DOC 56 **0873/001**

BELGISCHE KAMER VAN VOLKSVERTEGENWOORDIGERS

22 april 2025

VOORSTEL VAN RESOLUTIE

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

(ingediend door de heer Steven Coenegrachts c.s.)

CHAMBRE DES REPRÉSENTANTS DE BELGIQUE

22 avril 2025

PROPOSITION DE RÉSOLUTION

relative à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'État de droit démocratique

(déposée par M. Steven Coenegrachts et consorts)

01478

N-VA	:	*Nieuw-Vlaamse Alliantie*
VB	:	*Vlaams Belang*
MR	:	*Mouvement Réformateur*
PS	:	*Parti Socialiste*
PVDA-PTB	:	*Partij van de Arbeid van België – Parti du Travail de Belgique*
Les Engagés	:	*Les Engagés*
Vooruit	:	*Vooruit*
cd&v	:	*Christen-Democratisch en Vlaams*
Ecolo-Groen	:	*Ecologistes Confédérés pour l'organisation de luttes originales – Groen*
Open Vld	:	*Open Vlaamse liberalen en democraten*
DéFI	:	*Démocrate Fédéraliste Indépendant*

Afkorting bij de nummering van de publicaties:		*Abréviations dans la numérotation des publications:*	
DOC 56 0000/000	*Parlementair document van de 56e zittingsperiode + basisnummer en volgnummer*	*DOC 56 0000/000*	*Document de la 56e législature, suivi du numéro de base et numéro de suivi*
QRVA	*Schriftelijke Vragen en Antwoorden*	*QRVA*	*Questions et Réponses écrites*
CRIV	*Voorlopige versie van het Integraal Verslag*	*CRIV*	*Version provisoire du Compte Rendu Intégral*
CRABV	*Beknopt Verslag*	*CRABV*	*Compte Rendu Analytique*
CRIV	*Integraal Verslag, met links het definitieve integraal verslag en rechts het vertaalde beknopt verslag van de toespraken (met de bijlagen)*	*CRIV*	*Compte Rendu Intégral, avec, à gauche, le compte rendu intégral et, à droite, le compte rendu analytique traduit des interventions (avec les annexes)*
PLEN	*Plenum*	*PLEN*	*Séance plénière*
COM	*Commissievergadering*	*COM*	*Réunion de commission*
MOT	*Moties tot besluit van interpellaties (beigekleurig papier)*	*MOT*	*Motions déposées en conclusion d'interpellations (papier beige)*

TOELICHTING

DAMES EN HEREN,

1. **Inleiding**

Op 22 maart 2024 publiceerde de Senaat een informatieverslag ter bestrijding van de inmenging door buitenlandse mogendheden met het oog op het ondermijnen van de democratische rechtsstaat[1]. Op initiatief van Steven Coenegrachts (Open Vld) onderzocht de commissie voor de Democratische Vernieuwing, Burgerschap en Internationale Aangelegenheden twee jaar lang de verschillende gevaren en aandachtspunten waarop onze veiligheidsdiensten en de respectieve overheden moeten focussen. Hiervoor gaven 26 sprekers uiteenzettingen tijdens hoorzittingen die plaatsvonden van januari tot november 2023.

In het eerste deel werd een reeks vaststellingen uiteengezet die een stand van zaken van het verschijnsel als dusdanig weergeven. De gevaren en aandachtspunten, zoals uiteengezet door de 26 sprekers tijdens de hoorzittingen, staan er ook in vermeld. In het tweede deel van het verslag worden aanbevelingen geformuleerd. Die aanbevelingen moeten helpen om het verschijnsel, dat zich doorgaans onder de radar ontwikkelt, af te bakenen en efficiënter te bestrijden. In het algemeen is de intentie van de ontwerpaanbevelingen helder: het verduidelijken van regels en procedures om inmenging bij burgers en organisaties te voorkomen, het ontwikkelen van proactieve reflexen – met name een kritische geest – om minder vatbaar te zijn en het scheppen van een duidelijker en sterker kader om de aanstichters te vervolgen.

De 55 aanbevelingen, geformuleerd in samenwerking met de experts ter zake, werden opgedeeld in vier pijlers. De eerste pijler vervat strategieën met betrekking tot waarschuwingen en het verminderen van risico's met name gebaseerd op voorlichting en bewustwording, communicatie via dialoog en debat, onderzoek en repressieve maatregelen. De nadruk wordt onder meer gelegd op publieke mandatarissen en overheidsadministraties, academische kringen, journalisten, activisten en diasporagemeenschappen.

De tweede pijler focust op het streven naar meer transparantie met betrekking tot de sociale media, de politiek verantwoordelijken, de ngo's, de private bedrijven en de lobbyisten.

[1] Zie *Parl.St.*, Senaat, 2023-2024, DOC 7-344/2.

DÉVELOPPEMENTS

MESDAMES, MESSIEURS,

1. **Introduction**

Le Sénat a publié, le 22 mars 2024, un rapport d'information relatif à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique[1]. À l'initiative de Steven Coenegrachts (Open Vld), la commission du Renouveau démocratique, de la Citoyenneté et des Affaires internationales du Sénat a examiné, deux années durant, les différents dangers et points d'attention sur lesquels nos services de sécurité et les autorités respectives doivent se concentrer. Pour ce faire, elle s'est appuyée sur les exposés présentés par vingt-six intervenants lors d'auditions qui se sont tenues de janvier à novembre 2023.

Dans un premier volet, le rapport énonce une série de constatations qui dressent un état des lieux du phénomène en tant que tel. Les dangers et les points d'attention, tels qu'ils ont été exposés par les vingt-six personnes qui ont pris la parole lors des auditions, y sont aussi mentionnés. Dans un second volet, le rapport formule des recommandations qui doivent permettre de cerner et de combattre plus efficacement ce phénomène qui se développe généralement sous les radars. Globalement, le but des projets de recommandations est clair: il s'agit de clarifier les règles et les procédures afin de prévenir les ingérences auprès des citoyens et des organisations, de développer des réflexes proactifs – en particulier, l'esprit critique – afin d'être moins vulnérable aux influences, et de fixer un cadre plus strict et plus solide pour pouvoir poursuivre les instigateurs.

Les 55 recommandations, formulées en collaboration avec les experts en la matière, sont réparties en quatre piliers. Le premier pilier comprend les stratégies d'alerte et de réduction des risques, fondées notamment sur l'information et la sensibilisation, la communication par le dialogue et le débat, la recherche et des mesures répressives. Les mandataires publics et les administrations publiques, les milieux universitaires, les journalistes, les militants et les communautés de la diaspora, entre autres, font l'objet d'une attention particulière.

Le deuxième pilier porte sur la recherche d'une plus grande transparence en ce qui concerne les médias sociaux, les responsables politiques, les organisations non gouvernementales (ONG), les entreprises privées et les lobbyistes.

[1] Voir *Doc. parl.*, Sénat, 2023-2024, DOC 7-344/2.

De derde pijler beveelt juridische stappen aan op zowel nationaal als internationaal niveau.

Als laatste bespreekt de vierde pijler aanbevelingen voor het versterken van de belangrijkste actoren in de strijd tegen inmenging, zowel op nationaal als op Europees en internationaal niveau.

Inmenging van buitenlandse mogendheden gaat om het oneigenlijk gebruik van technologie om te destabiliseren, zoals cyberaanvallen, hacking, 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, de niet-gouvernementele organisaties (ngo's), de 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 proberen het land onbestuurbaar te maken. Inmenging gebeurt in het voordeel van de politieke, economische, en socioculturele 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-statelijke actor kan zijn.

De doelstelling van dit voorstel van resolutie, namelijk de bestrijding van de inmenging die erop gericht is democratische rechtsstaten te ondermijnen, komt overeen met de doelstelling van het informatieverslag en is dus van groot belang in de huidige politieke context. We moeten de Belgische democratie, de burgers en de politici weerbaar maken tegen kwaadwillige buitenlandse inmenging.

1. ***Kwaadwillige buitenlandse inmenging***

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. 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.

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

Le troisième pilier recommande des actions juridiques tant au niveau national qu'à l'échelle internationale.

Enfin, le quatrième pilier contient des recommandations visant à renforcer les acteurs clés de la lutte contre les ingérences, tant au niveau national qu'au niveau européen et international.

L'ingérence étrangère consiste, entre autres, en l'utilisation abusive de la technologie à des fins de déstabilisation, comme les cyberattaques, le piratage informatique (*hacking*) ou le recours à l'intelligence artificielle, aux vidéos hypertruquées (*deepfakes*), aux logiciels espions (*spyware*), aux armées de trolls et aux *bots*. L'ingérence étrangère peut aussi se traduire par le financement secret de partis politiques, d'hommes d'affaires ou autres. Enfin, elle peut passer par la coercition économique ou par une volonté de déstabiliser la société civile, par exemple par l'intermédiaire d'universités, d'ONG, de groupements religieux ou de la diaspora. Par tous ces moyens, les instigateurs d'ingérence tentent de perturber le débat démocratique au sein de la société, de fausser ou manipuler des élections et de polariser la société afin de nuire à la cohésion de la société en tentant de la rendre ingouvernable. L'ingérence se fait au profit des intérêts politiques, économiques et socioculturels de l'agresseur. La transparence et la publicité font place à des actes dissimulés, trompeurs, coercitifs ou même corrupteurs. Il est important de préciser à cet égard que l'agresseur n'est pas toujours un acteur étatique, mais peut tout aussi bien être un acteur non étatique.

