SÉNAT DE BELGIQUE

SESSION DE 2023-2024

22 MARS 2024

Rapport d'information relatif à la lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique

CONSTATATIONS ET RECOMMANDATIONS
ADOPTÉES PAR LA COMMISSION DU RENOUVEAU DÉMOCRATIQUE, DE LA CITOYENNETÉ ET DES AFFAIRES INTERNATIONALES

Voir:
Documents du Sénat:
7-344 – 2021/2022:
N° 1: Demande d'établissement d'un rapport d'information.

7-344 – 2023/2024:
N° 2: Rapport.

7-344/3

BELGISCHE SENAAT

ZITTING 2023-2024

22 MAART 2024

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

VASTSTELLINGEN EN AANBEVELINGEN
AANGENOMEN DOOR DE COMMISSIE VOOR DE DEMOCRATISCHE VERNIEUWING, BURGERSCHAP EN INTERNATIONALE AANGELEGENHEDEN

Zie:
Documenten van de Senaat:
7-344 – 2021/2022:
Nr. 1: Verzoek tot het opstellen van een informatieverslag.

7-344 – 2023/2024:
Nr. 2: Verslag.

PARTIE I: CONSTATATIONS

I. CADRE LÉGAL

A. Réglementation internationale et européenne

1. La Convention de Vienne du 18 avril 1961 sur les relations diplomatiques prévoit explicitement en son article 41.1 que les diplomates étrangers ont le devoir de ne pas s'immiscer dans les affaires intérieures de l'État accréditaire (1).

2. Il est important de mentionner 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) nº 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2).

   Le règlement européen (UE) 2022/2065 du Parlement européen et du Conseil du 19 octobre 2022 relatif à un marché unique des services numériques et modifiant la directive 2000/31/CE (règlement sur les services numériques) contient des éléments pour lutter contre la désinformation et la manipulation de l'information. Les principaux fondements à cet égard sont la transparence et la responsabilité. Le règlement doit être lu conjointement avec le code de bonnes pratiques 2022 en matière de désinformation (2).

3. Le Parlement européen a décidé, le 10 mars 2022, de constituer une commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne (UE), y compris la désinformation, et sur le renforcement de l'intégrité, de la transparence et de la responsabilité au Parlement européen (ING2) (3).

   Les travaux de la commission ING2 du Parlement européen ont abouti à l'adoption, entre autres, des deux textes suivants:

   – 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 (2022/2275(INI));

(1) Dr Luca Ferro, professeur adjoint en droit international, *Vrije Universiteit Brussel*.
(2) M. Lutz Güllner, *Head of Strategic Communications*, *European External Action Service* (EEAS).
(3) M. Dirk Janvier, commissaire divisionnaire, Service général du renseignement et de la sécurité (SGRS).

DEEL I: VASTSTELLINGEN

I. WETTELIJK KADER

A. Internationale en Europese regelgeving

1. Het Verdrag van Wenen van 18 april 1961 inzake diplomatiek verkeer geeft expliciet aan, in artikel 41.1, dat buitenlandse diplomaten de plicht hebben om zich niet te mengen in de binnenlandse aangelegenheden van de ontvangende staat (1).

2. Vermeldenswaard is richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van verordening (EU) nr. 910/2014 en richtlijn (EU) 2018/1972 en tot intrekking van richtlijn (EU) 2016/1148 (NIS2-richtlijn).

   De Europese verordening (EU) 2022/2065 van het Europees Parlement en de Raad van 19 oktober 2022 betreffende een eengemaakte markt voor digitale diensten en tot wijziging van richtlijn 2000/31/EG (de digitaledienstenverordening) bevat elementen om desinformatie en informatiemanipulatie aan te pakken. De belangrijkste uitgangspunten zijn transparantie en verantwoording. De verordening moet samen gelezen worden met de praktijkcode 2022 inzake desinformatie (2).

3. Het Europees Parlement heeft op 10 maart 2022 beslist om een bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie (EU), met inbegrip van desinformatie, en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), in te stellen (3).

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

   – de resolutie van het Europees Parlement van 1 juni 2023 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2022/2075(INI));

(1) dr. Luca Ferro, *assistant professor* internationaal recht, Vrije Universiteit Brussel.
(2) De heer Lutz Güllner, *Head of Strategic Communications*, *European External Action Service* (EEAS).
(3) De heer Dirk Janvier, afdelingscommissaris, Algemene Dienst inlichting en veiligheid (ADIV).

– 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)).

4. La Commission européenne a promulgué un paquet de mesures pour la défense de la démocratie (COM(2023) 630 final). Ce paquet contient aussi une recommandation sur la transparence du financement de la vie politique, car l'un des plus grands dangers d'ingérence étrangère est bien sûr le financement de partis politiques par des pays comme la Russie ou la Chine. Au niveau de l'UE, aucune mesure ne peut être prise à ce sujet puisqu'il s'agit d'une compétence nationale. Tout au plus peut-on formuler des recommandations européennes (4).

B. Réglementation nationale

5. Selon le Dr Luca Ferro, professeur adjoint en droit international à la *Vrije Universiteit Brussel*, le législateur national est libre d'adopter des lois qui empêchent, par exemple, le financement étranger de campagnes politiques, ou qui imposent un devoir de transparence aux lobbyistes, par analogie avec le *Foreign Agents Registration Act* aux États-Unis. L'orateur indique que rien n'empêche la Belgique d'opter, dans un cadre européen ou non, pour une législation plus stricte que celle prévue par le droit international tant que cela n'enfreint pas les réglementations internationales applicables.

6. La loi organique des services de renseignement et de sécurité du 30 novembre 1998 définit l'ingérence comme «la tentative d'influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins» (art. 8, 1° g)) (5).

7. Selon Kenneth Lasoen, *lector intelligence and security* au Département de Sciences politiques de l'*Universiteit Antwerpen*, il est indispensable de se pencher (plus avant) sur les brèches et les lacunes existant dans les lois actuelles sur le *lobbying*, les vulnérabilités administratives et sociétales, les initiatives et contremesures nationales, les motivations et objectifs des agresseurs et les effets des algorithmes.

(4) M. Raphaël Kergueno, *senior policy officer*, *Transparency International EU.*

(5) M. Dirk Janvier, commissaire divisionnaire, SGRS.

– de resolutie van het Europees Parlement van 13 juli 2023 over aanbevelingen voor de hervorming van de regels van het Europees Parlement inzake transparantie, integriteit, verantwoordingsplicht en corruptiebestrijding (2023/2034(INI)).

4. De Europese Commissie vaardigde een pakket maatregelen uit ter verdediging van de democratie (COM(2023) 630 final). Het pakket bevat ook een aanbeveling over de transparantie van de financiering van het politieke leven want één van de grootste gevaren van buitenlandse inmenging is uiteraard de financiering van politieke partijen door landen als Rusland of China. Hierover kunnen evenwel geen maatregelen worden genomen door de EU, omdat dit een nationale bevoegdheid betreft. Er kunnen dus hoogstens Europese aanbevelingen geformuleerd worden op dat vlak (4).

B. Nationale regelgeving

5. Volgens de heer Luca Ferro, *assistant professor* internationaal recht aan de Vrije Universiteit Brussel, staat het de nationale regelgever vrij om wetten aan te nemen die bijvoorbeeld de buitenlandse financiering van politieke campagnes aan banden leggen, of die een transparantieplicht opleggen aan lobbyisten naar analogie van de *Foreign Agents Registration Act* in de Verenigde Staten (VS). De spreker stelt dat niets verhindert dat België, al dan niet in EU verband, opteert voor een striktere wetgeving dan wat internationaalrechtelijk van toepassing is, zolang daarmee de geldende internationale voorschriften niet worden overtreden.

6. De organieke wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten omschrijft inmenging als: «de poging om met ongeoorloofde, bedrieglijke of clandestiene middelen beslissingsprocessen te beïnvloeden» (art. 8, 1° g)) (5).

7. Volgens de heer Kenneth Lasoen*, lector intelligence and security*, Departement Politieke Wetenschappen aan de Universiteit Antwerpen, is er nood aan (extra) analyse van de bestaande achterpoortjes en de tekortkomingen van huidige lobbywetten, van bestuurlijke en maatschappelijke kwetsbaarheden, van nationale initiatieven en tegenmaatregelen, van de motieven en doelen van de agressoren en van de effecten van algoritmes.

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

(5) De heer Dirk Janvier**,** afdelingscommissaris, ADIV.

8. Des initiatives législatives ont été prises, notamment la loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité (la loi MRD) et davantage de moyens ont aussi été débloqués. La Sûreté de l'État (VSSE) sera dotée d'effectifs qui s'élèveront à terme à mille personnes et le Service général du renseignement et de la sécurité (SGRS) a lancé récemment le *Cyber Command*. La situation des services s'est améliorée et cela porte clairement ses fruits: le *Qatargate* en est une belle illustration (6).

9. Le nouveau livre II du Code pénal (doc. Chambre, nº 55 3518/013) contient certaines dispositions qui incriminent des faits pouvant relever de manœuvres d'ingérence étrangère. Il s'agit notamment des dispositions du titre 8 «Les infractions contre l'État et son fonctionnement» et plus particulièrement des articles 546 (l'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), de même que de l'article 638 (corruption publique).

C. Répartition des compétences en Belgique

10. En ce qui concerne la délimitation de la matière, la VSSE n'utilise pas le terme «influence». Le terme «ingérence» par contre est clairement défini dans la loi régissant les compétences des services de renseignement, à savoir la loi du 30 novembre 1998 organique des services de renseignement et de sécurité (7).

11. Cette même loi définit clairement les missions des services concernés. Le SGRS fait des constatations et reçoit des informations: si celles-ci s'inscrivent dans le cadre de ses missions, une enquête peut être lancée. Les enquêtes peuvent avoir pour conséquence par exemple que la justice est saisie, que des habilitations de sécurité sont retirées, etc. En principe, le service décide en toute autonomie des enquêtes à mener, pour autant que celles-ci relèvent de sa mission. Le service est évidemment placé sous le contrôle du Comité permanent R, qui dispose à tout moment d'un droit de regard dans les enquêtes en cours, peut commenter celles-ci ou formuler des recommandations si nécessaire (8).

(6) M. Kristof Clerix, journaliste d'investigation, *Knack*.
(7) M. Peter Lanssens, directeur de l'analyse, Sûreté de l'État (VSSE).
(8) M. Dirk Janvier, commissaire divisionnaire, SGRS.

8. Er werden wetgevende initiatieven genomen, onder meer de wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (de BIM-wet), en er werden meer middelen vrijgemaakt. De Veiligheid van de Staat (VSSE) zit op een groeipad richting duizend effectieven en de Algemene Dienst inlichting en veiligheid (ADIV) lanceerde onlangs het *Cyber Command*. De diensten staan er beter voor en dit werpt heel zeker vruchten af: *Qatargate* is hier een mooie illustratie van (6).

9. Het nieuwe boek II van het Strafwetboek (doc. Kamer, nr. 55 3518/013) bevat een aantal bepalingen die handelingen strafbaar stellen die als buitenlandse inmenging kunnen worden beschouwd. Het betreft de bepalingen van titel 8 «Misdrijven tegen de Staat en zijn functioneren», en meer bepaald de artikelen 546 (aanvaarding van buitenlandse steun aan ondermijning van de essentiële nationale belangen), 573 (steun aan de politiek of doelstellingen van de vijand), 574 (aan het wankelen brengen van de trouw aan de Staat) en 596 (verstrekken van foute essentiële informatie) alsook artikel 638 (publieke omkoping).

