daarom moet de schemerzone beperkt worden. Hiertoe moeten zo snel mogelijk heldere deontologische richtlijnen worden uitgewerkt inzake vergoedingen, reizen, etentjes, cadeaus, enz. Om te voorkomen dat misbruik wordt gemaakt van deze schemerzones, is het belangrijk om te beschikken over duidelijke, strikte richtlijnen en een gedragscode die afdwingbaar moet zijn en waarbij sancties voorzien worden. Daartoe moeten in elk parlement deontologische codes worden opgesteld. Die regels omvatten onder meer een meldingsplicht voor buitenlandse contacten alsook een register waarin relatiegeschenken en zelfs gratis reizen worden genoteerd.

De assemblees en instanties van het land moeten deze regels ook zoveel mogelijk op elkaar afstemmen, met eerbiediging van de autonomie van de parlementen.

Wij bevelen binnen dit kader aan om een transparantieregister op te zetten zoals ook de EU er één heeft. Het betreft een databank waarin alle organisaties vermeld worden

die zich bezighouden met het (trachten te) beïnvloeden van de wetgevende en politieke activiteiten van de EU. Wie benaderd wordt door een derde partij, kan steeds in dit register nagaan of het hier om een legitieme organisatie gaat en wat haar oogmerk is. Dit kan helpen om het voor iedereen duidelijk te maken wie er achter een bepaalde lobbyactie zit.

23. Er moet een strikt kader worden opgesteld voor buitenlandse investeringen, gericht op bedrijfsleiders, vooral wanneer de overname van kritieke of strategische infrastructuur in het geding is.

Het is nodig om de regels en procedures die van toepassing zijn op buitenlandse overnames te verduidelijken en te investeren in een systeem voor het screenen van buitenlandse investeringen dat gevoelige strategische sectoren in kaart brengt, potentiële risico's beoordeelt en overnames onderzoekt op basis van een inschatting van de bedreiging voor de nationale veiligheid.

24. De kwetsbare technologieën moeten worden opgespoord en de bescherming ervan moet worden aangescherpt, zonder daarbij de internationale samenwerking op het gebied van onderzoek en ontwikkeling te ondermijnen.

25. De transparantie van de partijfinanciering en mediacampagnes naar aanleiding van verkiezingen vormen een belangrijk werkpunt. Een cruciale stap om dit probleem aan te pakken is het verbeteren van de openheid rondom partijfinanciering en mediabeleid tijdens verkiezingen. Hierbij moet speciale aandacht worden besteed aan het versterken van de regelgeving op dit gebied.

C. Ngo's, lobbyisten, enz.

26. Er moet een wetgeving worden uitgewerkt die buitenlandse financiering van politieke campagnes beperkt of transparantieverplichtingen oplegt aan lobbyisten, zonder echter zo ver te gaan als de *Foreign Agents Registration Act* in de Verenigde Staten. De nationale regelgever heeft de vrijheid om strengere wetten in te voeren dan internationale normen vereisen. Dit stelt België, eventueel in EU-verband, in staat om een robuuster juridisch kader te creëren voor bescherming tegen externe inmenging.

27. We zien steeds meer betrokkenheid van niet-gouvernementele actoren, zoals criminele en maffiaorganisaties, grote economische en financiële entiteiten, en andere groepen. Deze trend vereist een herziening van onze benaderingen en tactieken om dergelijke inmenging te bestrijden, en een aanpassing van de wetgeving om deze fenomenen te bestrijden.

28. Het is van essentieel belang dat de overheid aandringt op verbeterde transparantie met betrekking tot de financiering van niet-gouvernementele organisaties (ngo), verenigingen zonder winstoogmerk (vzw) en andere organisaties. Dit kan worden bereikt door wettelijke vereisten voor gedetailleerde openbaarmaking van financieringsbronnen en -bedragen in jaarverslagen en andere relevante documenten. Dit alles zal gebeuren in overeenstemming met de rechtspraak van het Europees Hof voor de Rechten van de Mens en de adviezen van de Commissie van Venetië. Het waarborgen van deze transparantie zal het vertrouwen in deze organisaties vergroten en mogelijke schimmige praktijken aan het licht brengen.