L'objectif de la présente proposition de résolution, à savoir la lutte contre les ingérences visant à saper les fondements de l'État de droit démocratique, rejoint celui du rapport d'information et revêt donc une grande importance dans le contexte politique actuel. Il s'agit de faire en sorte que la démocratie belge, les citoyens et les mandataires politiques soient capables de résister aux ingérences étrangères malveillantes.

1. ***Ingérence étrangère malveillante***

L'ingérence étrangère est un phénomène qui a toujours existé et qui fait partie intégrante de l'histoire des relations internationales. Les mobiles sont divers et peuvent être d'ordre économique, militaire, géopolitique ou politique. Dans la pratique contemporaine, l'ingérence étrangère procède de plus en plus souvent d'une volonté de saper les fondements d'un État de droit démocratique.

Des opérations d'influence sont des actes qui visent à favoriser des intérêts étrangers par la mise en œuvre illégitime de *soft power* dans le but de corrompre l'intégrité de certains processus et comportements politiques. La

begrip soft power staat centraal. Bij inmengingsoperaties gaat het niet echt om dwang, maar meer om overtuigingshandelingen die het politieke gedrag beïnvloeden.

De Noord-Atlantische Verdragsorganisatie (NAVO) hanteert veeleer de term *hybrid interference* waarmee wordt verwezen naar een verzameling van verdoken, niet-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 worden onderscheiden van *hybrid warfare*, die als een militaire benadering moet worden beschouwd. Drie instrumenten staan centraal in *hybrid interference*: clandestiene diplomatie, geo-economie en desinformatie.

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[2]. 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 worden afgebakend. Invloed is in ieder geval geen synoniem voor inmenging. Er ligt een vage grens tussen legitieme beïnvloeding en ongeoorloofde manipulatie.

Rechtmatige invloed en onwettige inmenging zijn twee conceptuele polen in een spectrum van soortgelijke activiteiten. Bepalen wat rechtmatig is, is een intrinsieke politieke activiteit. 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-statelijke actor die ingaan tegen onze soevereiniteit, waarden en belangen. Inmenging gebeurt in het voordeel van de politieke, economische, en socioculturele belangen van de agressor. Het is een belangrijk gegeven dat de agressor niet altijd een statelijke actor maar evengoed een niet-statelijke actor kan zijn. Inmenging is problematisch zodra besluitvormingsprocessen worden beïnvloed en

[2] *Clingendael, Netherlands Institute of International Relations, Policy Brief*, december 2022. Raadpleegbaar op: *https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf*

notion de *soft power* joue ici un rôle central. Dans les opérations d'influence, il n'est pas question de contrainte à proprement parler, mais plutôt d'actes de persuasion qui influencent le comportement politique.

L'Organisation du Traité de l'Atlantique Nord (OTAN) utilise plutôt l'expression "interférence hybride" (*hybrid interference*), qui fait référence à un ensemble de moyens déguisés, non militaires, dans le but de saper la cohésion interne et de renforcer la polarisation politique. Il s'agit donc d'une manipulation clandestine des intérêts stratégiques d'autres États. Cette expression se distingue clairement de la notion de "guerre hybride" (*hybrid warfare*), qui doit être considérée comme relevant d'une approche de type militaire. Trois instruments jouent un rôle central dans l'interférence hybride: la diplomatie clandestine, la géoéconomie et la désinformation.

Il y a plusieurs degrés d'ingérence, comme l'illustre le schéma présenté dans une note d'orientation de l'Institut Clingendael sur les initiatives européennes contre les ingérences[2]. Le schéma énonce un système de gradation allant de l'influence transparente sur l'opinion publique aux opérations paramilitaires entraînant la mort de personnes. Cela montre qu'il existe tout un spectre de formes d'ingérence. Il importe donc de définir clairement les concepts. Quoi qu'il en soit, influence n'est pas synonyme d'ingérence. La frontière est floue entre l'influence légitime et la manipulation illicite.

L'influence légitime et l'ingérence illégitime sont deux pôles conceptuels d'un spectre d'activités similaires. Déterminer ce qui est légitime est une activité intrinsèquement politique. L'influence est normale et fait partie de la diplomatie. Le fait que d'autres acteurs (privés) tentent d'influencer nos processus décisionnels en leur faveur fait partie de la manière traditionnelle de faire des affaires ou du commerce. Il n'y a aucun problème tant que l'influence est légitime.

L'ingérence illicite, en revanche, est problématique. L'ingérence recouvre des activités secrètes, trompeuses, coercitives, corruptrices ou d'autres activités illégales d'un acteur étranger étatique ou non, qui vont à l'encontre de notre souveraineté, de nos valeurs et de nos intérêts. L'ingérence se fait au profit des intérêts politiques, économiques et socioculturels de l'agresseur. Il est important de préciser à cet égard que l'agresseur n'est pas toujours un acteur étatique, mais peut tout aussi bien être un acteur non étatique. L'ingérence devient problématique dès l'instant où les processus décisionnels

[2] *Clingendael, Netherlands Institute of International Relations, Policy Brief*, décembre 2022. Disponible à l'adresse: *https://www.clingendael.org/sites/default/files/2022-12/Policy_brief_EU_Hybrid_Toolbox.pdf*

er wordt gepoogd om strategische economische processen te infiltreren en te manipuleren in het voordeel van de agressor en ten nadele van onze maatschappij en democratische waarden.

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)[3] 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 destabiliseren.

Volgens het Amerikaanse Federal Bureau of Investigation (FBI) kunnen inmengingsoperaties zich manifesteren als criminele pogingen om het stemmingsproces te ondermijnen en in illegale campagnefinanciering te voorzien of als cyberaanvallen op de steminfrastructuur, samen met computerinbraken gericht op onder meer verkozen ambtenaren, verkiezingsuitslagen en verkiezingskandidaten. Bijvoorbeeld via onlinedesinformatiecampagnes 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 trekken.

2. ***De agressor***

De term “agressor” kan doelbewust worden gebruikt 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 doen. De agressor poogt om het situationeel bewustzijn 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 agressor.

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

[3] 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 (INGE 2), (2022/C 347/28), bekendgemaakt in het *Publicatieblad van de Europese Unie* van 9 september 2022.

sont influencés et où l’on tente d’infiltrer et de manipuler des processus économiques stratégiques en faveur de l’agresseur et au détriment de notre société et de nos valeurs démocratiques.

Selon la décision du Parlement européen du 10 mars 2022 sur la constitution d’une commission spéciale sur l’ingérence étrangère dans l’ensemble des processus démocratiques de l’Union européenne, y compris la désinformation (INGE 2)[3], l’ingérence est le fait d’acteurs étrangers, malveillants et autoritaires, étatiques ou non, qui utilisent la manipulation de l’information et d’autres tactiques pour s’immiscer dans les processus démocratiques de l’Union européenne, l’objectif ultime étant de déstabiliser la démocratie européenne.

Selon le Bureau fédéral américain d’investigation (Federal Bureau of Investigation – FBI), les opérations d’influence peuvent prendre les formes de tentatives criminelles en vue de saper le processus électoral et de mettre en place un financement illégal des campagnes électorales, ou de cyberattaques contre l’infrastructure de vote, assorties de piratages informatiques visant entre autres des fonctionnaires élus, des résultats électoraux et des candidats aux élections. L’on peut penser, par exemple, aux campagnes de désinformation en ligne qui sont menées régulièrement et contribuent à la diffusion d’informations erronées dans le but d’influencer les résultats électoraux ou de mettre en doute la qualité du processus électoral.

2. ***L’agresseur***

Le terme “agresseur” peut être utilisé délibérément dans le présent contexte, en particulier pour les agressions perpétrées par des régimes autocratiques. Dans ce cas, il s’agit en effet d’une agression, qui consiste en une forme de guerre entre des régimes autocratiques et la société démocratique ouverte, et plus spécifiquement contre ses valeurs, son mode de vie et sa manière de faire de la politique. L’agresseur tente de perturber la capacité de la cible à apprécier la situation. Il exerce une pression sur la cible pour obtenir un résultat qui lui est favorable. Il s’agit de manipuler la perception de la cible, dans le but qu’elle prenne des décisions à l’avantage de l’agresseur.

L’ingérence étrangère n’est plus seulement le fait d’États plus ou moins malveillants; elle est aussi parfois, et le sera sans doute de plus en plus à l’avenir, opérée par des acteurs non étatiques: groupes criminels et

[3] Décision du Parlement européen du 10 mars 2022 sur la constitution d’une commission spéciale sur l’ingérence étrangère dans l’ensemble des processus démocratiques de l’Union européenne, y compris la désinformation (INGE 2), (2022/C 347/28), publiée au *Journal officiel de l’Union européenne* du 9 septembre 2022.

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 mogendheden 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 mogendheid.