C. Bevoegdheidsverdeling in België

10. Ten dienste van de afbakening van de materie maakt de VSSE geen gebruik van de term «beïnvloeding». De term «inmenging» is duidelijk gedefinieerd in de wet die de bevoegdheden van de inlichtingendiensten regelt, namelijk de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten (7).

11. Dezelfde wet bepaalt de opdrachten van de betrokken diensten. De ADIV doet vaststellingen en ontvangt informatie: als deze kaderen binnen hun opdracht, kan een onderzoek worden opgestart. De onderzoeken kunnen ervoor zorgen dat bijvoorbeeld het gerecht wordt ingeschakeld, dat veiligheidsmachtigingen worden ingetrokken, enz. In principe bepaalt de dienst autonoom welke onderzoeken er gevoerd worden zolang ze binnen de opdracht passen. De dienst valt uiteraard onder de controle van het Vast Comité I dat ten allen tijde inzage kan krijgen in de lopende onderzoeken, deze kan becommentariëren of aanbevelingen doen indien nodig (8).

(6) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.
(7) De heer Peter Lanssens, directeur van de Analyse, Veiligheid van de Staat (VSSE).
(8) De heer Dirk Janvier, afdelingscommissaris, ADIV.

12. La Cellule de traitement des informations financières (CTIF) est une instance active en matière de prévention du blanchiment de capitaux et du financement du terrorisme. Elle ne peut pas, par exemple, demander à ses analystes de lancer une enquête sur la base d'un article de presse. La CTIF doit nécessairement travailler sur la base d'un rapport établi soit par les entités assujetties visées par la loi, soit par les services administratifs de l'État, ainsi que par le ministère public dans une certaine mesure lorsqu'il s'agit de terrorisme. La cellule peut également agir dans le cas où elle est saisie par une autorité étrangère équivalente: il en existe environ cent soixante dans le monde (9).

13. Les compétences des Régions ne sont actuellement pas mobilisées dans la gestion des ingérences.

14. En principe, le SGRS ne se concerte pas avec les gouverneurs (10).

15. Quant aux contacts avec les services de police, il existe notamment une interaction efficace entre la VSSE et les services de la police locale via les *task forces* locales. On s'appuie entre autres sur un *information officer* qui est la personne de contact direct du bourgmestre. Cela permet une circulation efficace de l'information (11).

16. En ce qui concerne la communication entre les différents services de police, certains mécanismes permettent l'échange de nombreuses informations, particulièrement en matière de terrorisme, et il existe également une collaboration en la matière au sein de l'*Agile Task Force Information Operations* (ATFIO) (12) (qui a été remplacée depuis par d'autres partenariats ayant la même structure).

    La mise en place d'un *information officer* comme personne de contact direct du bourgmestre permet une circulation efficace de l'information, de même que les forums contre-terrorisme (13) (c'est-à-dire des réunions rassemblant tous les partenaires de sécurité au niveau de l'arrondissement).

(9) M. Philippe de Koster, président, Cellule de traitement des informations financières (CTIF).
(10) M. Dirk Janvier, commissaire divisionnaire, SGRS.
(11) M. Peter Lanssens, directeur de l'analyse, VSSE.
(12) M. Dirk Janvier, commissaire divisionnaire, SGRS.
(13) Rapport annuel de la Sûreté de l'État, 2019, p. 18.

12. De Cel voor financiële informatieverwerking (CFI) is een instantie die zich actief bezighoudt met het voorkomen van het witwassen van geld en de financiering van terrorisme. Zij kan bijvoorbeeld haar analisten niet vragen een onderzoek in te stellen op basis van een persartikel. Het CFI kan alleen werken op basis van een verslag dat is opgesteld, hetzij door de onderworpen entiteiten, hetzij door de administratieve diensten van de Staat, en tot op zekere hoogte ook door het openbaar ministerie als het gaat om terrorisme. De Cel kan ook optreden in het geval van een verwijzing door een vergelijkbare buitenlandse autoriteit. Er er zijn ongeveer honderdzestig van dergelijke eenheden in de wereld (9).

13. De Gewesten zijn momenteel niet betrokken bij de aanpak van inmenging.

14. De ADIV gaat in principe niet in overleg met gouverneurs (10).

15. Wat de contacten met de politiediensten betreft, is er onder andere een effectieve interactie tussen de VSSE en de lokale politie via de Lokale Taskforces. Hierbij wordt onder meer een beroep gedaan op een *information officer*, die het directe aanspreekpunt voor de burgemeester is. Op die manier wordt er een efficiënte informatiestroom gegarandeerd (11).

16. Voor wat betreft de communicatie tussen de verschillende politiediensten onderling, zijn er zeker op het vlak van terrorisme mechanismen in werking waar veel informatie wordt uitgewisseld, ook in de *Agile Taskforce Information Operations* (ATFIO) (dat intussen weliswaar is vervangen door andere samenwerkingsverbanden met hetzelfde opzet) bestaat er een samenwerking op dat vlak (12).

    De invoering van *information officers* als rechtstreeks aanspreekpunt voor de burgemeester zorgt voor een efficiënte informatiedoorstroom, net als de antiterrorismeforums (13): vergaderingen met alle veiligheidspartners op arrondissementsniveau.

(9) De heer Philippe de Koster, voorzitter, Cel voor financiële informatieverwerking (CFI).
(10) De heer Dirk Janvier, afdelingscommissaris, ADIV.
(11) De heer Peter Lanssens, directeur van de Analyse, VSSE.
(12) De heer Dirk Janvier, afdelingscommissaris, ADIV.
(13) Jaarrapport van de Veiligheid van de Staat, 2019, blz. 18.

II. DISCUSSION GÉNÉRALE

A. Ingérence étrangère visant à saper l'état de droit démocratique

1) Définition

17. Il est compliqué de formuler une définition de «l'ingérence étrangère»: il peut s'agir d'États étrangers, de citoyens étrangers ou d'intérêts étrangers.

Des opérations d'ingérence 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 notion de *soft power* joue ici un rôle central. Dans les opérations d'ingérence, il n'est pas question de contrainte à proprement parler, mais plutôt d'actes de persuasion qui influencent le comportement politique (14).

18. 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, destinés à saper la cohésion interne et à renforcer la polarisation politique. Il s'agit d'une manipulation clandestine des intérêts stratégiques d'autres États. L'expression «interférence hybride» doit être clairement distinguée 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 (15).

19. 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 (ING2), 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 (16).

(14) Mme Sofia Collignon, *lecturer* (professeure adjointe), *School of politics and IR*, *Queen Mary University of London*.
(15) M. Dirk Janvier, commissaire divisionnaire, SGRS.
(16) M. Dirk Janvier, commissaire divisionnaire, SGRS.

II. ALGEMENE BESPREKING

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

1) Definitie

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

Inmengingsoperaties zijn handelingen die erop gericht zijn buitenlandse belangen te bevorderen door de onrechtmatige inzet van *soft power* om de integriteit van politieke processen en gedragingen te corrumperen. Het begrip *soft power* staat centraal. Bij inmengingsoperaties gaat het niet echt om dwang, maar meer om overtuigingshandelingen die het politieke gedrag beïnvloeden (14).

18. De Noord-Atlantische Verdragsorganisatie (NAVO) hanteert veeleer de term *hybrid interference* waarmee verwezen wordt 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 onderscheiden worden van *hybrid warfare*, dat als een militaire benadering moet beschouwd worden. Drie instrumenten staan centraal in *hybrid interference*: clandestiene diplomatie, geo-economie en desinformatie (15).

19. Het besluit van het Europees Parlement van 10 maart 2022 over de instelling van een bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (ING2) stelt dat inmenging gaat over kwaadwillende en autoritaire buitenlandse overheids- en niet-overheidsactoren die gebruikmaken van manipulatie van informatie en andere tactieken om zich in democratische processen in de EU te mengen. Het uiteindelijke doel is de Europese democratie te destabiliseren (16).

(14) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*
(15) De heer Dirk Janvier**,** afdelingscommissaris, ADIV.
(16) De heer Dirk Janvier**,** afdelingscommissaris, ADIV.

20. 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. Le schéma énonce un système de gradation allant de l'influence transparente sur l'opinion publique aux opérations paramilitaires entraînant la mort de personnes. Il couvre donc tout un spectre de formes d'ingérence. Il importe de définir clairement les concepts. Influence n'est pas synonyme d'ingérence. La frontière est floue entre l'influence légitime et la manipulation illicite (17).

21. L'influence légitime et l'ingérence illégitime sont les deux pôles conceptuels d'un spectre d'activités similaires. De plus, déterminer ce qui est légitime est en soi intrinsèquement politique (18).

22. 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. La transparence et la publicité font place à des actes dissimulés, trompeurs, coercitifs, ou même corrupteurs. Élément important, il s'agit en l'espèce non seulement d'acteurs étatiques, mais aussi d'acteurs non étatiques.

23. Un problème se pose lorsque les processus décisionnels sont influencés et que 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 (19).

(17) Les différents degrés d'ingérence sont clairement présentés dans un schéma. Voir: Kenneth Lasoen, «*Realising the EU Hybrid Toolbox: opportunities and pitfalls*», *Clingendael Policy Brief*, décembre 2022.
(18) Prof. Dr Alexander Mattelaer, *vice dean research*, *Brussels School of Governance*, *Vrije Universiteit Brussel.*
(19) Prof. Dr Alexander Mattelaer, *vice dean research*, *Brussels School of Governance*, *Vrije Universiteit Brussel.*

20. Er zijn gradaties van inmenging, zoals wordt geïllustreerd in het schematisch overzicht in een *Policy Brief* van het *Clingendael Institute* over de Europese initiatieven tegen inmenging. Het schema bevat een trappensysteem dat gaat van transparante beïnvloeding van de publieke opinie tot paramilitaire operaties waarbij mensen worden omgebracht. Dit toont aan dat er een volledig spectrum van vormen van inmenging bestaat. De begrippen moeten dus duidelijk afgebakend worden. Invloed is in alle geval geen synoniem voor inmenging. Er ligt een vage grens tussen legitieme beïnvloeding en ongeoorloofde manipulatie (17).

21. Rechtmatige invloed en onwettige inmenging zijn twee conceptuele polen in een spectrum van soortgelijke activiteiten. Bepalen wat rechtmatig is, is een intrinsiek politieke activiteit (18).

22. Invloed is normaal en maakt deel uit van de diplomatie. Het feit dat andere (private) actoren proberen om onze besluitvormingsprocessen in hun voordeel te beïnvloeden, maakt deel uit van de traditionele manier van zaken of handel doen. Er stelt zich geen probleem zolang dit legitiem gebeurt.

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

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

23. Inmenging is problematisch van zodra besluitvormingsprocessen worden beïnvloed en er gepoogd wordt om strategische economische processen te infiltreren en te manipuleren in het voordeel van de agressor en ten nadele van onze maatschappij en democratische waarden (19).

(17) De gradaties worden duidelijk geïllustreerd in een schema met een trappensysteem: zie *Realising the EU Hybrid Toolbox: opportunities and pitfalls* (December 2022, Kenneth Lasoen, *Clingendael Policy Brief*).
(18) Prof. Dr. Alexander Mattelaer, *vice dean research*, *Brussels School of Governance*, Vrije Universiteit Brussel.
(19) Prof. Dr. Alexander Mattelaer, *vice dean research*, *Brussels School of Governance*, Vrije Universiteit Brussel

Le phénomène fait partie de l'histoire des relations internationales. Certains pays emploient des expressions consacrées pour décrire ce phénomène: «l'option silencieuse», «la main cachée», «les projets spéciaux», «la guerre psychologique»; les Russes parlent de «mesures actives» (20).