29. De buitenlandse financiering en vertegenwoordiging inzake *lobbying* moeten transparanter worden. Het is noodzakelijk dat er wetgevende maatregelen op Europees niveau worden genomen om dit te bereiken. Naast de implementatie van controles moeten er concrete stappen worden genomen om het fenomeen grondig te begrijpen en te analyseren.

III. JURIDISCHE ACTIES

A. Nationaal

30. Er moet op korte termijn in samenwerking met de academische wereld worden onderzocht hoe men «*hostile copyright claims*» kan stoppen. Er zou een snelle herzieningsprocedure moeten komen voor onterechte aantijgingen van plagiaat, om te voorkomen dat legitieme informatie van maatschappelijk belang ten onrechte *offline* wordt gehaald. Dat moet op Europees vlak gebeuren, aangezien de auteursrechten geregeld worden in een Europese richtlijn.

31. Om effectief om te gaan met de uitdaging van buitenlandse inlichtingenoperaties, bevelen wij aan dat de relevante diensten een duidelijk mandaat ontvangen om deze missie uit te voeren. Daarnaast moeten zij worden uitgerust met de benodigde juridische bevoegdheden om strenger en doortastender op te treden.

32. We bevelen aan om het proces van een «inlichtingendossier» naar een «gerechtelijk dossier» te stroomlijnen, zodat zodra er voldoende bewijs van een misdrijf is, er een naadloze overgang plaatsvindt. Dit vergroot de effectiviteit omdat de informatie soepeler wordt doorgegeven aan het parket, wat snellere en doeltreffendere maatregelen mogelijk maakt.

33. Nagaan of de nieuwe regelgeving inzake inmenging en beïnvloeding voldoende waarborgen biedt om een doeltreffende aanpak en sanctionering te waarborgen.

B. Internationaal

34. We bevelen aan om een breed scala aan benaderingen te hanteren bij het aanpakken van de kwestie van buitenlandse inmenging, aangezien deze kwestie invloed heeft op alle aspecten van onze samenleving. In dit opzicht is de definitie die wordt gebruikt door zowel de EU als de Noord-Atlantische Verdragsorganisatie (NAVO) richtinggevend.

35. In gevallen van flagrante inmenging door partnerlanden zal de overheid eerst en vooral discretie hoog in het vaandel dragen. Dit betekent dat de kwestie met de nodige omzichtigheid wordt behandeld, waarbij media-aandacht wordt vermeden.

36. Het concentreren op disruptie enerzijds en regulering anderzijds is essentieel voor het effectief aanpakken van buitenlandse inmenging. Dit omvat het identificeren van methoden om specifieke situaties te beëindigen, wat vaak een complexe uitdaging is, en dit niet alleen op juridisch vlak. Verschillende middelen kunnen worden benut in het digitale domein, inclusief de Europese wet betreffende digitale diensten, waarin transparantie en verantwoordingsplicht als centrale principes gelden.

37. Wij bevelen aan dat België op korte termijn een grondig onderzoek start om een helder standpunt in te nemen over de toepassing van internationaal recht in *cyberspace*. Dit initiatief werd reeds genomen door landen zoals Frankrijk, Nederland, Duitsland en Italië, die reeds hun positie hebben bepaald. Actieve deelname aan dit debat zou België niet alleen in staat stellen om het internationale kader mede vorm te geven, maar ook om waardevolle inzichten te leveren.

38. De recent aangenomen digitaledienstenverordening (*Digital Services Act* - DSA) verplicht transparantie van algoritmes op sociale media en het melden van schadelijke content. Er moet echter snel beoordeeld worden of deze regelgeving relevant is.

39. Voor een goed algoritmisch bestuur moet een democratisch aanvaardbaar kader worden gecreëerd. Door hierbij niet alleen politici, verantwoordelijken voor de veiligheidsstrategie, te betrekken, maar ook burgers, schept men de voorwaarden voor een goede werking ervan.

40. Een vergelijkbare situatie doet zich voor in verband met de nieuwe NIS2-richtlijn en het voorstel voor een verordening inzake cyberveerkracht (*Cyber Resilience Act*). In dit verband bevelen wij aan om een evenwicht te vinden tussen het tegengaan van buitenlandse inmenging en het behoud van open standaarden en een competitieve marktwerking, terwijl de interne markt wordt ondersteund.