3. ***Uitingen van buitenlandse inmenging***

Buitenlandse inmenging uit zich dus via diverse actoren en in uiteenlopende vormen. Naargelang de verschillen in de definiëring van inmenging, verschillen ook de praktische vaststellingen van het fenomeen. In 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))[4] en tijdens de hoorzittingen in de Senaat van het Amerikaanse Federal Bureau of Investigation (FBI), academici en experten uit diverse domeinen, onderzoeksjournalisten, onderzoeksinstellingen en hoge functionarissen van verschillende veiligheidsdiensten wordt de volgende niet-limitatieve lijst van technieken vastgesteld.

1. De "*reverse OODA-loop*" vormt een eerste voorbeeld van een techniek waarmee agressoren de handelingen van hun doelwitten beïnvloedden. Dat systeem is gebaseerd op de inversie van de OODA-loop (*observe–orient–decide–act-cyclus*). Hierbij vertrekt de agressor van het eindpunt, dat wil zeggen het gewenste scenario. Van hieruit gaat hij 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. Hiermee wil de agressor de democratische waarden ondermijnen, de besluitvorming manipuleren of via spionage inlichtingen over het doelwit verkrijgen. De Russische inmenging in de Amerikaanse verkiezingen van 2016 volgde de "*reverse OODA-loop*". Als eerste stap werd de observatie van het Amerikaanse publiek door beleidsmakers verstoord door desinformatie en *bots* op sociale media. Daarop werd de oriëntatie van beleidsdoelen gemanipuleerd door polarisatie en nepbewegingen. De besluitvorming werd ondermijnd door een vervuilde informatiestroom

[4] 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)) (2021/C 202/06), bekengemaakt in het *Publicatieblad van de Europese Unie* op 28 mei 2021.

mafieux, grands groupes économiques et financiers, et d'autres encore. Cette évolution nécessite une adaptation des outils et des stratégies de contre-ingérence et sans doute aussi une adaptation de la législation. Les choses se compliquent encore lorsqu'on observe que certains de ces acteurs non étatiques agissent comme sous-traitants de puissances soucieuses de ne pas apparaître en première ligne. C'est désormais presque devenu la règle dans le cyberespace, où les actions offensives d'ingérence sont confiées à des opérateurs privés qui, contre rémunération, réalisent les actions commanditées par la puissance contractante.

3. Manifestations d'ingérence étrangère

L'ingérence étrangère peut donc être le fait de différents acteurs et revêtir diverses formes. Les observations du phénomène de l'ingérence dans la pratique varient aussi suivant les définitions qu'on lui donne. La liste, non exhaustive, des techniques d'ingérence utilisées, telle que figurant ci-dessous, a été établie sur la base de la résolution du Parlement européen du 10 octobre 2019 sur l'ingérence électorale étrangère et la désinformation dans les processus démocratiques nationaux et européen (2019/2810(RSP))[4] et à la lumière des auditions, au Sénat américain, du Bureau fédéral américain d'investigation (Federal Bureau of Investigation, FBI), d'universitaires et d'experts dans divers domaines, de journalistes d'investigation, d'instituts de recherche et de hauts fonctionnaires de différents services de sécurité.

1. La boucle OODA inversée constitue un premier exemple de technique permettant à des agresseurs d'influencer les agissements de leurs cibles. Ce système repose sur l'inversion de la boucle OODA (*observe–orient–decide–act-cyclus*). L'"agresseur" part de la fin du cycle, c'est-à-dire du résultat souhaité. À partir de là, il va faire de la rétro-ingénierie et parcourir les étapes permettant de faire agir – inconsciemment – la cible de son propre chef pour réaliser le résultat final. L'agresseur entend ainsi saper les valeurs démocratiques, manipuler la prise de décision ou obtenir des informations sur la cible par des techniques d'espionnage. L'ingérence russe dans les élections américaines de 2016 reposait sur la boucle OODA inversée. Tout d'abord, l'observation du public américain par les décideurs politiques a été perturbée par de la désinformation et des robots sur les médias sociaux. Ensuite, l'orientation des objectifs politiques a été manipulée par la polarisation et les manœuvres. Le processus décisionnel a été miné par un flux de fausses informations et, enfin, l'action des décideurs politiques

[4] Résolution du Parlement européen du 10 octobre 2019 sur l'ingérence électorale étrangère et la désinformation dans les processus démocratiques nationaux et européen (2019/2810(RSP)) (2021/C 202/06), publiée au *Journal officiel de l'Union européenne* le 28 mai 2021.

en als laatste werd de actie van de beleidsmakers verlamd door politieke chaos en wantrouwen. Zo werd de VS gedwongen reactief te handelen, terwijl Rusland zijn invloed vergrootte zonder fysiek in te grijpen.

2. Daarnaast kunnen in desinformatie gespecialiseerde bedrijven bijdragen aan buitenlandse inmenging. Pegasus-spyware dient hierbij als voorbeeld. Het Pegasus-project, opgezet door een journalistencollectief, onthulde dat journalisten en mensenrechtenactivisten wereldwijd het slachtoffer werden van Pegasus-spyware, ontwikkeld door de Israëlische NSO Group. Ook in België waren er slachtoffers van de spyware. Die laat toe om vanop afstand de software van smartphones volledig over te nemen en te controleren.

3. Ook via politieke actoren, verenigingen, instellingen, religieuze groeperingen en bekende personen kunnen buitenlandse mogendheden zich ongeoorloofd inmengen. Met financiering of andere drukkingsmiddelen beïnvloedden zij invloedrijke actoren. Die actoren hebben op hun beurt een impact op de publieke opinie of de praktische besluitvorming. Op financieel vlak komt inmenging er op neer om financiële afhankelijkheid te creëren van het doelwit. Via strategische investeringen en schenkingen aan belangengroepen, politieke partijen of onderzoeksfinanciering creëert de agressor afhankelijkheid en drukt hij zijn kwaadwillige invloed door. 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 Research & Development en/of leningen verstrekt onder bepaalde voorwaarden.

4. Er ontstond een nieuw fenomeen: het gebruik van "*freelance*-agenten" die geen directe link hebben met de Russische inlichtingendienst. Een zoekertje met een simpele opdracht verschijnt in een Telegramgroep: "Ga een stel anti-Oekraïense stickers plakken in het straatbeeld en krijg 20 euro." Een geïnteresseerde gaat erop in. Een *bot* stelt hem enkele basisvragen. Wanneer de kandidaat slaagt voor die eerste test, neemt een Russische inlichtingenofficier de *chat* over en geeft verdere instructies. De gerekruteerde voert daarna zijn taak uit, stuurt een foto als bewijs en wordt betaald in cryptomunten. Vanaf dat punt volgen opdrachten elkaar op, alsmaar zwaarder. De uitvoerder komt diep in de illegaliteit terecht. Uiteindelijk volgt een vraag tot daadwerkelijke sabotage. In verschillende Duitse steden spoten bijvoorbeeld meerdere daders in aanloop naar de verkiezingen bouwschuim in de uitlaten van meer dan 270 auto's. Stickers van de Duitse groene partij moesten

a été paralysée par le chaos politique et la méfiance. Alors que les États-Unis ont été contraints d'agir de manière réactive, la Russie a renforcé son influence sans intervenir physiquement.

2. En outre, des sociétés spécialisées dans la désinformation peuvent participer à des opérations d'ingérence étrangère. Citons, à cet égard, l'exemple du logiciel espion Pegasus. Le projet Pegasus, mis sur pied par un collectif de journalistes, a révélé que partout dans le monde, des journalistes et militants des droits de l'homme avaient été victimes du logiciel espion Pegasus, développé par la société israélienne NSO Group. En Belgique aussi, des personnes ont été victimes de ce logiciel, qui permet de prendre complètement le contrôle de smartphones à distance.

3. Des puissances étrangères peuvent aussi se livrer à des ingérences illicites par le biais d'acteurs politiques, d'associations, d'institutions, de groupements religieux et de personnes connues. Elles influencent des acteurs de premier plan par de l'argent ou d'autres moyens de pression. Ces acteurs ont à leur tour une influence sur l'opinion publique ou le processus décisionnel pratique. Sur le plan financier, l'ingérence consiste à créer une dépendance financière de la cible. Au moyen d'investissements stratégiques et de dons à des groupes d'intérêts ou à des partis politiques ou de l'octroi d'un financement de recherche, l'agresseur crée une dépendance et exerce son influence malveillante. Un exemple connu est celui de l'Institut Confucius qui est financé par les autorités chinoises. Par le biais d'activités dans le milieu universitaire, cet institut tente à la fois de donner une meilleure image de la Chine et d'infiltrer l'économie de la connaissance en lorgnant les résultats de la recherche et du développement et/ou en octroyant des prêts sous certaines conditions.

4. Un nouveau phénomène a fait son apparition: le recours à des agents *freelance*, qui n'ont pas de lien direct avec les services de renseignement russes. Une petite annonce décrivant une mission simple à réaliser est publiée dans un groupe sur Telegram: "Collez une série d'autocollants anti-ukrainiens dans les rues et recevez 20 euros!". Celui qui réagit à l'annonce doit ensuite répondre à quelques questions élémentaires, qui lui sont posées par un robot. Si le candidat réussit ce premier test, un agent des services de renseignement russes prend le relais et lui donne des instructions supplémentaires. Le candidat recruté exécute ensuite sa mission, envoie une photo comme preuve et est rémunéré en cryptomonnaies. À partir de là, les missions se succèdent et deviennent de plus en plus délicates. L'exécutant s'enfonce de plus en plus dans l'illégalité. Il lui est finalement demandé de réaliser un véritable acte de sabotage. Dans plusieurs villes allemandes, par

suggereren dat die partij achter de sabotage zat. Maar het was Rusland die op deze manier "*freelance*-agenten" aanstuurde om bewust haat aan te wakkeren en de samenleving te verdelen.