2) Rôle d'amplification de l'intelligence artificielle

24. En ce qui concerne l'incidence potentielle d'un outil comme *ChatGPT* en matière de désinformation, il est précisé que l'intelligence artificielle (IA) est déjà largement utilisée aujourd'hui. Le système AIMS (*Advanced Impact Media Solutions*) proposé par l'entreprise «*Team Jorge*» mentionnée ci-dessous comporte une composante d'intelligence artificielle qui évite à l'utilisateur du système d'écrire lui-même des messages au nom des avatars: il suffit d'introduire quelques mots clés et de préciser le «ton» souhaité (neutre, négatif ou positif), et le système fait le reste. La création automatique de contenus est donc déjà une réalité (21).

25. Selon M. Raphaël Glucksmann, président de la commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, et sur le renforcement de l'intégrité, de la transparence et de la responsabilité au Parlement européen (ING2), l'intelligence artificielle 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»: c'est là le cœur du problème qu'il faut traiter (22). 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 M. Glucksmann juge peu vraisemblable que la recherche scientifique sur l'IA puisse être arrêtée.

26. Selon M. Maxime Lebrun, *deputy director – Research & Analysis*, *The European Centre of Excellence for Countering Hybrid Threats*, le fil conducteur de la discussion sur l'intelligence

(20) M. Kenneth Lasoen, *lector intelligence and security, D*épartement des Sciences politiques, *Universiteit Antwerpen*.

(21) M. Kristof Clerix, journaliste d'investigation, *Knack*.

(22) Le Sénat a, lui aussi, déjà eu l'occasion de se pencher sur le rôle de l'intelligence artificielle dans la production et la diffusion d'infox (*fake news*) (doc. Sénat, nº 7-110).

Inmenging maakt deel uit van de geschiedenis van de internationale betrekkingen. In verschillende landen bestaat er een ingeburgerde term om het fenomeen te omschrijven: «*the silent option*», «the hidden hand», «*special projects*», «psychologische oorlogsvoering»; de Russen hebben het bijvoorbeeld over «actieve maatregelen» (20).

2) Versterkende rol van artificiële intelligentie

24. Voor wat betreft de mogelijke impact van een tool als *ChatGPT* op vlak van desinformatie, wordt gesteld dat artificiële intelligentie (AI) nu al volop aan zet is. Het *Advance Impact Media Solutions* (AIMS)-systeem van het hieronder vermeld bedrijf «*Team Jorge»* heeft een *AI*-component die ervoor zorgt dat de gebruiker van het systeem zelf geen berichten meer hoeft te schrijven in naam van de avatars: een paar steekwoorden en een «toon» (neutraal, negatief, positief) voldoen: het systeem doet de rest. Content wordt dus zeker al automatisch gecreëerd (21).

25. Volgens de heer Raphaël Glucksmann, voorzitter van de bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie, en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), vormt artificiële intelligentie (AI) een zeer groot probleem voor onze democratieën. Er is nood aan reglementering, alsook aan controle en een vorm van traceerbaarheid. Het grote probleem van het genereren van beelden of klankfragmenten via artificiële intelligentie is dat dit productieproces «achter de schermen» gebeurt: dat is de kern van de problematiek die moet aangepakt worden (22). De suggestie vanwege sommige bekende figuren om tijdelijk de ontwikkeling van deze technologie stop te zetten, kan enig nut hebben omdat het ons wijst op de gevaren, maar de heer Glucksmann acht het niet echt waarschijnlijk dat het wetenschappelijk onderzoek op vlak van AI kan worden stopgezet.

26. Volgens de de heer Maxime Lebrun, *deputy director – Research & Analysis* in *The European Centre of Excellence for Countering Hybrid Threats*, is de rode draad in de discussie over artificiële intelligentie het

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

(21) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.

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

artificielle concerne la question de la gouvernance algorithmique. L'intelligence artificielle est un algorithme apprenant; elle implique des outils techniques qui lui permettent de calculer, d'agréger un énorme ensemble de données pour trouver une solution à un problème donné. La difficulté de la mise en place de la gouvernance algorithmique concerne le choix du secteur dans lequel elle s'applique. Il n'y aura pas de pause dans le développement de l'intelligence artificielle. Il ne peut y avoir d'interdiction de cette technologie, cela irait à l'encontre du sens de l'histoire et de l'évolution de la science et de la technologie. Selon M. Lebrun, il s'agit principalement d'un choix politique: il faut déterminer dans quels secteurs la réglementation des techniques algorithmiques est souhaitable ou non. Par exemple, la communication politique peut-elle être basée sur l'algorithmique? En d'autres termes, est-il éthique et souhaitable pour le débat démocratique de permettre l'utilisation de ce type d'outils par les partis politiques en période électorale? Par ailleurs, l'utilisation de l'intelligence artificielle dans des secteurs tels que la lutte contre le réchauffement climatique, l'urbanisme et la santé publique semble particulièrement utile et peut apporter des solutions aux grands problèmes de notre temps.

Selon M. Lebrun, ce n'est pas la régulation du contenu des messages qui est le cœur du problème – en dehors des messages illégaux, des appels à la haine ou des contenus non autorisés –, mais c'est plutôt un cadre réglementaire qu'il faut envisager pour éviter que les techniques algorithmiques ne faussent profondément le débat démocratique. Ceci vaut particulièrement pour les grandes plateformes et/ou les réseaux sociaux numériques. Il s'agit d'un choix politique visant à déterminer dans quels secteurs les outils algorithmiques sont souhaitables ou doivent être réglementés.

3) Manifestations d'ingérence étrangère

27. 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)) donne une vue d'ensemble des diverses formes d'ingérence étrangère et des points d'attention éventuels.

28. Selon le *Federal Bureau of Investigation* (FBI) américain, les opérations d'ingérence peuvent prendre les formes suivantes:

algoritmebeheer. AI is een zelflerend algoritme; het maakt gebruik van technologie om berekeningen te maken en om een groot aantal datasets met elkaar te vergelijken om zo een oplossing te vinden voor een gegeven probleem. De moeilijkheid in verband met beheerskaders voor algoritmen gaat over de keuze van de sector waarin ze van toepassing zijn. De ontwikkeling van artificiële intelligentie zal niet opgeschort worden; deze technologie kan niet verboden worden want dat zou ingaan tegen de loop van de geschiedenis en de ontwikkeling van wetenschap en technologie. Volgens de heer Lebrun, is het voornamelijk een politieke keuze: er moet bepaald worden in welke sectoren de regulering van algoritmebeheersingstechnieken al dan niet wenselijk is. Mag politieke communicatie bijvoorbeeld gebaseerd zijn op algoritmes? Met andere woorden: is het ethisch verantwoord en wenselijk voor het democratische debat dat dit soort van hulpmiddelen gebruikt worden door politieke partijen in de verkiezingsperiode? Overigens is het zo dat het gebruik van artificiële intelligentie in domeinen als de strijd tegen de klimaatopwarming, ruimtelijke ordening of volksgezondheid heel nuttig lijkt en oplossingen kan aanbrengen voor grote problemen waar we tegenwoordig mee geconfronteerd worden.

Volgens de heer Lebrun is het niet de regulering van de inhoud van de boodschappen die van belang is – behalve wanneer die inhoud onwettig is, zoals bij het oproepen tot haat of bij ongeoorloofde content – maar moet men veeleer een reglementair kader overwegen om te voorkomen dat de gebruikte algoritmen het democratisch debat grondig zouden vervalsen. Dat geldt in het bijzonder voor grote digitale platformen en/of sociale netwerken. Het gaat om een politieke keuze die erop gericht moet zijn te bepalen in welke sectoren het gebruik van algoritmen wenselijk is of aan reglementering dient te worden onderworpen.

3) Uitingen van buitenlandse inmenging

27. De resolutie van het Europees Parlement van 10 oktober 2019 over buitenlandse inmenging in verkiezingen en desinformatie in de nationale en Europese democratische processen (2019/2810(RSP)) schetst een overzicht van de verscheidenheid aan vormen van buitenlandse inmenging en van de mogelijke aandachtspunten.

28. Volgens het Amerikaanse *Federal Bureau of Investigation* (FBI) kunnen inmengingsoperaties zich als volgt manifesteren:

– tentatives criminelles en vue de saper le processus électoral et de mettre en place un financement illégal des campagnes électorales;

– cyberattaques contre l'infrastructure de vote, assorties de piratages informatiques visant entre autres des fonctionnaires élus, des résultats électoraux et des candidats aux élections. Pendant les auditions, Mme Sofia Collignon a évoqué un cas spécifique d'opération d'influence: les 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 (23).

a) Via la boucle OODA inversée

29. Au cours des auditions, il a été fait référence notamment au système qui repose sur l'inversion de la boucle OODA (observer, s'orienter, décider, agir), une technique éprouvée qui est surtout utilisée par les pilotes de chasse pour le ciblage.

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.

Les objectifs stratégiques sont les suivants:

– obtenir des informations sur la cible par des techniques d'espionnage, autrement dit en savoir plus sur la cible que celle-ci n'en sait sur elle-même; à cet effet, l'agresseur doit connaître parfaitement les faiblesses de la cible et les canaux nécessaires pour la manipuler;

– manipuler la prise de décision sur toute la ligne;

– saper les valeurs démocratiques (24).

b) Via des sociétés privées spécialisées dans la désinformation

30. 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

(23) Mme Sofia Collignon, *lecturer* (assistant professor), *School of politics and IR*, *Queen Mary University of London.*
(24) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen.*

– criminele pogingen om het stemmingsproces te ondermijnen en in illegale campagnefinanciering te voorzien;

– cyberaanvallen op de steminfrastructuur, samen met computerinbraken gericht op onder meer verkozen ambtenaren, verkiezingsuitslagen en verkiezingskandidaten. Tijdens de hoorzittingen werd er door mevrouw Sofia Collignon verwezen naar een specifieke beïnvloedingsoperatie: online desinformatiecampagnes die regelmatig worden gevoerd en bijdragen tot de verspreiding van verkeerde informatie met als doel de verkiezingsuitslag te beïnvloeden of de kwaliteit van het verkiezingsproces in twijfel te trekken (23).

a) Via de reverse *OODA-loop*

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

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

De gestelde strategische doelen zijn:

– inlichtingen over het doelwit verkrijgen via spionage, dat wil zeggen meer weten over het doelwit dan het doelwit over zichzelf weet. Hiervoor moet de agressor heel goed de kwetsbaarheden van het doelwit kennen alsook de nodige kanalen om het doelwit te kunnen manipuleren;

– besluitvorming manipuleren over de ganse lijn en

– democratische waarden ondermijnen (24).

b) Via in desinformatie gespecialiseerde privéondernemingen

30. Het *Pegasus*-project, opgezet door een journalistencollectief, onthulde dat journalisten en mensenrechtenactivisten wereldwijd het slachtoffer waren

(23) Mevrouw Sofia Collignon, *lecturer* (*assistant professor*), *School of politics and IR*, *Queen Mary University of London*.
(24) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

avaient été victimes du logiciel espion *Pegasus*, développé par la société israélienne *NSO Group*. Des victimes de ce logiciel ont été identifiées en Belgique également. C'est le cas, entre autres, de Carine Kanimba, fille de Paul Rusesabagina, le héros du film *Hôtel Rwanda*, qui a probablement été espionnée par le Rwanda, et d'El Mahjoub Maliha, un militant des droits de l'homme originaire du Sahara occidental, qui soupçonne le Maroc de l'avoir surveillé. Le logiciel en question permettait de prendre complètement le contrôle de smartphones à distance (25).

M. Kristof Clerix, journaliste d'investigation au *Knack*, suggère de diligenter des poursuites contre le déploiement en Belgique du logiciel espion *Pegasus*, de communiquer en toute transparence sur les enquêtes de renseignement et les enquêtes judiciaires menées sur ce logiciel et, par l'intermédiaire des Affaires étrangères, d'envoyer un signal clair aux pays impliqués pour leur notifier que le déploiement de tels logiciels espions n'est pas toléré en Belgique.