IV. DE BELANGRIJKSTE ACTOREN IN DE STRIJD TEGEN INMENGING ONDERSTEUNEN

A. Nationaal

41. Analoot aan het Franse voorbeeld is het van groot belang om het werkterrein van de inlichtingendiensten (en dus ook de Cel voor financiële informatieverwerking (CFI)) zo nauwkeurig mogelijk af te bakenen en grondig te definiëren.

42. Het efficiënter opsporen van inmenging vergt bijkomende versterking van ons inlichtingenapparaat, zowel inzake personeelssterkte als inzake werkmiddelen.

43. Wij bevelen aan om de organisatorische uitdagingen aan te pakken door een grondige evaluatie uit te voeren van de specifieke behoeften voor het bestrijden van nieuwe vormen van inmenging die gebruik maken van sociale media, artificiële intelligentie en *spyware* technologieën. De verbetering van onze gespecialiseerde diensten dient niet alleen rekening te houden met de snelgroeiende personeelsbehoefte, maar ook met de absorptiecapaciteit om de effectiviteit van de diensten te waarborgen. Naast voldoende middelen adviseren wij het ontwikkelen van een duidelijke strategie, inclusief heldere doelstellingen en prioriteiten, om een efficiënte en doelgerichte werking te garanderen. De wervingsprocedures dienen nauwer afgestemd te worden op de unieke eisen en gevoeligheden van de diverse functies binnen elk veiligheidsorgaan. Hierdoor kan adequaat worden voorzien in mensen en middelen die de voortdurend evoluerende fenomenen kunnen detecteren, opvolgen en tegengaan.

44. Er dient tevens verder geïnvesteerd te worden in het versterken van *counter-intelligence* (CI)-capaciteiten en de veiligheidsdiensten. Een heroriëntatie van prioriteiten is cruciaal om de recente focus op terrorismebestrijding aan te vullen en tegelijkertijd met opkomende bedreigingen zoals contraspionage om te gaan.

45. Krachtdadiger optreden tegen corruptie is ook essentieel, omdat het een duidelijke indicator is van het risico op inmenging. Die strijd wordt ook steeds meer gevoerd op Europees niveau, met de vorderingen van het Europees Openbaar Ministerie. Bovendien bevelen we ook aan om de aanbevelingen van de Groep van Staten tegen corruptie (GRECO) van de Raad van Europa en van de Commissie van Venetië zoveel mogelijk uit te voeren.

46. We bevelen aan om een nauwere samenwerking te stimuleren tussen technologiebedrijven, die na *screening* (of via een federaal bestek) als «veilig» worden bestempeld, alsook *cybersecurity*-experts en overheidsinstanties om voortdurend de nieuwste *spyware*-technologieën en -methoden te monitoren en tegen te gaan. Dit kan onder meer resulteren in regelmatige updates van beveiligingsprotocollen en het identificeren van kwetsbaarheden in mobiele besturingssystemen, bijvoorbeeld in spionagesoftware zoals *Pegasus*.

47. We bevelen aan om ruimte te geven aan initiatieven die helpen om desinformatie en complottheorieën die aangestuurd worden via buitenlandse inmenging, te counteren en te debunkten, onder meer via factchecks en betrouwbare bronnen (*credible voices*). Heel wat reguliere media en tal van andere organisaties hebben al diverse initiatieven ontwikkeld op dit vlak. Het opzet is om foute of gemanipuleerde informatie te confronteren met geverifieerde feiten.

48. In België vindt de coördinatie en het overleg tussen de verschillende inlichtingen- en interventiediensten plaats binnen het Coördinatiecomité voor inlichtingen en veiligheid (CCIV), een uniek mechanisme, zelfs op wereldniveau. Om het probleem van buitenlandse politieke inmenging aan te pakken, is een alomvattende benadering nodig, aangezien deze kwestie zich op verschillende niveaus manifesteert, van lokaal tot internationaal. Het betrekken van de lokale overheden hierbij is van cruciaal belang om deze uitdaging effectief aan te pakken.