5. Verder waarschuwde ook de Veiligheid van de Staat (VSSE) voor cyberaanvallen. Op het vlak van tactieken en technieken is er sprake 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.

6. 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, conform de definitie in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten[5]. Een andere partner die wordt bevraagd is de Cel voor Financiële Informatieverwerking (CFI), die onderzoek kan voeren naar mogelijke financiering uit een derde land.

7. Een andere 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).

8. De *modus operandi* van het Spaans bedrijf Eliminalia is een volgend voorbeeld van buitenlandse inmenging. Die inmenging 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

[5] Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, bekendgemaakt in het *Belgisch Staatsblad* van 18 december 1998.

exemple, plusieurs auteurs ont pulvérisé de la mousse de construction dans les pots d'échappement de plus de 270 voitures avant les élections. Des autocollants du parti écologiste allemand étaient censés faire croire que ce parti était à l'origine du sabotage. Or ces actes ont été commis à l'instigation de la Russie, qui a eu recours à des agents *freelance* pour appeler délibérément à la haine et diviser la société.

5. La Sûreté de l'État (VSSE) a aussi lancé une mise en garde contre de possibles cyberattaques. En matière de tactiques et de techniques, il est question de cyberintrusion (sabotage) ou de l'acquisition d'infrastructures (numériques) critiques à des fins d'espionnage ou de pressions. Un exemple qui peut être cité à cet égard est l'emploi de technologies de communication de fabrication chinoise, qui induit le risque que la Chine maîtrise les lignes de communication.

6. Dans le cadre de sa mission légale en matière d'ingérences, la Sûreté de l'État examine aussi, par exemple, les formes possibles d'influence par le biais d'églises et de groupements religieux. Dans le cadre de la guerre en Ukraine par exemple, il a été constaté dans plusieurs pays européens que la Russie tentait d'exercer une influence à travers l'Église orthodoxe.

Dans la procédure utilisée en Belgique pour la reconnaissance d'un culte ou d'une philosophie, l'avis de la VSSE et d'autres partenaires de sécurité est demandé. Un des aspects que vérifie la VSSE à cet égard est le risque d'ingérence, tel qu'il est défini dans la loi du 30 novembre 1998 organique des services de renseignement et de sécurité[5]. Un autre partenaire sollicité en l'espèce est la Cellule de Traitement des informations financières (CTIF), qui peut procéder à des analyses sur des financements éventuels en provenance d'un pays tiers.

7. Une autre pratique d'ingérence dans les affaires d'un pays tiers consiste à recruter, placer ou imposer, à court ou long terme, des individus à des positions stratégiques (en utilisant des moyens d'ingénierie sociale, de corruption, de chantage ou d'intimidation).

8. Le *modus operandi* de la société espagnole Eliminalia est un autre exemple d'ingérence étrangère et se présente comme suit: un client demande, par exemple, de supprimer d'internet un article défavorable. L'équipe d'Eliminalia copie et colle l'article concerné sur la plateforme d'un fournisseur d'infox en antidatant la date de publication, ce qui donne l'impression que l'article

[5] Loi du 30 novembre 1998 organique des services de renseignement et de sécurité, publiée au *Moniteur belge* du 18 décembre 1998.

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 halen.

Artificiële intelligentie (AI) vormt een uitdaging voor onze democratieën. Er is nood aan reglementering, evenals 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. Het gebrek aan transparantie is de kern van de problematiek die moet worden aangepakt. 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 het is niet echt waarschijnlijk dat het onderzoek op het vlak van AI kan worden stopgezet.

Zowel binnenlandse als buitenlandse veiligheidsdiensten stelden afgelopen jaren desinformatiecampagnes vast waarmee Rusland de democratie probeerde te destabiliseren. In Brussel was in september 2023 veel protest tegen de Franstalige seksuele voorlichting EVRAS. De Belgische veiligheidsdiensten merken dat buitenlandse accounts dit versterken op sociale media om de maatschappij te verdelen. In 2024 zaait een vermoedelijk Russische desinformatiecampagne onrust over een bedwantsenplaag in Parijs. De campagne stelt de plaag groter voor en duidt Oekraïense vluchtelingen aan als de oorzaak. Op de zender BabyTV is eind maart 2024 kort Russische propaganda te zien. De verstoring werd veroorzaakt door hackers die het eigenlijk op de Oekraïense televisie hadden gemunt. Ook in andere landen, waaronder in België, worden zenders verstoord. Een aan Rusland gelinkt beïnvloedingsnetwerk was rond de Europese verkiezingen in juni 2024 online actief om Franse en Duitse radicaal-rechtse partijen te promoten. In Duitsland bleek zeker 10 % van alle tweets over de rechtse AfD-partij afkomstig van Russische accounts.

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

copié avait été publié plus tôt. Eliminalia dénonce ensuite l'article original pour plagiat et demande par conséquent aux moteurs de recherche Internet de supprimer l'article original de leurs fichiers de recherche. Cette intervention – simple – a été fructueuse dans de nombreux cas. La législation est donc utilisée de manière abusive pour faire en sorte que des informations présentant un intérêt public ne soient plus disponibles en ligne.

L'intelligence artificielle (IA) pose un énorme problème à nos démocraties. Il faut réguler, contrôler et imposer une forme de traçabilité. Le gros problème de la production d'images ou de récits par l'intelligence artificielle est qu'il s'agit d'une production "cachée". Le manque de transparence est le cœur du problème qu'il faut traiter. L'idée, émise par de grandes personnalités, d'arrêter temporairement le développement de cette technologie est utile parce qu'elle nous alerte sur ses risques. Mais il est peu vraisemblable que la recherche sur l'IA puisse être arrêtée.

Ces dernières années, les services de sécurité, tant nationaux qu'étrangers, ont constaté que la Russie menait des campagnes de désinformation pour tenter de déstabiliser la démocratie. En septembre 2023, de nombreuses manifestations ont eu lieu à Bruxelles contre l'éducation à la vie relationnelle, affective et sexuelle (EVRAS) en Communauté française. Les services de sécurité belges ont observé que l'opposition à l'EVRAS a été exacerbée sur les réseaux sociaux par des comptes étrangers, afin de diviser la société. En 2024, une campagne de désinformation, dont l'origine est probablement russe, a semé le trouble à propos d'une infestation de punaises de lit à Paris. Cette campagne a exagéré l'ampleur du problème et a présenté les réfugiés ukrainiens comme en étant la cause. L'émetteur BabyTV a brièvement diffusé de la propagande russe à la fin du mois de mars 2024. Cette perturbation a été causée par des pirates informatiques qui ciblaient en réalité la télévision ukrainienne. Certains émetteurs rencontrent également des perturbations dans d'autres pays, parmi lesquels la Belgique. Dans le contexte des élections européennes de juin 2024, un réseau d'influence lié à la Russie a activement fait la promotion, sur Internet, des partis de droite radicale français et allemands. En Allemagne, au moins 10% de l'ensemble des tweets publiés au sujet du parti de droite AfD semblaient provenir de comptes russes.

La diffusion de fausses informations sur les candidats a des conséquences sur les élections. Nous pouvons en effet dire avec certitude – bien qu'il soit difficile de déterminer dans chaque cas spécifique la source et l'influence étrangère visée – que l'objectif est d'influencer

– dat het de bedoeling is om de verkiezingsuitslag te beïnvloeden. Kandidaten die een grote kanshebber zijn om de verkiezingen te winnen, lopen in dat kader meer kans om het doelwit van desinformatie te worden.

Een onderzoek over de kandidaten voor de Britse verkiezingen van 2019 toonde aan dat de doelwitten van desinformatie konden worden herleid 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 personen met bepaalde kenmerken te ondermijnen.

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 sneeuwbaleffect 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 sneeuwbaleffect heel grote gevolgen kunnen hebben.

Buitenlandse invloeden manifesteren zich niet enkel in het politiek systeem maar kunnen ook gericht zijn tegen de rechterlijke macht. 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 bonafide de belangen van een buitenlandse mogendheid verdedigt en dat er geen sprake is van een doelbewuste demarche.

4. ***Wat te doen?***

Als de samenleving haar onafhankelijkheid wil bewaren en haar lot in eigen handen wil houden, moet ze weerbaar worden gemaakt tegen 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.

Er moet een breed scala aan benaderingen worden gehanteerd bij het aanpakken van de kwestie van

les résultats électoraux. Dans ce cadre, les candidats qui ont de fortes chances d'être élus sont plus susceptibles d'être la cible de la désinformation.