Story Killers, un projet international d'un collectif de journalistes visant à enquêter sur les organisations et entreprises spécialisées dans la manipulation de l'opinion publique et dans la diffusion de fausses informations, a prouvé, à son tour, que des opérations qui étaient auparavant organisées uniquement par des pays le sont désormais aussi pour et par des particuliers ou des entreprises:

– *Team Jorge*, par exemple, est un acteur privé, qui possède certes des racines dans l'armée israélienne; quiconque est capable de payer peut faire appel à lui;

– *NSO Group*, la société qui a développé *Pegasus*, collaborait uniquement avec des pouvoirs publics (26).

c) Via des acteurs politiques

31. L'ingérence peut également prendre la forme de subversion sociale et de tentatives illicites, par l'entremise de mandataires, de hauts fonctionnaires ou de groupes de pression, dans le but d'exercer une pression sur le processus décisionnel et la législation (27).

(25) M. Kristof Clerix, journaliste d'investigation, *Knack*.
(26) M. Kristof Clerix, journaliste d'investigation, *Knack*.
(27) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen*.

geworden van de *Pegasus-spyware*, ontwikkeld door de Israëlische *NSO Group*. Ook in België waren er slachtoffers van de software, onder meer Carine Kanimba, dochter van *Hotel Rwanda*-held Paul Rusesabagina, die vermoedelijk door Rwanda werd bespioneerd, en El Mahjoub Maliha, een mensenrechtenactivist afkomstig uit de Westelijke Sahara die er van uit gaat dat hij door Marokko werd gevolgd. De software in kwestie liet toe om vanop afstand de software van smartphones volledig over te nemen en te controleren (25).

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

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

– *Team Jorge* bijvoorbeeld is een privéspeler, weliswaar met roots in het Israëlische leger; het kan ingeschakeld worden voor éénieder die geld op tafel legt;

– *NSO Group*, het bedrijf achter *Pegasus*, werkte daarentegen enkel samen met overheden (26).

c) Via politieke actoren

31. Inmenging kan ook de vorm aannemen van maatschappelijke subversie en ongeoorloofde pogingen, via mandatarissen of hoge functionarissen of drukkingsgroepen, om druk uit te oefenen op de besluitvorming en de wetgeving (27).

(25) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.
(26) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.
(27) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

d) Via des associations et des institutions

32. 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 (28).

e) Via des Églises et groupements religieux

33. Dans le cadre de sa mission légale, la VSSE examine par exemple également les formes possibles d'influence illicites, frauduleuses ou clandestines 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 russe. En outre, 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 est le risque d'ingérence suivant la définition qu'en donne la loi organique des services de renseignement et de sécurité du 30 novembre 1998. La CTIF est un autre partenaire qui peut aussi être interrogé, car elle peut enquêter sur un éventuel financement en provenance d'un pays tiers (29).

f) Via des «influenceurs» ou des personnalités

34. Un autre moyen possible pour s'ingérer 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) (30).

g) Via des cyberattaques

35. En matière de tactiques et de techniques, il peut être 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

(28) M. Kenneth Lasoen, *lector intelligence and security,* Département de Sciences politiques, *Universiteit Antwerpen.*
(29) M. Peter Lanssens, directeur de l'analyse, VSSE.
(30) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen.*

d) Via verenigingen en instellingen

32. Een bekend voorbeeld is het Confuciusinstituut dat gefinancierd wordt door de Chinese overheid. Via activiteiten op universiteiten probeert het een gunstiger beeld van China te projecteren en tegelijk te infiltreren in de kenniseconomie waarbij het aast op de resultaten van R&D en/of leningen verstrekt onder bepaalde voorwaarden (28).

e) Via kerken en religieuze groeperingen

33. De VSSE onderzoekt in het kader van haar wettelijke opdracht met betrekking tot inmenging bijvoorbeeld ook mogelijke vormen van ongeoorloofde, bedrieglijke of clandestiene beïnvloeding via kerken en religieuze groeperingen. In het kader van de oorlog in Oekraïne bijvoorbeeld werd in verschillende Europese landen vastgesteld dat Rusland invloed probeert uit te oefenen via de Russisch Orthodoxe kerk. Daarnaast wordt in de procedure die in België wordt aangewend voor de erkenning van een eredienst of een levensbeschouwing, het advies van de VSSE en van andere veiligheidspartners gevraagd. Een van de aspecten die de VSSE nakijkt is het risico op inmenging, volgens de definitie in de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten. Een andere partner die wordt bevraagd is de CFI, dewelke onderzoek kan voeren naar mogelijke financiering uit een derde land (29).

f) Via «influencers» of bekende personen

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

g) Via cyberaanvallen

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

(28) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.
(29) De heer Peter Lanssens, directeur van de Analyse, VSSE.
(30) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

induit le risque que la Chine maîtrise les lignes de communication. La VSSE a en tout cas déjà lancé une mise en garde à ce sujet (31).

h) Via la coercition économique

36. Sur le plan financier, l'ingérence consiste à créer une dépendance financière de la cible au moyen d'investissements stratégiques, de dons à des groupes d'intérêts ou à des partis politiques ou de l'octroi d'un financement de recherche. À propos de ce dernier point, on peut se référer aux pratiques de l'Institut Confucius susmentionné (32).

4) Risques pour la démocratie

37. Les influences étrangères ne se manifestent pas uniquement envers le système politique; elles peuvent également viser le système judiciaire (33).

38. 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 les intérêts d'une puissance étrangère parce que des affinités sont en jeu, et qu'il ne s'agisse pas d'une démarche délibérée: comment déterminer ou différencier l'auteur et la victime et l'intérêt étranger en jeu (34)?

39. La diffusion de fausses informations sur les candidats a des conséquences sur les élections:

– bien qu'il soit difficile de déterminer dans chaque cas spécifique la source et l'influence étrangère visée, nous pouvons en effet dire avec certitude que l'objectif est d'influencer les résultats électoraux, puisque les candidats qui ont de fortes chances d'être élus sont plus susceptibles d'être la cible de la désinformation;

– nous savons que les tentatives orchestrées de diffusion de fausses informations sur des acteurs politiques peuvent mettre les candidats en danger (35).

(31) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen.*
(32) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen*.
(33) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen.*
(34) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London*
(35) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*

beheersen. De VSSE heeft hier in ieder geval al voor gewaarschuwd (31).

h) Via economische dwang

36. Op financieel vlak komt inmenging er op neer om financiële afhankelijkheid te creëren van het doelwit via strategische investeringen, schenkingen aan belangengroepen of politieke partijen of onderzoeksfinanciering. Wat dit laatste betreft, kan worden verwezen naar de praktijken van het hogervermelde Confuciusinstituut (32).

4) Risico's voor de democratie

37. Buitenlandse invloeden manifesteren zich niet enkel in het politiek systeem maar kunnen ook gericht zijn op de rechterlijke macht (33).

38. Het is een uitdaging om te bepalen hoe met binnenlandse actoren moet worden omgegaan in de context van beïnvloedingsoperaties: het kan namelijk zo zijn dat een binnenlandse actor de belangen van een buitenlandse mogendheid verdedigt omdat er affiniteit aan zet is en dat er geen sprake is van een doelbewuste demarche: hoe bepaal je of waar leg je de grens tussen wie dader en wie slachtoffer is en waar het buitenlandse belang zich manifesteert (34)?

39. De verspreiding van desinformatie over kandidaten heeft gevolgen voor de verkiezingen:

– we kunnen namelijk met zekerheid zeggen – hoewel het moeilijk is om in elk specifiek geval na te gaan welke bron er aan de oorsprong ligt en welke buitenlandse invloed er wordt nagestreefd – dat het de bedoeling is om de verkiezingsuitslag te beïnvloeden aangezien kandidaten die grote kanshebber zijn om de verkiezingen te winnen meer kans lopen om het doelwit van desinformatie te zijn;

– we weten dat de georkestreerde pogingen om desinformatie over politieke actoren te verspreiden de kandidaten in gevaar kunnen brengen (35).

(31) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.
(32) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.
(33) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.
(34) Mevrouw Sofia Collignon, *lecturer* (*assistant professor*), *School of politics and IR*, *Queen Mary University of London.*
(35) Mevrouw Sofia Collignon, *lecturer* (*assistant professor*), *School of politics and IR*, *Queen Mary University of London.*

40. Les ingérences des pays «partenaires» posent un problème particulier. Le traitement d'ingérence flagrante de pays avec lesquels la Belgique entretient des relations soutenues – et la présence d'une diaspora importante n'y est souvent pas étrangère – nécessite des précautions particulières afin de conserver un équilibre coût-bénéfice correct. Les autorités belges se montrent donc prudentes et mesurées dans ce cas de figure, en particulier en préférant un traitement de la question à l'abri du regard des médias et en préférant, le cas échéant, l'expulsion à la judiciarisation des personnes impliquées. Les liens avec des pays tels que le Maroc et la Turquie constituent de bons exemples à cet égard. En l'occurrence, la question de l'ingérence ne peut pas être traitée *ex nihilo*, mais doit tenir compte du contexte des relations existantes avec les partenaires concernés (36).

41. Une conséquence – ou un corollaire – du climat d'information brutal est l'insinuation implicite, voire l'encouragement explicite d'une eschatologie violente dans le discours, dans les débats parlementaires et dans la contestation sociale. L'insinuation de la violence cherche à s'unir à un discours qui rejette toute forme de délibération politique. L'usage répété d'insultes lors des débats parlementaires et la diabolisation des opposants constituent la matière première de la radicalisation et de la violence physique et politique, qui vont directement à l'encontre de l'état de paix nécessaire au débat parlementaire et à la délibération démocratique (37).

42. 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 certaines personnes présentant des caractéristiques déterminées (38).

43. 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

(36) M. Michel Liégeois, professeur, Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain.
(37) M. Maxime Lebrun, *deputy director – Research & Analysis, The European Centre of Excellence for Countering Hybrid Threats.*
(38) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR, Queen Mary University of London*.

40. De inmenging door «partnerlanden» vormt een bijzonder probleem. De behandeling van flagrante inmenging door landen waarmee België nauwe betrekkingen onderhoudt – en de aanwezigheid van een grote diaspora is daar vaak niet vreemd aan – vereist bijzondere voorzorgsmaatregelen om een juiste kosten-batenverhouding te handhaven. De Belgische overheid gaat in dergelijke gevallen dan ook voorzichtig en beredeneerd te werk, met name door de kwestie buiten de media om te behandelen en door, indien nodig, de voorkeur te geven aan uitzetting boven vervolging van de betrokkenen. De banden met landen als Marokko en Turkije zijn in deze context goede voorbeelden. De kwestie van inmenging kan in dezen niet *ex nihilo* worden behandeld, maar moet gekaderd worden rekening houdend met de context van de bestaande betrekkingen met de desbetreffende partners (36).

41. Ten gevolge van – of samengaand met – een brutaal klimaat van informatieverspreiding, is er de impliciete insinuatie of zelfs expliciete aanmoediging van een gewelddadige eschatologie in het discours, in de parlementaire debatten en in de sociale protesten. Deze gewelddadige ondertoon zoekt aansluiting bij een discours dat elke vorm van politieke dialoog uitsluit. Het herhaaldelijk beledigen tijdens het parlementair debat en diaboliseren van tegenstanders leveren voedingsbodem voor radicalisering en voor fysiek en politiek geweld dat een rechtstreekse bedreiging vormt voor een vreedzaam parlementair debat en een verdraagzame politieke dialoog (37).