49. Om de effectiviteit te vergroten, moeten de verschillende veiligheidsdiensten nauwer samenwerken, met als doel de resultaten en conclusies van werkgroepen die bestaan onder auspiciën van het Strategisch Comité voor inlichtingen en veiligheid (SCIV) en die belanghebbenden samenbrengen concreter te maken. Verbeterde informatie-uitwisseling en een holistisch overzicht van de problematiek zijn cruciaal. Het betreft het zogenaamde idee van de «*whole-society*», om inmenging te voorkomen. Men moet fragmentatie voorkomen, de samenhang tussen de verschillende veiligheidsstrategieën tussen de verschillende niveaus is hierbij van uiterst belang. Dit zal helpen bij het identificeren van kwetsbare sectoren, actieve landen en het effectief aanpakken van externe inmenging, waarbij de beschikbaarheid van relevante informatie prioriteit heeft.

B. Internationaal

50. Het Europees kader is uiterst belangrijk om inmenging te voorkomen en om de strategische belangen van Europa en elke lidstaat te beschermen. Wij pleiten voor een nauwe samenwerking met de Europese instanties om de verantwoordelijkheid en volledige autonomie van handelen niet louter aan de lidstaten over te laten.

51. Daarnaast bevelen we aan dat de Europese landen mechanismen opzetten om de ongewenste beïnvloeding van buitenlandse actoren tegen te gaan. Dit omvat duidelijke richtlijnen en transparantievereisten voor politici, opiniemakers, journalisten en denk-

tanks met betrekking tot hun interacties en financiële bronnen. Een gecoördineerde aanpak om de verspreiding van specifieke narratieven via digitale mediaplatforms te monitoren en tegen te gaan, moet worden overwogen.

52. Europese landen moeten samenwerken om zelf meer invloed te kunnen uitoefenen en weerbaarder te zijn tegenover de strategische activiteiten van bepaalde mogendheden zoals Rusland of China. China probeert politici van zowel de regeringsmeerderheid als de oppositie, zowel op nationaal als op Europees niveau, te beïnvloeden. Het richt zich op lokale politici via subnationale diplomatie en probeert opiniemakers, journalisten en leden van denktanks in te lijven.

53. Naast de inmenging die rechtstreeks tegen België gericht is, is het belangrijk dat ook rekening wordt gehouden met bedrijven die kwetsbaar zijn voor inmenging, vooral als zij werken met strategisch waardevolle data. Bij uitbreiding kan dit dus ook schadelijk zijn voor België.

Om economische inmenging tegen te gaan, moeten we onze economie, samenleving en grondgebieden weerbaarder maken.

54. Ook de internationale dreiging vereist een eensgezind internationaal antwoord. Daarom is een blijvende samenwerking met overkoepelende strategische actoren van groot belang. Voorbeelden hiervan zijn het intensiveren van de samenwerking met bestaande internationale organisaties, zoals de Verenigde Naties, de NAVO en de Organisatie voor veiligheid en samenwerking in Europa (OVSE), om gezamenlijke initiatieven te ontwikkelen ter bevordering van democratische stabiliteit en het voorkomen van inmenging. Dit omvat ook een constructieve diplomatieke benadering op zowel nationaal als Europees niveau, waarbij politici van zowel de meerderheid als de oppositie betrokken worden.

55. We bevelen aan dat internationale organisaties en regeringen druk uitoefenen op ondernemingen die *spyware* ontwikkelen en verkopen om te zorgen voor de transparantie en juridische aansprakelijkheid van deze bedrijven.



IV.

HOORZITTINGEN

De notulen van de hoorzittingen worden in doc. Senaat, nr. 7-344/4 gepubliceerd. De volgende personen en instanties werden door de commissie gehoord:

Op 9 januari 2023

- mevrouw Sofia Collignon, *lecturer (assistant professor), School of politics and IR, Queen Mary University of London*;
- de heer Kenneth Lasoen, *lector intelligence and security, Departement Politieke Wetenschappen, Universiteit Antwerpen*;
- Prof. dr. Alexander Mattelaer, *vice dean research, Brussels School of Governance, Vrije Universiteit Brussel*.