Une étude portant sur les candidats aux élections de 2019 en Grande-Bretagne a montré que les cibles de la désinformation peuvent être réduites à certains groupes. Les candidats des minorités noire et asiatique étaient beaucoup plus souvent ciblés. Cela signifie donc que les campagnes de désinformation peuvent être utilisées dans le cadre d'une tentative organisée de saper la représentation de personnes présentant des caractéristiques déterminées.

L'étude a révélé aussi que les candidats qui sont victimes de désinformation en attribuent la faute à leurs adversaires, tout en admettant qu'ils ne savent pas vraiment d'où elle provient. Même lorsque des moyens techniques permettent de tracer cette désinformation, son effet "boule de neige" reste difficile à stopper. Il est prouvé que la désinformation peut mener à d'autres formes d'intimidation et de violence. On sait également que les interventions à petite échelle peuvent avoir des conséquences très importantes en raison de ce même effet "boule de neige".

Les influences étrangères ne se manifestent pas uniquement envers le système politique; elles peuvent également viser le système judiciaire. Le défi à relever est de déterminer comment traiter les acteurs nationaux dans le cadre d'opérations d'influence. Il se peut en effet qu'un acteur national défende de bonne foi les intérêts d'une puissance étrangère, et qu'il ne s'agisse pas d'une démarche délibérée.

4. ***Que faire?***

Si elle veut préserver son indépendance et rester maîtresse de son destin, la société doit apprendre à résister à de telles menaces. Les individus, les gouvernements, les sociétés et les communautés internationales doivent œuvrer ensemble au développement d'une approche coordonnée visant à protéger le principe de l'État de droit démocratique contre les ingérences étrangères. Pour garantir l'intégrité des processus démocratiques, il est essentiel d'adopter une approche holistique qui permette de renforcer la capacité de résistance non seulement du citoyen individuel, mais aussi de nos institutions. Les mesures à prendre pour lutter contre les ingérences sont d'ordre politique, technologique, juridique mais aussi social.

Il faut utiliser un large éventail d'angles sous lesquels aborder la question de l'ingérence étrangère, étant

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.

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 moet worden georganiseerd.

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. Daarbij wordt een belangrijke rol weggelegd voor het onderwijs, als een effectieve manier om inmengingscampagnes te counteren. Overheden en sociale mediabedrijven moeten 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.

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.

De nationale regelgever heeft de vrijheid om strengere wetten in te voeren dan internationale normen vereisen om buitenlandse financiering van politieke campagnes te beperken en transparantieverplichtingen op te leggen aan lobbyisten. Dit zonder echter zo ver te gaan als de *Foreign Agents Registration Act* in de Verenigde Staten. Dit stelt België, eventueel in EU-verband, in staat om een robuuster juridisch kader te creëren voor de bescherming tegen externe inmenging. Naast de implementatie van controles moeten er concrete stappen worden genomen om het fenomeen grondig te begrijpen en te analyseren.

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 benadering en tactieken om dergelijke inmenging te bestrijden, en een aanpassing van de wetgeving om deze fenomenen te bestrijden.

donné qu'elle affecte tous les aspects de notre société. La définition employée à la fois par l'UE et par l'Organisation du Traité de l'Atlantique Nord (OTAN) doit servir de guide à cet égard.

La protection de nos systèmes démocratiques contre les ingérences demande à la fois une action spécialisée de services de renseignement et de sécurité performants, mais également un apprentissage de la culture du risque d'ingérence et de la protection à organiser.

Il est indispensable de ne pas se fier uniquement à la vérification des faits (*fact-checking*) et à la démystification (*debunking*), mais aussi d'œuvrer à un changement plus large de mentalité. L'approche doit également viser à développer l'esprit critique, l'éducation aux médias et la résilience face à la désinformation. À cet égard, un rôle important est dévolu à l'enseignement en tant que moyen efficace de contrer les mécanismes d'ingérence. Les autorités publiques et les entreprises de médias sociaux doivent collaborer pour développer des programmes éducatifs qui aideront les citoyens à adopter une attitude plus critique à l'égard des informations et à en vérifier les sources avant de les partager.

La transparence du financement des partis politiques et des campagnes médiatiques dans le cadre d'élections est un point important. Il est crucial à cet égard d'améliorer la transparence du financement des partis et des politiques médiatiques pendant les élections. Une attention particulière doit être accordée au renforcement de la réglementation dans ce domaine.

Le législateur national est libre d'adopter des lois plus strictes que les normes internationales pour limiter le financement étranger de campagnes politiques et imposer des obligations de transparence aux lobbyistes, sans aller cependant aussi loin que le *Foreign Agents Registration Act* aux États-Unis. Cela permet à la Belgique d'instaurer, éventuellement au niveau de l'UE, un cadre juridique plus solide pour se prémunir contre les ingérences extérieures. Outre la mise en place de contrôles, il faut prendre des mesures concrètes pour que l'on puisse analyser et comprendre en profondeur le phénomène.

Nous constatons de plus en plus l'implication d'acteurs non gouvernementaux, tels que des organisations criminelles ou mafieuses, de grandes entités économiques ou financières ou d'autres groupes. Cette tendance nous oblige à revoir les approches et tactiques que nous déployons pour lutter contre l'ingérence et à adapter la législation pour combattre ces phénomènes.

Het is van essentieel belang dat de overheid aandringt op verbeterde transparantie met betrekking tot de financiering van niet-gouvernementele organisaties (ngo's), verenigingen zonder winstoogmerk (vzw's) 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. De recente oprichting van het Interfederal Screening Committee (ISC), dat de betrouwbaarheid van directe buitenlandse investeringen screent, is alvast een stap in de juiste richting.

Krachtdadiger optreden tegen corruptie is essentieel, omdat het een duidelijke indicator is van het risico op inmenging. Die strijd wordt steeds meer gevoerd op Europees niveau, met de vorderingen van het Europees openbaar ministerie. Dus moeten de aanbevelingen van de Groep van Staten tegen corruptie (GRECO) van de Raad van Europa en van de Commissie van Venetië zo veel mogelijk worden uitgevoerd.

België moet op korte termijn een grondig onderzoek starten 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 hun positie al hebben bepaald. Actieve deelname aan dit debat zou België niet alleen in staat stellen om het internationale kader mee vorm te geven, maar ook om waardevolle inzichten te leveren. Voor een goed algoritmisch bestuur moet een democratisch aanvaardbaar kader worden gecreëerd. Door hierbij niet alleen politici en de verantwoordelijken voor de veiligheidsstrategie, te betrekken, maar ook burgers, schept men de voorwaarden voor een goede werking ervan. Een vergelijkbare situatie doet zich voor in verband met de nieuwe NIS2-richtlijn en de verordening inzake cyberweerbaarheid (*Cyber Resilience Act*[6]). 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.

[6] Verordening (EU) 2024/2847 van het Europees Parlement en de Raad van 23 oktober 2024 betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordeningen (EU) nrs. 168/2013 en (EU) 2019/1020 en Richtlijn (EU) 2020/1828 (Verordening cyberweerbaarheid), bekendgemaakt in het *Publicatieblad van de Europese Unie* op 20 november 2024.

Il est essentiel que les pouvoirs publics œuvrent en faveur d'une transparence accrue en ce qui concerne le financement des organisations non gouvernementales (ONG), associations sans but lucratif (ASBL) et autres organisations. Cela peut être réalisé par le biais d'exigences légales relatives à une divulgation détaillée des sources et montants de financement dans les rapports annuels et autres documents pertinents. Tout cela sera réalisé conformément à la jurisprudence de la Cour européenne des droits de l'homme et aux avis de la Commission de Venise. Cette transparence renforcera la confiance dans les organisations concernées et mettra en lumière d'éventuelles pratiques nébuleuses. La création récente du Comité de filtrage interfédéral (CFI), qui analyse la fiabilité des investissements directs étrangers, est en tout cas un pas dans la bonne direction.

Le renforcement de la lutte contre la corruption est essentiel, car elle constitue un indicateur clair du risque d'ingérence. Cette lutte s'organise de plus en plus au niveau européen, avec les demandes du Parquet européen. Il convient donc de mettre en œuvre autant que possible les recommandations du Groupe d'États contre la corruption (GRECO) du Conseil de l'Europe et de la Commission de Venise.

La Belgique doit entamer à court terme une étude approfondie en vue d'adopter une position claire à l'égard de l'application du droit international dans le cyberespace. Des pays tels que la France, les Pays-Bas, l'Allemagne et l'Italie ont déjà pris une initiative en la matière et ont défini leur position. Le concours actif de la Belgique au débat lui permettrait non seulement de participer à la concrétisation du cadre international, mais aussi d'y apporter une contribution précieuse. Pour assurer une bonne gouvernance algorithmique, il importe de fournir un cadre qui soit démocratiquement acceptable. En y associant non seulement les dirigeants politiques et les responsables de la stratégie de sécurité, mais également les citoyens, on se donne les conditions pour qu'il fonctionne bien. La situation est similaire au sujet de la nouvelle directive NIS2 et du règlement européen sur la cyberrésilience (connu sous le nom de "*Cyber Resilience Act*[6]"). À cet égard, nous recommandons de trouver un équilibre entre la protection contre l'ingérence étrangère et le maintien de standards ouverts et d'un fonctionnement concurrentiel du marché, tout en soutenant le marché intérieur.