42. Een onderzoek over de kandidaten voor de Britse verkiezingen van 2019 toonde aan dat de doelwitten van desinformatie herleid konden worden tot bepaalde groepen: kandidaten van zwarte en Aziatische minderheidsgroepen waren significant vaker het doelwit. Dit betekent dus dat desinformatiecampagnes kunnen worden ingezet als een georganiseerde poging om de vertegenwoordiging van bepaalde personen met bepaalde kenmerken te ondermijnen (38).

43. Onderzoek wees ook uit dat kandidaten die het slachtoffer zijn van desinformatie de oorzaak hiervan bij hun tegenstanders leggen, ook al geven ze toe dat ze eigenlijk niet echt weten wie aan de oorsprong ligt van de desinformatie. En zelfs als dit nog technisch

(36) De heer Michel Liégeois, professor, *Institut de sciences politiques Louvain-Europe* (ISPOLE), *UCLouvain.*
(37) De heer Maxime Lebrun, *deputy director – Research & Analysis*, *The European Centre of Excellence for Countering Hybrid Threats.*
(38) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*

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 l'effet boule de neige (39).

B. Acteurs principaux

1) Acteurs «positifs» (cherchant à contrer et à prévenir les tentatives d'ingérence)

a) Au niveau international

44. *Transparency International* (TI) est un mouvement mondial qui lutte contre la corruption. TI est présent dans 126 pays. L'institution travaille sur différents thèmes. Le bureau de Bruxelles travaille principalement autour et avec les institutions européennes. À cet égard, TI formule des recommandations aux institutions de l'UE afin d'optimiser leur intégrité politique (40).

45. Au niveau de l'UE a été mise en place, au sein du Parlement européen, la Commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, et sur le renforcement de l'intégrité, de la transparence et de la responsabilité au Parlement européen (ING2), déjà évoquée ci-dessus. Cette commission a élaboré, le 13 juillet 2023, la résolution 2023/2034 (INI) susmentionnée, laquelle contient des recommandations précises proposant des solutions à certaines formes d'ingérence étrangère malveillante. Elle a en outre défini des règles afin de prévenir les conflits d'intérêts, d'améliorer la transparence, ainsi que de prévenir, de décourager et de détecter les ingérences étrangères et la corruption.

46. La problématique de l'ingérence touchant toutes les couches de la société, son approche ne saurait être trop large. Les définitions utilisées au sein de l'UE et de l'Organisation du traité de l'Atlantique Nord (OTAN) peuvent servir de fil rouge à cet égard (41).

47. Il est possible de recourir à la disruption et à la réglementation pour mettre fin à certaines situations, même si cela n'est pas simple.

(39) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR, Queen Mary University of London*.
(40) M. Raphaël Kergueno, *senior policy officer, Transparency International EU.*
(41) M. Dirk Janvier, commissaire divisionnaire, SGRS.

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 (39).

B. Belangrijkste actoren

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

a) Internationaal

44. *Transparency International* (TI) is een wereldwijde beweging die zich inzet tegen corruptie. TI is aanwezig in 126 landen. De instelling werkt rond verschillende thema's. Het kantoor in Brussel werkt vooral rond en met de Europese instellingen. Hierbij doet TI aanbevelingen aan de EU-instellingen om hun politieke integriteit te optimaliseren (40).

45. Op het niveau van de EU werd binnen het Europees Parlement de hoger vermelde Bijzondere Commissie buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2) opgericht. Deze commissie formuleerde op 13 juli 2023 de eerder vermelde resolutie 2023/2034 (INI) die precieze aanbevelingen bevat met oplossingen voor vormen van kwaadwillige buitenlandse inmenging. Ze stelde ook regels op om belangenconflicten te voorkomen, de transparantie te verbeteren en om buitenlandse inmenging en corruptie te voorkomen, te ontmoedigen en op te sporen.

46. De benadering van de problematiek van inmenging kan niet ruim genoeg zijn omdat ze impact heeft op alle lagen van de samenleving. De omschrijvingen die gehanteerd worden binnen de EU en de de Noord-Atlantische Verdragsorganisatie (NAVO) kunnen hier tot leidraad dienen (41).

47. Disruptie en reglementering kunnen ingezet worden om bepaalde situaties een halt toe te roepen, ook al is dat niet eenvoudig.

(39) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*
(40) M. Raphaël Kergueno, *senior policy officer*, *Transparency International EU.*
(41) De heer Dirk Janvier, afdelingscommissaris, ADIV.

Différents instruments peuvent, par exemple, être mis en œuvre sur le plan numérique. Le règlement relatif aux services numériques, déjà évoqué ci-dessus, et le code de bonnes pratiques 2022 en matière de désinformation, qui a été renforcé, offrent aussi des possibilités. Il s'agit d'un code d'autorégulation destiné à toutes les grandes plateformes, qui vise à établir un équilibre entre une manière concrète de lutter contre la manipulation de l'information et la désinformation et la liberté d'expression (42).

b) Au niveau de la Belgique

48. Au niveau de la Belgique, différentes instances sont concernées. Il s'agit entre autres de la Sûreté de l'État (VSSE), du Service général du renseignement et de la sécurité (SGRS), de la police judiciaire fédérale et, en particulier, de l'Office central pour la répression de la corruption (OCRC), de l'Organe de coordination pour l'analyse de la menace (OCAM), de la Cellule de traitement des informations financières (CTIF) et du Centre pour la cybersécurité Belgique (CCB).

49. Selon M. Alexander Mattelaer, *vice dean research*, *Brussels School of Governance* de la *Vrije Universiteit Brussel*, le *Cyber Command* de la Défense belge, qui vient d'être déclaré opérationnel, se concentre, entre autres, sur la détection des opérations d'influence numérique et les éventuelles tentatives de manipulation des élections par des autorités étrangères à l'aide des médias sociaux. Il est parfaitement possible qu'à l'avenir, il soit fait état de campagnes de désinformation orchestrées dans l'intention de manipuler les résultats électoraux. Il faut donc réfléchir aux procédures à suivre et à la manière dont nous pouvons renforcer notre propre capacité de communication stratégique, pour le cas où les constats de nos propres autorités seraient activement contestés par des acteurs étrangers.

50. L'ère numérique actuelle implique qu'il faut tenir compte des influences (légitimes et non légitimes) de toutes sortes. Il est donc d'une importance cruciale d'atténuer l'incidence d'influences hostiles sur la population. Les services de renseignement accomplissent un travail important en termes de détection et de sensibilisation des différents acteurs aux menaces liées à l'ingérence. Dans le cadre de la Stratégie Terrorisme Extrémisme et Radicalisation (TER), l'OCAM suit avec intérêt les initiatives

(42) M. Lutz Güllner, *Head of Strategic Communications*, *European External Action Service* (EEAS).

Op digitaal vlak kunnen er bijvoorbeeld verschillende *tools* ingezet worden. Daarnaast is er ook de hogervermelde digitaledienstenverordening en de aangescherpte praktijkcode 2022 inzake desinformatie. Het gaat om een zelfreguleringscode voor alle grote platforms die streeft naar een evenwicht tussen een concrete aanpak van informatiemanipulatie en desinformatie, en de vrijheid van meningsuiting (42).

b) In België

48. Op Belgisch niveau kan onder meer verwezen worden naar de Veiligheid van de Staat (VSSE), de Algemene Dienst inlichting en veiligheid (ADIV), de federale gerechtelijke politie (FGP) en in het bijzonder de Centrale Dienst voor de bestrijding van corruptie (CDBC), het Coördinatieorgaan voor de dreigingsanalyse (OCAD), de Cel voor financiële informatieverwerking (CFI) en het Centrum voor cybersecurity België (CCB).

49. De heer Alexander Mattelaer, *vice dean research*, *Brussels School of Governance* aan de Vrije Universiteit Brussel, stelt dat het recent operationeel verklaarde *Cyber Command* van de Belgische Defensie zich onder meer toelegt op het detecteren van digitale beïnvloedingsoperaties en eventuele pogingen van buitenlandse overheden om verkiezingen te manipuleren via sociale media. Het is verre van ondenkbaar dat er in de toekomst meldingen worden gedaan van georkestreerde desinformatiecampagnes met als doel de verkiezingsresultaten te manipuleren. Dit maakt het noodzakelijk om na te denken over de te volgen procedures en over de vraag hoe de eigen strategische communicatiecapaciteit versterkt kan worden in de gevallen dat de bevindingen van onze eigen overheden actief gecontesteerd worden door buitenlandse actoren.

50. Het huidige digitale tijdperk, houdt in dat er rekening moet worden gehouden met (legitieme en niet legitieme) invloeden uit allerhande hoeken. Het verminderen van de impact van vijandige invloeden op de bevolking is dan ook van cruciaal belang. De inlichtingendiensten verrichten belangrijk werk op het vlak van detectie en sensibilisering van de verschillende actoren rond de dreigingen gelinkt aan inmenging. In het kader van de Strategie Terrorisme Extremisme en Radicalisering

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

des entités fédérées en matière d'éducation aux médias (43).

51. Selon M. Eric Kalajzic, directeur du Centre d'études de sécurité et de défense à l'Institut royal supérieur de défense (IRSD), il faut suivre une stratégie misant notamment sur le développement d'une culture de la sécurité et du renseignement. Si le monde anglo-saxon est généralement sensibilisé aux questions de sécurité et à l'utilité du renseignement, notre société libérale ouverte est plus réfractaire à se voir imposer des contraintes pour des raisons de sécurité. De plus, nos dirigeants ignorent souvent ce qu'ils peuvent demander et attendre de leurs services de renseignement.

Il faut donc organiser et répéter des campagnes de formation dans les services publics fédéraux (SPF), les administrations publiques, les entreprises privées et auprès des citoyens pour pouvoir faire évoluer les mentalités. Les ministres et leurs conseillers doivent aussi être formés. En tout cas, une prise de conscience a été observée ces dernières années au niveau européen, comme en témoignent la commission ING2 précitée du Parlement européen et la création de la «boîte à outils hybride» de l'UE destinée à lutter contre la manipulation de l'information et l'ingérence étrangère.

52. M. Philippe de Koster, président de la Cellule de traitement des informations financières (CTIF), plaide en faveur d'un encadrement et d'une définition aussi précis que possible de la politique et de la stratégie de défense nationale. Il n'appartient qu'au législateur d'en déterminer les règles et non à la CTIF. C'est d'ailleurs ainsi que les choses se sont passées en France; en novembre 2022, les grandes lignes de la stratégie de défense nationale française ont été annoncées par le président Macron. Il s'agit, en résumé, de la protection des acquis démocratiques et de la protection contre les influences et les ingérences d'acteurs étrangers. Le champ d'action des services de renseignement – et donc de l'homologue français de la CTIF, Traitement du renseignement et action contre les circuits financiers clandestins (Tracfin) – est ainsi clairement défini. Sur cette base, Tracfin peut par exemple demander des informations sur le trafic des paiements entre la Belgique et la France lorsqu'il y a des soupçons d'utilisation

(43) M. Gert Vercauteren, directeur *a.i.*, Organe de coordination pour l'analyse de la menace (OCAM).

(TER) volgt het OCAD met belangstelling de educatieve initiatieven van de deelstaten op het vlak van mediageletterdheid (43).

51. Volgens de heer Eric Kalajzic, directeur van het Studiecentrum voor veiligheid en defensie aan het Koninklijk Hoger Instituut voor defensie (KHID) moet er een strategie gevolgd worden waarin onder meer ingezet wordt op de ontwikkeling van een veiligheids- en inlichtingencultuur. Terwijl de Angelsaksische wereld zich meestal bewust is van de veiligheidsproblemen en van het nut van inlichtingen, stelt onze open, liberale samenleving zich echter weigerachtiger op tegenover verplichtingen uit veiligheidsoverwegingen. Meer nog, onze leiders weten vaak niet wat ze van hun inlichtingendiensten mogen eisen en verwachten.