Op 27 januari 2023

- de heer Dirk Janvier, afdelingscommissaris, Algemene Dienst inlichting en veiligheid (ADIV);
- de heer Peter Lanssens, directeur van de Analyse, Veiligheid van de Staat (VSSE).

Op 6 februari 2023

- mevrouw Ivana Karásková, *European China Policy fellow, Mercator Institute for China Studies*;
- de heer Michel Liégeois, professor, en de heer Tanguy Struye de Swielande, professor, *Institut de Sciences politiques Louvain-Europe (ISPOLE), UCLouvain*.

Op 27 februari 2023

- de heer Etienne Soula, *research analyst, Alliance for Securing Democracy*;
- de heer Kristof Clerix, onderzoeksjournalist, Knack.

Op 13 maart 2023

- dr. Luca Ferro, assistant professor internationaal recht, Vrije Universiteit Brussel;
- de heer Lutz Güllner, *head of Strategic Communications, European External Action Service (EEAS)*.

Op 31 maart 2023

- de heer Raphaël Glucksmann, voorzitter van de bijzondere commissie Buitenlandse Inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie, en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), Europees Parlement;
- de heer Maxime Lebrun, *deputy director - research & analysis, The European Centre of Excellence for Countering Hybrid Threats*.

Op 14 april 2023

- de heer Eric Snoeck, directeur-generaal federale gerechtelijke politie, Centrale Dienst voor de bestrijding van de corruptie (CDBC);
- de heer Gert Vercauteren, directeur a.i., Coördinatie-orgaan voor de dreigingsanalyse (OCAD);
- de heer Philippe de Koster, voorzitter, Cel voor financiële informatieverwerking (CFI).

Op 26 mei 2023

- de heer Raphaël Kergueno, *senior policy officer, Transparency International EU*;
- de heer Miguel De Bruycker, directeur-generaal, Centrum voor cybersecurity België (CCB).

Op 5 juni 2023

- de heer Guy De Pauw, CEO en medeoprichter, *Textgain*;
- mevrouw Ksenia Iliuk, *strategic communication expert* en medeoprichtster, *LetsData*.

Op 19 juni 2023

- de heer Paul Van Tigchelt, adjunct-kabinetschef, kabinet van vice-eersteminister en minister van Justitie, belast met Noordzee, de heer Van Quickenborne;
- de heer Eric Kalajzic, directeur van het Studiecentrum voor Veiligheid en Defensie, Koninklijk Hoger Instituut voor Defensie (KHID);
- de heer Christopher Houtkamp, *senior research fellow - head Connected Security programme*, *Clingendael - the Netherlands Institute of International Relations*.

Op 20 november 2023

- de heer Etienne Klein, onderzoeksleider, *Commissariat à l'énergie atomique et aux énergies alternatives (CEA)*;
- de heer Samuel Profumo, *chief data officer*, *Radio-télévision belge de la Communauté française (RTBF)*.

DE INFORMATIEVERSLAGEN VAN DE SENAAT

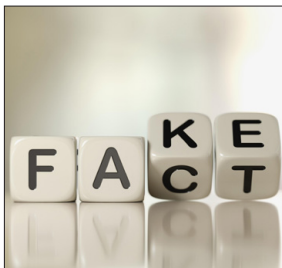
Alle informatieverlagen zijn beschikbaar op de website:
<https://www.senate.be/informatieverlagen>

LEGISLATUUR 2019 - 2024



Informatieverlag over de noodzaak om ons democratisch systeem te moderniseren door de representatieve democratie aan te vullen met meer burgerparticipatie in de besluitvorming op de verschillende bevoegdheidsniveaus alsook in de samenleving

([dossier 7-117](#)) - aangenomen op 18 juni 2021



Informatieverlag betreffende de noodzakelijke samenwerking tussen de federale overheid en de Gemeenschappen inzake de bestrijding van fake news

([dossier 7-110](#)) - aangenomen op 19 november 2021



Informatieverlag over lichamelijke zelfbeschikking en het tegengaan van obstetrisch geweld

([dossier 7-245](#)) - Aangenomen op 15 januari 2024