[6] Règlement (UE) 2024/2847 du Parlement européen et du Conseil du 23 octobre 2024 concernant des exigences de cybersécurité horizontales pour les produits comportant des éléments numériques et modifiant les règlements (UE) n^{os} 168/2013 et (UE) 2019/1020 et la directive (UE) 2020/1828 (règlement sur la cyberrésilience), publié dans le *Journal officiel de l'Union européenne* du 20 novembre 2024.

In België vindt de coördinatie en het overleg tussen de 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. Analoog met 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.

Om de effectiviteit te vergroten, moeten de veiligheidsdiensten nauwer samenwerken. Dit 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 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.

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.

Daarom moeten 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 denktanks 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.

En Belgique, la coordination et la concertation entre les services de renseignement et d'intervention sont assurées au sein du Comité de coordination du renseignement et de la sécurité (CCRS), un mécanisme unique en son genre, même au niveau mondial. Pour pouvoir faire face au problème de l'ingérence politique étrangère, il faut également adopter une approche globale, étant donné que cette question se manifeste à différents niveaux, du niveau local jusqu'au niveau international. Il est crucial d'impliquer les pouvoirs locaux pour pouvoir relever efficacement ce défi. Par analogie avec l'exemple français, il est capital de délimiter le champ d'action des services de renseignement (et donc aussi de la Cellule de traitement des informations financières (CTIF)) avec la plus grande précision et de définir celui-ci de manière approfondie.

Pour accroître l'efficacité, il faut une coopération plus étroite entre les services de sécurité, afin de faire en sorte que les résultats et les conclusions des groupes de travail qui existent sous les auspices du Comité stratégique du renseignement et de la sécurité (CSRS) et qui rassemblent les parties prenantes deviennent plus concrets. Il est d'une importance cruciale d'améliorer le partage des informations et d'avoir une vue d'ensemble de la problématique. Cela renvoie au concept de l'approche pansociétale (*whole-society*), une nécessité pour prévenir toute ingérence. Il faut éviter la fragmentation et garantir absolument la cohérence entre les différentes stratégies de sécurité aux différents niveaux. Cela permettra d'identifier les secteurs vulnérables et les pays actifs et de lutter efficacement contre l'ingérence extérieure, la disponibilité des informations pertinentes étant une priorité.

Les pays européens doivent œuvrer conjointement afin de renforcer leurs propres influence et résilience face aux activités stratégiques de certaines puissances comme la Russie ou la Chine. La Chine tente d'influencer des mandataires politiques, de la majorité gouvernementale comme de l'opposition, aussi bien au niveau national qu'à l'échelle européenne. Elle vise des responsables politiques locaux, par le biais d'une diplomatie infranationale, et tente de recruter des leaders d'opinion, des journalistes et des membres de groupes de réflexion.

C'est pourquoi les pays européens doivent mettre en place des mécanismes afin de contrer l'influence indésirable d'acteurs étrangers. Cela implique des directives claires et des exigences de transparence pour les responsables politiques, les leaders d'opinion, les journalistes et les membres de groupes de réflexion en ce qui concerne leurs interactions et leurs sources financières. Une approche coordonnée pour surveiller et contrer la diffusion de récits spécifiques via des plateformes numériques doit être envisagée.

De internationale dreiging vereist een eensgezind internationaal en nationaal 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 VN, 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 worden betrokken.

Steven Coenegrachts (Open Vld)
Alexander De Croo (Open Vld)
Paul Van Tigchelt (Open Vld)
Kjell Vander Elst (Open Vld)

La menace internationale exige une réponse internationale et nationale unanime. Une collaboration permanente avec des organisations faîtières stratégiques est donc une nécessité. On peut, par exemple, intensifier la collaboration avec des organisations internationales existantes comme les Nations Unies, l'OTAN et l'Organisation pour la sécurité et la coopération en Europe (OSCE), en vue d'élaborer des initiatives conjointes visant à promouvoir la stabilité démocratique et à prévenir les ingérences. Cela implique aussi de développer des approches diplomatiques constructives au niveau tant national qu'européen auxquelles participent les responsables politiques aussi bien de la majorité gouvernementale que de l'opposition.

VOORSTEL VAN RESOLUTIE

De Kamer van volksvertegenwoordigers,

A. gelet op het informatieverslag van de Senaat (*Parl. St.*, Senaat, 2023-2024, DOC 7-344/2) ter bestrijding van de inmenging door buitenlandse mogendheden met het oog op het ondermijnen van de democratische rechtsstaat;

B. gelet op de door de Kamer van volksvertegenwoordigers aangenomen resolutie betreffende het efficiënt en effectief bestrijden van de buitenlandse inmenging en de ondermijning van onze democratie (*Parl. St.*, Kamer, 2022-2023, DOC 55 3045/007) van 11 mei 2023;

C. gelet op de *Cybersecurity Strategy Belgium* 2.0[7] 2021-2025 gepubliceerd in mei 2021 door het Centre for Cyber Security Belgium *(under the authority of the prime minister)*;

D. gelet op het rapport van Veiligheid van de Staat (VSSE) van 2024 dat waarschuwt voor de escalatie van hybride dreigingen in België en Europa[8];

E. gelet op het jaarverslag van de Algemene Dienst Inlichting en Veiligheid (ADIV) van 2024 dat een toename van hybride dreigingen en ontwrichtende technologieën vaststelt;

F. gelet op de organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten, waarin inmenging wordt omschreven als: “de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden” (artikel 8, 1°, g));

G. gelet op het nieuwe Boek II van het Strafwetboek (*Parl.St.*, Kamer, 2023-2024, DOC 55 3518/013). dat een aantal bepalingen bevat die handelingen strafbaar stellen die als buitenlandse inmenging kunnen worden beschouwd, meer bepaald de bepalingen van Titel 8 “Misdrijven tegen de Staat en zijn functioneren”, en in het bijzonder 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);

7 Cybersecurity Strategy Belgium 2.0, mei 2021 – Raadpleegbaar op: *https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf*

8 VVSE: *https://www.vsse.be/nl/intelligence-report-2024*

PROPOSITION DE RÉSOLUTION

La Chambre des représentants,

A. vu le rapport d’information du Sénat relatif à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l’État de droit démocratique (*Doc. parl.*, Sénat, 2023-2024, DOC 7-344/2);

B. vu la résolution relative à la lutte efficace et effective contre l’ingérence étrangère et la mise à mal de notre démocratie, adoptée par la Chambre des représentants (*Doc. parl.*, Chambre, 2022-2023, DOC 55 3045/007) du 11 mai 2023;

C. vu la Stratégie Cybersécurité Belgique 2.0 2021-2025[7], publiée en mai 2021 par le Centre for Cyber Security Belgium (sous l’autorité du premier ministre*)*;

D. vu le rapport de 2024 de la Sûreté de l’État (VSSE) qui met en garde contre l’escalade des menaces hybrides en Belgique et en Europe[8];

E. vu le rapport annuel du Service général du renseignement et de la sécurité (SGRS) de 2024, qui fait état d’une augmentation des menaces hybrides et des technologies disruptives;

F. vu la loi du 30 novembre 1998 organique des services de renseignement et de sécurité, qui définit l’ingérence comme “la tentative d’influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins” (article 8, 1°, g));

G. vu le nouveau Livre II du Code pénal (*Doc. parl.*, Chambre, 2023-2024, DOC 55 3518/013), dont certaines dispositions punissent des actes pouvant être considérés comme constitutifs d’une ingérence étrangère, notamment le Titre 8 “Les infractions contre l’État et son fonctionnement” et, en particulier, les articles 546 (acceptation d’une aide étrangère pour saper les intérêts nationaux essentiels), 573 (soutien à la politique ou aux objectifs de l’ennemi), 574 (ébranlement de la fidélité envers l’État) et 596 (communication d’informations essentielles erronées), ainsi que l’article 638 (corruption publique);

7 Stratégie Cybersécurité Belgique 2.0.2021-2025 – consultable sur: *https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_FR_DP2.pdf*

8 VSSE: *https://www.vsse.be/sites/default/files/vsse_intelligence_report_2024_fr.pdf*

H. gelet op 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));

I. gelet op 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));

J. gelet op 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));

K. gelet op 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));

L. gelet op de resolutie van het Europees Parlement van 25 april 2024 over de nieuwe beschuldigingen van Russische inmenging in het Europees Parlement en in de komende Europese verkiezingen en de gevolgen daarvan voor de Europese Unie (2024/2696(RSP));

M. gelet op het pakket maatregelen dat de Europese Commissie uitvaardigde ter verdediging van de democratie (COM(2023) 630 final);

N. gelet op het "strategisch kompas voor veiligheid en defensie" (Raad van de Europese Unie, 21 maart 2022, 7371/22);

O. gelet op het onderzoek van de het Amerikaanse Federal Bureau of Investigation (FBI) dat vaststelt dat inmengingsoperaties zich op verschillende manieren manifesteren[9];

VERZOEKT DE FEDERALE REGERING:

1. om – rekening houdend met de geopolitieke context – dringend een nieuw multidisciplinaire *Cybersecurity* Strategie 3.0 voor de periode 2026-2030 op te stellen;