Men moet dus opleidingscampagnes in de federale overheidsdiensten (FOD), de overheidsadministraties, de privéondernemingen en onder de burgers organiseren en herhalen, om tot een mentaliteitswijziging te kunnen komen. Ook de ministers en hun adviseurs moeten worden opgeleid. Op Europees niveau is er in alle geval de jongste jaren sprake van enige bewustwording, de hogervermelde commissie ING2 van het Europees Parlement en de totstandkoming van de «*hybrid toolbox*» van de EU ter bestrijding van informatiemanipulatie en buitenlandse inmenging zijn hier het bewijs van.

52. De heer Philippe de Koster voorzitter van de Cel voor Financiële Informatieverwerking (CFI), houdt een pleidooi voor een zo nauwkeurig mogelijke afbakening en definitie van het nationaal defensiebeleid en -strategie. Enkel de wetgever kan hiervan de regels vastleggen, de CFI is niet aan zet. Zo ging het ook in Frankrijk: in november 2022 kondigde president Macron de grote lijnen aan van de Franse nationale defensiestrategie. Kort samengevat betreft het de bescherming van de democratische verworvenheden en het voorkomen dat buitenlandse spelers invloed uitoefenen of zich inmengen. Het werkterrein van de inlichtingendiensten – en dus ook van de Franse tegenhanger van de CFI, de *Traitement du renseignement et action contre les circuits financiers clandestins* (Tracfin) – is daarmee duidelijk afgebakend. Op basis hiervan kan Tracfin bijvoorbeeld informatie opvragen over betalingsverkeer tussen België en Frankrijk wanneer het vermoeden bestaat dat de Belgische rekeningen in kwestie uitsluitend worden

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

des comptes belges en question dans le seul but de déstabiliser l'infrastructure (économique) française.

53. Le principe de base des recommandations que M. Etienne Soula, *research analyst*, *Alliance for Securing Democracy*, souhaite formuler est l'importance d'une réponse unie des démocraties. La Belgique n'est pas seule: M. Soula, se réfère à la résolution précitée du Parlement européen du 9 mars 2022 relative à l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation (2020/2268(INI)), qui montre que cela concerne l'ensemble de l'UE. Tous les partenaires de la Belgique sont directement touchés par ces incidents d'ingérence. Il existe un défi commun à toutes les démocraties: les exemples d'ingérence viennent de partout et l'ampleur du problème dépasse les frontières d'un pays ou même d'un continent.

54. Dans le domaine de l'ingérence, la police judiciaire fédérale (PJF) fait face à des défis spécifiques. En effet, elle est une cible potentielle pour l'ingérence, car, en tant que service d'enquête, elle est habilitée à mener certaines enquêtes dans le domaine de la corruption et, par ailleurs, elle est chargée d'assurer la protection nécessaire dans le cadre de son rôle de policier. La PJF peut ainsi être dépositaire d'informations sensibles susceptibles d'intéresser des acteurs étrangers, publics ou non (44).

2) Acteurs «stratégiques» pouvant servir de canaux d'entrée pour les ingérences

55. Il faut tenir compte non seulement des canaux traditionnels du processus décisionnel, mais également des groupes de réflexion qui développent des idées et approches innovatrices. Des influences sont par ailleurs exercées par le biais de groupements activistes, parfois par le biais d'«idiots utiles» qui promeuvent certains agendas politiques sans en avoir conscience. Il est toutefois à noter que les détracteurs de ces approches doivent souvent faire face à des intimidations et contre-mesures, ce qui peut faire obstacle au libre échange d'idées et à un débat ouvert (45).

56. Les opérations d'influence via les médias sociaux visent souvent des thématiques (politiques) semant

(44) M. Eric Snoeck, directeur général de la police judiciaire fédérale, Office central pour la répression de la corruption (OCRC).
(45) M. Kenneth Lasoen, *lector intelligence and security*, Département de Sciences politiques, *Universiteit Antwerpen.*

gebruikt om de Franse (economische) infrastructuur te destabiliseren.

53. Het uitgangspunt van de aanbevelingen die de heer Etienne Soula, *research analyst* aan de *Alliance for Securing Democracy*, wenst te formuleren, is het belang van een eensgezinde reactie van de democratische landen. België staat niet alleen: de heer Soula verwijst naar de hoger vermelde resolutie van het Europees Parlement van 9 maart 2022 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2020/2268(INI)), waaruit blijkt dat dit de hele EU aangaat. Alle partners van België worden immers rechtstreeks getroffen door gevallen van inmenging. Het gaat om een gemeenschappelijke uitdaging voor alle democratieën: de voorbeelden van inmenging komen overal vandaan en de omvang van het probleem overstijgt de grenzen van één land of zelfs één continent.

54. Op het gebied van inmenging zijn er specifieke uitdagingen op het niveau van de federale gerechtelijke politie (FGP). De FGP is namelijk een potentieel doelwit voor inmenging, omdat ze als onderzoeksdienst bevoegd is om bepaalde onderzoeken naar corruptie uit te voeren en daarnaast belast is met het verlenen van de nodige bescherming als politietaak. Hierdoor kan ze in het bezit zijn van gevoelige informatie die relevant kan zijn voor buitenlandse – zowel private als publieke – actoren (44).

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

55. Er wordt niet alleen vertrouwd op de traditionele kanalen van beleidsvorming, maar er wordt tevens gebruik gemaakt van denktanks die innovatieve ideeën en benaderingen ontwikkelen. Daarnaast wordt er invloed uitgeoefend via activistische groeperingen, soms via «nuttige idioten» die onbewust bepaalde politieke agenda's bevorderen. Het valt echter op dat critici van deze benaderingen vaak geconfronteerd worden met intimidatie en tegenmaatregelen, wat de vrije uitwisseling van ideeën en open debat kan belemmeren (45).

56. Beïnvloedingsoperaties via sociale media mikken vaak op (politieke) kwesties die haat zaaien en

(44) De heer Eric Snoeck, directeur-generaal federale gerechtelijke politie, Centrale Dienst voor de bestrijding van de corruptie (CDBC).
(45) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

la haine et se voulant choquantes et qui sont choisies parce qu'elles sont plus faciles à partager sur les médias sociaux. Le défi est de savoir comment les gérer lorsqu'elles sont utilisées pour défendre une cause particulière ou pour susciter le débat en période électorale (46).

57. Avec l'arrivée des *large language models* (LLM) ou grands modèles de langage, il est tout à fait possible que nous soyons submergés, dans un avenir proche, d'éléments de désinformation provenant de divers dialogueurs (*chatbots*) (47).

58. M. Raphaël Glucksmann, président de la commission spéciale sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation, et sur le renforcement de l'intégrité, de la transparence et de la responsabilité au Parlement européen (ING2), s'est attardé sur les pratiques de *TikTok*. Selon lui, *TikTok* doit être en mesure de prouver qu'il ne permet pas que nos données soient utilisées au service du Parti communiste chinois. Cette preuve est nécessaire parce que *TikTok* n'est pas une entreprise privée comme les autres. En Chine, il existe en effet une loi de sécurité nationale qui oblige les grands groupes ou entreprises chinois, malgré leur caractère privé, à être sous l'autorité du Parti communiste et à transmettre tout ce qui est intéressant en termes de renseignement pour la sécurité nationale chinoise. Un énorme problème se pose donc. Cependant, M. Glucksmann ne veut pas dire que *TikTok* devrait être complètement interdit, mais plutôt qu'il devrait être tenu de prouver qu'il ne transmet pas les données en question à la sécurité nationale chinoise.

3) Acteurs «agresseurs»

59. 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'initiateur de l'opération d'ingérence (c'est-à-dire l'agresseur) (48).

60. L'ingérence étrangère n'est plus seulement le fait d'États plus ou moins malveillants; elle est aussi

(46) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*
(47) M. Guy De Pauw, CEO et cofondateur, *Textgain.*
(48) M. Kenneth Lasoen, *lector intelligence and security*, Département de sciences politiques, *Universiteit Antwerpen.*

shockeren omdat dergelijke kwesties makkelijker gedeeld worden op sociale media. De uitdaging bestaat erin om te weten hoe er mee om te gaan als ze worden ingezet om te pleiten voor een bepaalde zaak of om de discussie aan te zwengelen in verkiezingstijden (46).

57. Met de komst van de *large language models* (LLM's), is het perfect mogelijk dat we in de nabije toekomst worden overspoeld met desinformatie afkomstig van allerhande *chatbots* (47).

58. De heer Raphaël Glucksmann, voorzitter van de bijzondere commissie buitenlandse inmenging in alle democratische processen in de Europese Unie met inbegrip van desinformatie en ter versterking van de integriteit, transparantie en verantwoordingsplicht in het Europees Parlement (ING2), stond stil bij de praktijken van *TikTok*. Volgens hem moet *TikTok* aantonen dat het niet toestaat dat onze gegevens worden gebruikt ten behoeve van de Chinese Communistische Partij. Dit is nodig omdat *TikTok* nu eenmaal geen privébedrijf is als een ander. In China is er namelijk een nationale veiligheidswet van kracht die grote Chinese groepen of bedrijven verplicht – ook als ze in de privésector actief zijn – om zich onder het gezag te scharen van de Chinese Communistische Partij en alle voor-de-Chinese-nationale-veiligheid-interessante informatie door te spelen. Dat vormt een enorm probleem. De heer Glucksmann wil evenwel niet gezegd hebben dat dat *TikTok* volledig verboden moet worden, maar wel dat het veeleer dient te bewijzen dat het de gegevens in kwestie niet aan de Chinese nationale veiligheidsdiensten doorgeeft.

3) «Aanvallers»

59. De «agressor» poogt om de *situational awareness* van het doelwit te verstoren. Er wordt druk uitgeoefend op het doelwit om een gunstige uitkomst voor de agressor te bewerkstelligen. Men poogt om de perceptie van het doelwit te manipuleren, zodanig dat het doelwit besluiten neemt in het voordeel van de initiator (dat wil zeggen de agressor) van de inmengingsoperatie (48).

60. Buitenlandse inmenging is niet langer uitsluitend het werk van Staten die al dan niet slechte bedoelingen

(46) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*
(47) De heer Guy De Pauw, CEO en medeoprichter, *Textgain*.
(48) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.

parfois, et le sera sans doute de plus en plus à l'avenir, opérée par des acteurs non étatiques: groupes criminels et 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 (49).

61. 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 (50).

62. Lors des auditions, le *modus operandi* de la société espagnole *Eliminalia* a été expliqué. 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 copié a 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 (51).

63. Lors des auditions, le projet *Pegasus* (précité) a également été évoqué. 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*. Des victimes de ce logiciel

(49) M. Michel Liégeois, professeur, Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain.
(50) M. Kenneth Lasoen, *lector intelligence and security*, Département de sciences politiques, *Universiteit Antwerpen*.
(51) M. Kristof Clerix, journaliste d'investigation, *Knack*.

hebben, maar soms ook, en in de toekomst waarschijnlijk vaker, van niet-gouvernementele actoren: misdaad- en maffiaorganisaties, grote economische en financiële groepen, en andere groeperingen. Die ontwikkeling vergt een aanpassing van de middelen en strategieën ter bestrijding van inmenging en ongetwijfeld ook van de wetgeving.

Het wordt nog ingewikkelder wanneer men ziet dat sommige niet-gouvernementele actoren als onderaannemers optreden van 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 (49).

61. De term «agressor» kan doelbewust gebruikt worden in deze context, zeker wanneer de agressie uitgaat van autocratische regimes. In dat laatste geval gaat het namelijk om agressie waarin er een vorm van oorlog wordt uitgevochten tussen de open democratische maatschappij en autocratische regimes, gericht tegen onze waarden, onze manier van leven en onze manier van aan politiek doen (50).