2. om in te zetten op bewustmaking rond de risico's van inmenging op alle niveaus van elke organisatie waarbij een cruciale stap hierbij is het ontwikkelen door alle leden van de organisatie, ongeacht hun functie, niveau

[9] FBI: *https://media.defense.gov/2024/Feb/27/2.003.400.753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF*

H. vu la stratégie de cybersécurité et la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148));

I. vu la résolution du Parlement européen du 10 octobre 2019 sur l'ingérence électorale étrangère et la désinformation dans les processus démocratiques nationaux et européen (2019/2810(RSP));

J. vu la résolution du Parlement européen du 1er juin 2023 sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (2022/2075(INI));

K. vu la résolution du Parlement européen du 13 juillet 2023 sur des recommandations pour la réforme des règles du Parlement européen en matière de transparence, d'intégrité, de responsabilité et de lutte contre la corruption (2023/2034(INI));

L. vu la résolution du Parlement européen du 25 avril 2024 sur les nouvelles allégations d'ingérence russe au Parlement européen, dans les prochaines élections européennes, et incidence sur l'Union (2024/2696(RSP));

M. vu le train de mesures promulguées par la Commission européenne pour la défense de la démocratie (COM(2023) 630 final);

N. vu la "boussole stratégique en matière de sécurité et de défense" (Conseil de l'Union européenne, 21 mars 2022, 7371/22);

O. vu l'étude réalisée par le Federal Bureau of Investigation (FBI) des États-Unis qui constate que les opérations d'ingérence se manifestent de différentes manières[9];

DEMANDE AU GOUVERNEMENT FÉDÉRAL:

1. compte tenu du contexte géopolitique, d'élaborer d'urgence une nouvelle stratégie multidisciplinaire de cybersécurité 3.0 pour la période 2026-2030;

2. de poursuivre les efforts de sensibilisation aux risques d'ingérence à tous les niveaux de chaque organisation. Cela passe par une étape cruciale, à savoir le développement par chaque membre de l'organisation,

[9] FBI: *https://media.defense.gov/2024/Feb/27/2.003.400.753/-1/-1/0/CSA-Russian-Actors-Use-Routers-Facilitate-Cyber_Operations.PDF*

of graad, van een “situationeel bewustzijn” waarbij moet worden onderzocht wie manipuleert, met welke methoden en via welke actoren, evenals hoe we dit fenomeen en zijn impact kunnen meten;

3. om in samenwerking met de deelstaten en veiligheidsdiensten bewustmakingscampagnes op te zetten gericht op journalisten, mensenrechtenactivisten en andere potentiële doelwitten van spyware-aanvallen;

4. om concrete stappen, zoals frequente veiligheidsbriefings tijdens interacties met buitenlandse partners, systematisch te implementeren, om ons beter te beschermen tegen potentiële bedreigingen;

5. om de communicatie tussen de Veiligheid van de Staat (VSSE) en de academische, wetenschappelijke en politieke actoren te versterken, bijvoorbeeld via de oprichting van een adviesbureau dat de informatie van de verschillende overheidsdiensten kan samenbrengen om universiteiten te adviseren over de risico’s van bepaalde samenwerkingsverbanden;

6. om de versterking van de cybersecurity binnen de instellingen te ondersteunen;

7. om samen met de VSSE en alle bevoegdheidsniveaus aan het begin van elke zittingsperiode een briefing te organiseren om politieke mandatarissen bewust te maken van de mogelijke gevaren voor de veiligheid en de risico’s van inmenging;

8. om, vooral in verkiezingstijden, een gedragscode in te voeren voor politieke partijen en kandidaten;

9. 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. om een contactpunt tussen specifieke overheidsdiensten en de verenigingen van de diaspora op te richten dat bewustmakingsprogramma’s en programma’s voor media- en informatiegeletterdheid op maat ontwikkelt voor diasporagemeenschappen;

11. om middelen uit te trekken voor extra studies betreffende de detectie, de analyse en de weerbaarheid tegen de verspreiding van desinformatie, waarbij veiligheidsdiensten en universiteiten betrokken zijn;

quels que soient sa fonction, son niveau ou son grade, d’une “conscience situationnelle”, l’objectif étant d’analyser qui est derrière la manipulation, quelles sont les méthodes utilisées, qui sont les acteurs impliqués et comment le phénomène et son impact peuvent être quantifiés;

3. de mener, en collaboration avec les entités fédérées et les services de sécurité, des campagnes de sensibilisation à destination des journalistes, des militants des droits humains et d’autres cibles possibles sur les risques d’attaques menées au moyen de logiciels espions;

4. de mettre systématiquement en œuvre des mesures concrètes, telles que de fréquents briefings de sécurité lors d’interactions avec des partenaires étrangers, afin de mieux nous prémunir contre les menaces potentielles;

5. de renforcer la communication entre la Sûreté de l’État (VSSE) et les acteurs académiques, scientifiques et politiques, par exemple en mettant en place un bureau consultatif qui pourrait agréger les informations émanant des différents services publics pour éclairer les universités sur les risques de certaines collaborations;

6. de soutenir le renforcement de la cybersécurité au sein des institutions;

7. d’organiser au début de chaque mandature, conjointement avec la VSSE et l’ensemble des niveaux de pouvoir, un *briefing* de sensibilisation à la sécurité et aux risques d’ingérence à l’intention des mandataires politiques;

8. d’instaurer, en particulier en période électorale, un code de bonne conduite pour les partis politiques et les candidats;

9. d’organiser la contribution des citoyens à l’identification des risques d’ingérence, à l’instar du système de signalements via l’adresse de courriel “*suspect@safeonweb.be*”;

10. de créer un point de contact entre des services publics spécifiques et les associations des diasporas, qui développe des programmes de sensibilisation et d’éducation aux médias et à l’information à destination des diasporas;

11. de dégager des moyens pour mener de nouvelles études sur la détection et l’analyse de la désinformation ainsi que la résilience face à celle-ci, en veillant à y associer les services de sécurité et les universités;

12. om aan het Parlement een voorstel van wetswijziging voor te leggen om de bestaande lacunes in de huidige wetgeving over *lobbying* aanpakken;

13. om de administratieve en maatschappelijke kwetsbaarheden, nationale initiatieven en tegenmaatregelen, motieven en doelstellingen van de agressors, en de effecten van algoritmes te analyseren;

14. om in te zetten op de continue ontwikkeling van detectietechnieken van teksten die door *bots* zijn geschreven en artificieel gegenereerde beelden;

15. om hier, in overleg met de Gemeenschappen, permanent middelen en mensen op in te zetten;

16. om doelgericht potentiële actoren op het gebied van inmenging te onderzoeken, of het nu gaat om landen waarvan al is vastgesteld dat er sprake is van inmenging, bedrijven of diasporagemeenschappen;

17. om onderzoek te starten naar het ontwikkelen van duidelijke richtlijnen en criteria om een onderscheid te maken tussen binnenlandse actoren die bewust handelen in lijn met buitenlandse belangen en diegenen die simpelweg hun affiniteit uiten;

18. om onze nationale cybercapaciteit verder te ontwikkelen door de bestaande investeringen verder op te drijven en de samenwerking met partnerlanden te versterken om cybergerelateerde opleidingen te voorzien en expertise uit te wisselen;

19. om de aankoopprocedures en de procedure voor aanwerving van personeel voor de *Cyber Command* aan te passen opdat men autonomer, sneller en reactiever kan schakelen;

20. om repressief tegen buitenlandse informatieoperaties op te treden door met een vergelijkbaar initiatief als dat van de Europese Unie (EU) specifieke buitenlandse propagandakanalen te weren;

21. om een mechanisme op Europees niveau te ontwikkelen met betrekking tot een beter wettelijk kader en transparantie-eisen voor onlinecontent, die gerelateerd is aan politieke kwesties wat inhoudt dat platforms sociale media-accounts en advertenties moeten identificeren die betrokken zijn bij beïnvloedingsoperaties;

22. om een wachttijd bij het aanwerven van politici, topambtenaren en andere leidinggevenden door buitenlandse (overheids-)bedrijven, te combineren met strengere transparantieregels en de openbaarmaking van deze samenwerkingsverbanden;

12. de soumettre au Parlement une proposition de modification de loi en vue de remédier aux lacunes existant dans les lois actuelles sur le *lobbying*;

13. d'analyser les vulnérabilités administratives et sociétales, les initiatives et contre-mesures nationales, les motivations et objectifs des agresseurs et les effets des algorithmes;

14. de promouvoir le développement continu des techniques permettant de détecter les textes écrits par des robots et les images générées par intelligence artificielle;

15. d'y affecter en permanence des moyens matériels et humains, en concertation avec les Communautés;

16. de procéder à une analyse ciblée des potentiels acteurs d'ingérence, que ce soient des pays déjà reconnus pour leur ingérence, des entreprises ou des communautés de la diaspora;

17. de mener des études afin d'élaborer des directives et critères clairs permettant de distinguer les acteurs nationaux agissant délibérément dans l'intérêt d'acteurs étrangers de ceux qui ne font qu'exprimer leurs affinités;

18. de poursuivre le développement de notre cybercapacité nationale en accroissant les investissements existants et en renforçant la coopération avec les pays partenaires afin d'organiser des formations en cybernétique et d'échanger les expertises;

19. d'adapter les procédures d'achat et la procédure de recrutement de personnel pour le C*yber Command* afin de gagner en autonomie, en vitesse et en réactivité;

20. de prendre une initiative similaire à celle de l'Union européenne (UE) pour interdire certains canaux spécifiques de propagande étrangère afin de lutter contre les opérations d'information étrangères;

21. de développer, au niveau européen, un mécanisme en vue d'améliorer le cadre légal et de fixer des exigences de transparence pour les contenus en ligne relatifs à des questions politiques, ce qui suppose que les plateformes soient tenues d'identifier les comptes de médias sociaux et les publicités en lien avec des opérations d'influence;

22. de combiner un délai de carence dans l'embauche de responsables politiques, de hauts fonctionnaires et d'autres dirigeants par des entreprises (publiques) étrangères à des règles de transparence plus strictes et à la publication de ces partenariats;

23. om transparantie aan de dag te leggen omtrent financiële belangen van politieke mandatarissen en openbare ambten door eventuele belangenconflicten openbaar te maken;

24. om voor politieke mandatarissen, leden van de regering en (hoge) openbare ambtenaren transparantieregisters en heldere en afdwingbare deontologische richtlijnen uit te werken inzake vergoedingen, reizen, etentjes, cadeaus, enzovoort en in die richtlijnen onder meer een meldingsplicht voor buitenlandse contacten op te nemen alsook een register waarin relatiegeschenken en zelfs gratis reizen worden genoteerd;

25. om deze regels ook zo veel mogelijk met de parlementen en instanties van het land op elkaar af te stemmen, met eerbiediging van de autonomie van de parlementen en de deelstaten;

26. om kwetsbare technologieën op te sporen en de bescherming ervan aan te scherpen, zonder daarbij de internationale samenwerking op het gebied van onderzoek en ontwikkeling te ondermijnen;

27. om aan te dringen op een verbeterde transparantie met betrekking tot de financiering van niet-gouvernementele organisaties (ngo's), verenigingen zonder winstoogmerk (vzw's) en andere organisaties wat kan worden bereikt door wettelijke vereisten voor gedetailleerde openbaarmaking van financieringsbronnen en -bedragen in jaarverslagen en andere relevante documenten;

28. om juridische acties tegen buitenlandse inmenging te treffen door de relevante diensten een duidelijk mandaat te geven om met de uitdaging van buitenlandse inlichtingenoperaties om te gaan;

29. om de relevante diensten uit te rusten met de benodigde juridische bevoegdheden om strenger en doortastender op te treden en 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;

30. na te gaan of de nieuwe regelgeving inzake inmenging en beïnvloeding voldoende waarborgen biedt om een doeltreffende aanpak en sanctionering te waarborgen;

31. om op korte termijn een grondig onderzoek te starten om een helder standpunt in te nemen over de toepassing van internationaal recht in cyberspace om België aldus in staat te stellen om het internationale kader mede vorm te geven en om waardevolle inzichten te leveren;

23. de garantir la transparence en ce qui concerne les intérêts financiers des mandataires politiques et des fonctions publiques en dévoilant publiquement les éventuels conflits d'intérêts;

24. d'élaborer, pour les mandataires politiques, les membres du gouvernement et les membres de la (haute) fonction publique, des registres de transparence et des directives déontologiques claires et contraignantes en matière d'indemnités, de voyages, de repas, de cadeaux, etc., en les assortissant d'une obligation de signalement de contacts étrangers bien définis, ainsi qu'un registre des cadeaux d'affaires et même des voyages offerts;

25. de veiller à harmoniser ces règles au maximum entre les parlements et instances du pays, dans le respect de l'autonomie des parlements et des entités fédérées;

26. d'identifier les technologies sensibles et de renforcer leur protection, tout en veillant à ne pas nuire à la collaboration internationale en matière de recherche et développement;

27. d'insister sur une transparence accrue en ce qui concerne le financement des organisations non gouvernementales (ONG), associations sans but lucratif (ASBL) et autres organisations, ce qui peut être réalisé par le biais d'exigences légales relatives à une divulgation détaillée des sources et montants de financement dans les rapports annuels et autres documents pertinents;

28. de mener des actions juridiques contre l'ingérence étrangère en donnant un mandat clair aux services appropriés afin de relever efficacement le défi que posent les opérations de renseignement étrangères;

29. de doter ces services des compétences juridiques nécessaires pour pouvoir agir avec rigueur et détermination et de rationaliser le processus de passage d'un "dossier de renseignement" à un "dossier judiciaire", de sorte que la transition se déroule sans accroc dès que des preuves suffisantes d'une infraction ont été collectées;

30. de vérifier si la nouvelle réglementation en matière d'ingérence et d'influence offre des garanties suffisantes pour assurer l'efficacité de l'approche et des sanctions;

31. de lancer à court terme une étude approfondie en vue de l'adoption d'une position claire concernant l'application du droit international dans le cyberespace afin de permettre à la Belgique de participer à la concrétisation du cadre international et d'y apporter une contribution précieuse;

32. om de inlichtingendiensten financieel en vormelijk te versterken, zowel inzake personeelssterkte als inzake werkmiddelen en tevens te investeren in het versterken van *counterintelligence* (CI)-capaciteiten en de veiligheidsdiensten;

33. om de prioriteiten te heroriënteren door de recente focus op terrorismebestrijding aan te vullen en tegelijkertijd om te gaan met opkomende bedreigingen zoals contraspionage;

34. om een grondige evaluatie uit te voeren van de specifieke behoeften voor het bestrijden van nieuwe vormen van inmenging die gebruikmaken van sociale media, artificiële intelligentie en spywaretechnologieën;

35. om de wervingsprocedures nauwer af te stemmen op de unieke eisen en gevoeligheden van de diverse functies binnen elk veiligheidsorgaan;

36. om een nauwere samenwerking te stimuleren tussen technologiebedrijven, die na screening (of via een federaal bestek) als "veilig" worden bestempeld, alsook met cybersecurity-experts en overheidsinstanties om voortdurend de nieuwste spyware-technologieën en -methoden te monitoren en tegen te gaan;

37. om via Buitenlandse Zaken een duidelijk signaal uit te sturen naar de betrokken landen dat de inzet van spyware in België niet wordt geduld;

38. om samen met internationale organisaties en andere regeringen druk uit te oefenen op ondernemingen die spyware ontwikkelen en verkopen om te zorgen voor de transparantie en juridische aansprakelijkheid van deze bedrijven;

39. om samen met de Gemeenschappen ruimte te geven aan initiatieven die helpen om desinformatie en complottheorieën die worden aangestuurd via buitenlandse inmenging, te counteren en te debunken, onder meer via factchecks en betrouwbare bronnen (*credible voices*);

40. om nauwer internationaal samen te werken met de Europese instanties door met een Europees kader

32. de renforcer financièrement et formellement l'appareil de renseignement, tant sur le plan de la capacité en personnel que sur celui des ressources de travail, et d'investir aussi dans le renforcement de la capacité de contre-renseignement (CI) et dans les services de sécurité;

33. de réorienter les priorités en soutenant davantage la lutte contre le terrorisme, qui bénéficie depuis peu d'une attention prioritaire, et en faisant face aussi aux menaces émergentes telles que le contre-espionnage;

34. de procéder à une évaluation approfondie des besoins spécifiques pour faire face aux formes nouvelles d'ingérence facilitées par les réseaux sociaux, l'intelligence artificielle et les technologies *spyware*;

35. de faire en sorte que les procédures d'engagement de personnel prennent davantage en compte les exigences et les sensibilités propres des différentes fonctions au sein de chaque organe de sécurité;

36. de mettre en place une collaboration plus étroite entre les entreprises technologiques, identifiées après *screening* (ou par un cahier des charges fédéral) comme des entreprises "sûres", les experts en cybersécurité et les instances publiques afin de pouvoir garantir une surveillance permanente des technologies et des méthodes les plus récentes en matière de logiciels espions et ainsi de lutter contre elles;

37. d'adresser, par le biais des Affaires étrangères, un signal clair aux pays impliqués pour leur notifier que le déploiement de tels logiciels espions n'est pas toléré en Belgique;

38. d'exercer, conjointement avec des organisations internationales et d'autres gouvernements, des pressions sur les entreprises qui développent et vendent les logiciels espions afin de garantir la transparence et de les rendre responsables juridiquement;

39. de laisser l'espace nécessaire, conjointement avec les Communautés, pour le développement d'initiatives qui contribuent à contrer et à démystifier la désinformation et les théories du complot pilotées depuis l'étranger, notamment en procédant à la vérification des faits et en faisant appel à des sources fiables (*credible voices*);

40. de collaborer plus étroitement au niveau international avec les instances européennes afin de prévenir

inmenging te voorkomen en de strategische belangen van Europa en elke lidstaat te beschermen.

13 maart 2025

Steven Coenegrachts (Open Vld)
Alexander De Croo (Open Vld)
Paul Van Tigchelt (Open Vld)
Kjell Vander Elst (Open Vld)

des ingérences et de protéger les enjeux stratégiques de l'Europe et de chacun des États membres par le biais d'un cadre européen.

13 mars 2025

Centrale drukkerij - Imprimerie centrale