62. Tijdens de hoorzittingen werd de *modus operandi* toegelicht van het Spaans bedrijf *Eliminalia*. Die zit als volgt in elkaar: een klant vraagt bijvoorbeeld om een ongunstig artikel van het internet te verwijderen. Het team van *Eliminalia* copy-pastet het geviseerde artikel op het platform van een *fakenews*-leverancier waarbij de publicatiedatum wordt geantidateerd waardoor het er op lijkt dat het gekopieerde artikel al eerder verscheen. *Eliminalia* ontkracht vervolgens het oorspronkelijk artikel op grond van plagiaat en verzoekt de internetzoekmachines dan ook om het oorspronkelijke artikel uit de zoekbestanden te verwijderen. Dergelijke – eenvoudige – interventie leverde resultaten op in tal van gevallen. De wetgeving wordt hier dus misbruikt om informatie met een *public interest* gehalte offline te kunnen halen (51).

63. Er werd in de hoorzittingen ook verwezen naar het *Pegasus*-project (hoger vermeld) waarin een journalistencollectief onthulde dat journalisten en mensenrechtenactivisten wereldwijd het slachtoffer waren geworden van de *Pegasus-spyware*, ontwikkeld door de Israëlische *NSO Group*. Ook in België

(49) De heer Michel Liégeois, professor, *Institut de sciences politiques Lo)uvain-Europe* (ISPOLE), *UCLouvain*.
(50) De heer Kenneth Lasoen, *lector intelligence and security*, Departement Politieke Wetenschappen, Universiteit Antwerpen.
(51) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.

ont aussi été identifiées en Belgique. Le logiciel en question permettait de prendre complètement le contrôle de smartphones à distance (52).

C. Ingérences identifiées

64. Au cours des auditions, un certain nombre de pays ont été cités comme sources d'ingérence: la Turquie, le Qatar (notamment à la suite du *Qatargate*, qui a amené le Parlement européen à élaborer la résolution susmentionnée 2023/2034(INI)), le Maroc (*Marocgate* en lien avec le Sahara occidental), le Congo et le Rwanda (53).

La Chine et la Russie ont, elles aussi, été abondamment citées.

Les États-Unis ont également été évoqués, ce qui montre que l'ingérence peut aussi émaner de pays occidentaux.

65. Afin de s'assurer un terreau stratégiquement favorable à sa sphère d'influence, la Chine s'attelle à «gagner les cœurs et les esprits», non seulement parmi l'élite européenne, mais aussi auprès de la population locale. Elle tente d'influencer des mandataires politiques, de la majorité comme de l'opposition, aussi bien au niveau national qu'à l'échelle européenne. Elle vise des responsables politiques locaux – par le biais de la diplomatie infranationale – et coopte des *leaders* d'opinion, des journalistes et des membres de groupes de réflexion. La Chine a par ailleurs investi dans des médias européens et tente de construire des récits spécifiques via des plateformes numériques telles que *Facebook*, *Twitter* ou *TikTok*. Elle a approché des centres de recherche et des instituts d'enseignement supérieur en Europe en vue du transfert éventuel de nouvelles technologies importantes, propices au potentiel militaire (54).

66. Le conflit en Ukraine a placé une nouvelle fois la doctrine de la «guerre hybride» au centre de l'attention. Il s'agit d'une guerre qui est menée au moyen d'armes non militaires destinées à déstabiliser un ennemi potentiel, à semer la division ou à paralyser certains secteurs critiques et sensibles de celui-ci. Un élément important de cette guerre hybride est la stratégie d'influence et de manipulation. Depuis plusieurs années déjà, la Russie mène des campagnes complexes d'opérations d'information (OI) dans le

(52) M. Kristof Clerix, journaliste d'investigation, *Knack*.
(53) M. Kristof Clerix, journaliste d'investigation, *Knack*.
(54) Mme Ivana Karásková, *European China Policy Fellow*, *Mercator Institute for China Studies*.

waren er slachtoffers. De software in kwestie liet toe om vanop afstand de software van smartphones volledig over te nemen en te controleren. (52)

C. Geïdentificeerde gevallen van inmenging

64. Tijdens de hoorzittingen werden een aantal landen vernoemd als bronnen van inmenging: Turkije, Qatar (met name sinds *Qatargate* dat het Europees Parlement aanzette tot het uitvaardigen van hogervermelde resolutie 2023/2034(INI)), Marokko (*Marocgate* in verband met de Westelijke Sahara), Congo, Rwanda (53).

China en Rusland kwamen ook uitvoerig aan bod.

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

65. Om een strategisch gunstige voedingsbodem te garanderen voor haar invloedsfeer, richt China zich bijvoorbeeld op het «winnen van harten en geesten», niet alleen onder de Europese elite, maar ook onder de lokale bevolking. Het probeert om politici – zowel op regerings- als op oppositieniveau, zowel op nationaal als Europees niveau – te beïnvloeden. Het richt zich op lokale politici – via «subnationale diplomatie» – en coöpteert opiniemakers, journalisten en leden van denktanks. China investeerde voorts in Europese media en probeert om via digitale mediaplatforms – *Facebook*, *Twitter*, *TikTok*, enz. – specifieke narratieven tot stand te brengen. Ze heeft onderzoekscentra en instellingen voor hoger onderwijs in Europa benaderd met het oog op een mogelijke transfer van belangrijke en nieuwe technologieën bevorderlijk voor het militair potentieel (54).

66. Het conflict met Oekraïne heeft de aandacht acuut gevestigd op de doctrine van de «hybride oorlogsvoering» aangestuurd vanuit Rusland. Het gaat hier om niet-militaire wapens die moeten helpen om een potentiële vijand te destabiliseren, om verdeeldheid te zaaien of om bepaalde kritieke en gevoelige sectoren van de tegenstander lam te leggen. Een belangrijke component van deze hybride oorlogsvoering is de strategie van beïnvloeding en manipulatie. Rusland voert al sinds jaren complexe *Information*

(52) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.
(53) De heer Kristof Clerix, onderzoeksjournalist, *Knack*.
(54) Mevrouw Ivana Karásková, *European China Policy Fellow*, *Mercator Institute for China Studies.*

but d'influencer l'opinion publique et de saper le consensus politique et social occidental (55).

67. Le Service européen pour l'action extérieure (SEAE) gère le projet *EUvsDisinfo*, qui vise tout particulièrement à lutter contre la désinformation russe. Le projet passe au peigne fin les narratifs utilisés, cherche à révéler des faits et à sensibiliser à cette question (56).

D. Mesures prises

1) Niveau national

68. Selon M. Luca Ferro, professeur adjoint en droit international à la *Vrije Universiteit Brussel*, bon nombre des critères juridiques en lien avec l'ingérence étrangère sont flous et insuffisamment élaborés. Tout État souverain, y compris la Belgique, peut prendre explicitement position: selon M. Luca Ferro, il serait utile que la Belgique le fasse. M. Luca Ferro se réfère à l'initiative de la Belgique – pionnière en la matière – concernant l'inscription du délit d'écocide dans le nouveau Code pénal, par laquelle la Belgique contribue à donner forme à l'interprétation du droit international. Par analogie, il devrait en être de même pour le phénomène de l'ingérence étrangère.

Un autre exemple dans ce domaine est le cas de l'application du droit international dans le cyberespace, source de très nombreuses discussions parmi les juristes. La Belgique n'a pas encore pris position à cet égard, contrairement à la France, aux Pays-Bas, à l'Allemagne et à l'Italie. Selon M. Luca Ferro, la Belgique peut donc, dans ce domaine également, participer à la concrétisation du cadre international et apporter une contribution concrète au débat.

69. Lors des élections de 2019, la VSSE et le SGRS ont informé les présidents de partis sur les risques d'ingérence dans le processus électoral. Pour les prochaines élections aussi, la VSSE entend poursuivre sur cette voie (57).

Pour les élections de 2019, la VSSE, en collaboration avec le SGRS et le Centre pour la cybersécurité Belgique (CCB), a élaboré une brochure spécifique («Surfer en toute sécurité pendant la campagne électorale»). Une *Joint Intelligence Task Force* (JITF) a

(55) M. Gert Vercauteren, directeur *a.i.*, OCAM.
(56) M. Lutz Güllner, *Head of Strategic Communications,* EEAS.
(57) M. Peter Lanssens, directeur de l'analyse, VSSE.

Operations (IO)-campagnes om de publieke opinie te beïnvloeden en de westerse politieke en maatschappelijke consensus te ondergraven (55).

67. De *European External Action Service* (EEAS) runt het project *EUvsDisinfo*, dat zich in het bijzonder richt op Russische desinformatie. Het zoomt in op de gebruikte narratieven, probeert feiten te onthullen en het bewustzijn daaromtrent te verhogen (56).

D. Getroffen maatregelen

1) Op nationaal niveau

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

Een ander voorbeeld op dat vlak is de casus van de toepassing van het internationaal recht in cyberspace, bron voor heel wat discussiemateriaal onder rechtsgeleerden. Hier heeft België nog geen positie ingenomen; Frankrijk, Nederland, Duitsland en Italië daarentegen wel. Volgens de heer Luca Ferro kan België ook op dat vlak het internationaal kader mee vorm geven en een concrete bijdrage leveren aan het debat.

69. Tijdens de verkiezingen van 2019 hebben de VSSE en de ADIV de partijvoorzitters geïnformeerd over de risico's van inmenging in het verkiezingsproces. Ook voor de nakende verkiezingen wil de VSSE hier op inzetten (57).

Voor de verkiezingen van 2019 stelde de VSSE in samenwerking met de ADIV en het Centrum voor cybersecurity België (CCB) een specifieke brochure op («Veilig online tijdens de verkiezingscampagne»). Er werd toen trouwens ook een *Joint Intelligence*

(55) De heer Gert Vercauteren, directeur *a.i.*, OCAD.
(56) De heer Lutz Güllner, *Head of Strategic Communications*, EEAS.
(57) De heer Peter Lanssens, directeur van de Analyse, VSSE.

d'ailleurs été mise en place afin de déterminer s'il était ou non question d'ingérence.

70. Le Comité permanent R a décidé, au début de 2019, d'ouvrir une enquête sur la manière dont les services de renseignement belges avaient réagi (collecte de renseignements, avertissements, coopération internationale, possibles entraves, etc.) à l'ingérence éventuelle de services ou d'États étrangers dans le processus électoral belge (58). La conclusion était qu'aucune grande irrégularité n'avait été constatée au niveau structurel, mais bien quelques cas individuels mineurs d'influence et/ou d'ingérence dans le processus électoral.

71. Selon M. Tanguy Struye de Swielande, professeur à l'Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain, nous disposons d'une stratégie de sécurité nationale. En revanche, personne ne sait ce qu'elle signifie vraiment, et personne ne la pilote. Elle contient des concepts très précieux tels que le besoin de résilience – primordial en cas d'ingérence –, et l'idée d'une approche pansociétale (*whole-society*) pour lutter contre les ingérences. Le problème est toutefois que l'approche est trop compartimentée: il n'y a absolument aucune cohérence ou coopération concernant la mise en œuvre de ce plan.

72. Aux Pays-Bas, plusieurs initiatives ont été prises dans ce domaine, entre autres la modification de la loi interdisant l'espionnage de la diaspora et la création d'un guichet de signalement où les membres de la diaspora qui se sentent victimes d'intimidations peuvent le faire savoir. Ces initiatives montrent que les autorités néerlandaises prennent très au sérieux l'ingérence dans la diaspora et tentent de la combattre. Elles ont aussi une valeur symbolique, car les perspectives d'action semblent parfois limitées (59).

73. Une autre initiative prise de longue date déjà par les Pays-Bas est de favoriser des contacts étroits entre certains ministères et les principales communautés immigrées. C'est, pour les autorités néerlandaises, une manière de se tenir informées, dans la mesure du possible, de ce qui se passe au sein de ces communautés et de détecter quels éléments de ces

(58) Comité permanent R: *Rapport d'activités 2020*, p. 22 et suiv.

(59) M. Christopher Houtkamp, s*enior research fellow – head Connected Security programme, Clingendael – the Netherlands Institute of International Relations.*

Task Force (JITF) opgericht om na te gaan of er al dan niet sprake was van inmenging.

70. Het Vast Comité I besloot begin 2019 om een onderzoek te voeren naar de manier waarop de Belgische inlichtingendiensten reageerden (inwinnen van informatie, waarschuwingen, internationale samenwerking, mogelijke belemmeringen, enz.) op mogelijke inmenging van buitenlandse diensten of landen in de Belgische verkiezingen (58). Het besluit was dat er geen grote structurele onregelmatigheden waren vastgesteld, alleen enkele minder belangrijke individuele gevallen van beïnvloeding en/of inmenging in het verkiezingsproces.

71. Volgens de heer Tanguy Struye de Swielande, professor aan het *Institut de sciences politiques Louvain-Europe* (ISPOLE) van de *UCLouvain*, beschikken we enerzijds over een nationale veiligheidsstrategie. Anderzijds weet niemand wat die strategie werkelijk inhoudt en stuurt niemand ze aan. Ze bevat heel waardevolle concepten zoals de behoefte aan veerkracht – die van het grootste belang is bij inmenging – en het idee van een *whole society approach* om inmenging te bestrijden. Het probleem is echter dat de aanpak te gefragmenteerd is: er is absoluut geen samenhang of samenwerking met betrekking tot de uitvoering van het plan.

72. In Nederland werden er een aantal initiatieven genomen, onder meer de wetswijziging die diasporaspionage verbiedt en de oprichting van een meldpunt waar leden van diasporagemeenschappen die zich geïntimideerd voelen dit kenbaar kunnen maken. Deze initiatieven laten zien dat de Nederlandse overheid inmenging in diasporagemeenschappen uitermate serieus neemt en probeert om er iets aan te doen. Ze hebben ook een symbolische waarde omdat het handelingsperspectief soms beperkt lijkt (59).

73. Een ander initiatief dat Nederland al geruime tijd neemt, is het bevorderen van nauw contact tussen bepaalde ministeries en de grotere migrantengemeenschappen. Op die manier kan de overheid in de mate van het mogelijke de vinger aan de pols houden van wat er binnen de gemeenschappen speelt, en detecteren welke delen van de gemeenschappen

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

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

communautés font l'objet d'intimidations. Elles peuvent alors éventuellement offrir une aide et une protection (60).

74. Le Royaume-Uni reconnaît que l'ingérence constitue un problème majeur et plusieurs propositions de modification de la législation y sont ou ont été débattues:

– un amendement a été déposé pour lier le projet de loi sur la sécurité nationale (*National Security Bill*) au projet de loi sur la sécurité en ligne (*Online Safety Bill*);

– le système d'enregistrement des influences étrangères (*Foreign Influence Registration Scheme*) a été intégré dans le projet de loi sur la sécurité nationale (*National Security Bill*);

– l'infraction d'ingérence étrangère (*Foreign Interference Offence*) a été ajoutée à la liste des infractions prioritaires du projet de loi sur la sécurité en ligne;

– l'ingérence étrangère, de même que la désinformation liée à l'État (*state-linked disinformation*), ont été rendues punissables;

– sont punissables: les comportements commis pour ou au nom d'une puissance étrangère, ou dans le but de la favoriser, et qui violent les droits du Royaume-Uni; les comportements qui discréditent les institutions démocratiques, manipulent la participation des citoyens aux institutions et portent atteinte à la sécurité des intérêts du Royaume-Uni;

– est également punissable le comportement qui consiste à présenter des informations fausses ou trompeuses, en ce compris l'utilisation d'informations vraies, mais présentées de manière trompeuse ou de manière à falsifier l'identité d'une personne (61).

2) Niveau européen

75. L'Union européenne a émis un certain nombre de recommandations et proposé des procédures.

(60) M. Christopher Houtkamp, *senior research fellow – head Connected Security programme, Clingendael – the Netherlands Institute of International Relations.*
(61) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*

te maken hebben met intimidatie. Dit kan mogelijk steun en bescherming bieden (60).

74. Het Verenigd Koninkrijk erkent dat inmenging een belangrijk probleem is en verschillende voorstellen tot aanpassing van de wetgeving werden of worden er besproken:

– er werd een amendement ingediend om de *National Security Bill* te koppelen aan de *Online Safety Bill*;

– het *Foreign Influence Registration Scheme* (FIRS) werd opgenomen in de *National Security Bill*;

– het strafbaar feit van buitenlandse inmenging (*Foreign Interference Offence*) werd toegevoegd aan de lijst van prioritaire misdrijven in de *Online Safety Bill*;

– de strafbaarstelling van buitenlandse inmenging is vastgelegd met inbegrip van de aan-de-staat-gelinkte desinformatie (*state-linked disinformation*);

– wordt strafbaar gesteld: de gedraging waarbij voor, namens of met de bedoeling een buitenlandse mogendheid te bevoordelen, inbreuk wordt gemaakt op de rechten van het Verenigd Koninkrijk; de gedraging die de democratische instellingen in diskrediet brengt, die de deelname van de burgers aan de instellingen manipuleert en die de veiligheid van de belangen van het Verenigd Koninkrijk ondermijnt;

– het strafbare feit omvat de gedraging waarbij een valse of misleidende voorstelling van de zaken wordt gegeven, met inbegrip van het gebruik van informatie die juist is maar op een misleidende manier wordt gepresenteerd of waarbij de identiteit van een persoon verkeerd wordt voorgesteld (61).

2) Op Europees niveau

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

(60) De heer Christopher Houtkamp, *senior research fellow – head Connected Security programme*, *Clingendael – the Netherlands Institute of International Relations.*
(61) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*

Il existe notamment:

– 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));

– 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));

– 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) no 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2);

– la «boussole stratégique en matière de sécurité et de défense» (Conseil de l'Union européenne, 21 mars 2022, 7371/22);

– 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);

– la *East StratCom Task Force* (*task force* de communication stratégique orientée vers le voisinage oriental) du Service européen pour l'action extérieure (SEAE);

– le cadre commun en matière de lutte contre les menaces hybrides (JOIN(2016) 18 final);

– la boîte à outils cyberdiplomatique de l'UE (*Cyber Diplomacy Toolbox* – CDT);

– les règles de l'UE relatives au renforcement de la démocratie (entre autres intégrité des élections, transparence et ciblage de la publicité à caractère politique, financement des partis politiques, droits électoraux).

76. Il y a aussi le Centre européen d'excellence pour la lutte contre les menaces hybrides (*European*

Er zijn onder meer:

– de resolutie van het Europees Parlement van 13 juli 2023 over aanbevelingen voor de hervorming van de regels van het Europees Parlement inzake transparantie, integriteit, verantwoordingsplicht en corruptiebestrijding (2023/2034(INI));

– de resolutie van het Europees Parlement van 1 juni 2023 over buitenlandse inmenging in alle democratische processen in de Europese Unie, met inbegrip van desinformatie (2022/2075(INI));

– de cybersecurity-strategie en de richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van verordening (EU) nr. 910/2014 en richtlijn (EU) 2018/1972 en tot intrekking van richtlijn (EU) 2016/1148 (NIS2-richtlijn);

– het «strategisch kompas voor veiligheid en defensie» (Raad van de Europese Unie, 21 maart 2022, 7371/22);

– de resolutie van het Europees Parlement van 10 oktober 2019 over buitenlandse inmenging in verkiezingen en desinformatie in de nationale en Europese democratische processen (2019/2810(RSP);

– de *East Stratcom Task Force* van de Europese Dienst voor extern optreden (EEAS);

– het gezamenlijk kader voor de bestrijding van hybride bedreigingen (JOIN(2016) 18 final);

– de EU *Cyber Diplomacy Toolbox* (CDT);

– de EU-regels ter versterking van de democratie (onder andere integriteit van de verkiezingen, transparantie en gerichte politieke reclame, partijfinanciering, kiesrechten).

76. Er is ook het *European Centre of Excellence for Countering Hybrid Threats* (Hybrid CoE), een

Centre of Excellence for Countering Hybrid Threats – Hybrid CoE), une organisation internationale autonome de lutte contre les menaces hybrides fondée sur des réseaux.

77. On peut souligner la volonté de moderniser et d'opérationnaliser la transparence en créant des registres des *lobbies*, en rendant obligatoire le signalement des contacts entre des élus et divers groupes de pression et en améliorant le contrôle en la matière. On peut noter à cet égard que le registre de transparence prévoit l'obligation pour toute structure, y compris les organisations non gouvernementales (ONG), dès lors qu'elle bénéficie de financements – c'est-à-dire dès lors qu'elle n'est pas une entité commerciale – d'indiquer toutes ses sources de financement (62).

78. L'attention portée aux aspects sécuritaires dans les nouvelles réglementations européennes est également fondamentale:

– le règlement relatif aux services numériques (susmentionné) adopté récemment impose par exemple des obligations en matière de transparence des algorithmes sur lesquels reposent les médias sociaux, et la mise en place de mécanismes de signalement des contenus manifestement nuisibles. La question centrale est de savoir si cette nouvelle réglementation va déjà trop loin ou justement pas encore assez loin;

– un autre exemple concerne la nouvelle directive SRI 2 (susmentionnée) sur la cybersécurité des réseaux et des systèmes d'information ainsi que la proposition de règlement du Parlement européen et du Conseil concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020 (COM(2022)454 final – connue sous le nom «*Cyber Resilience Act*»). Pour le marché intérieur, l'enjeu est de réduire au maximum toute menace d'ingérence étrangère, tout en maintenant des standards ouverts et un fonctionnement concurrentiel du marché (63).

3) Évaluation et limites des mesures prises

79. Ces dernières années, l'accroissement significatif des ressources allouées aux services de renseignement et la diminution graduelle de la menace terroriste

(62) M. Raphaël Kergueno, *senior policy officer*, *Transparency International EU.*

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

autonome, netwerkgebaseerde internationale organisatie voor de bestrijding van hybride bedreigingen.

77. Er is duidelijk een wil om de transparantie te moderniseren en operationeel te maken door lobbyregisters aan te maken, en door de melding van contacten tussen verkozen vertegenwoordigers en verschillende drukkingsgroepen verplicht te maken en beter te controleren. In dit verband moet worden opgemerkt dat het transparantieregister vereist dat elke structuur, met inbegrip van niet gouvernementele organisaties (ngo) die financiering ontvangt – en die dus geen commerciële entiteit is – al haar financieringsbronnen moet vermelden (62).

78. Ook de aandacht voor de veiligheidsaspecten van nieuwe Europese regelgeving is van groot belang:

– de recente digitaledienstenverordening (hoger vermeld) legt bijvoorbeeld verplichtingen op inzake de transparantie van algoritmes waarop sociale media berusten en de nood aan mechanismen om manifest schadelijke content te rapporteren. De hamvraag is of deze nieuwe regelgeving al te ver of net niet ver genoeg gaat;

– een ander voorbeeld betreft de nieuwe NIS2-richtlijn (hogervermeld) met betrekking tot cybersecurity van netwerken en informatiesystemen en het voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van verordening (EU) 2019/1020 (COM(2022)454 final, de zogenaamde *Cyber Resilience Act*). De inzet voor de interne markt is het minimaliseren van de dreiging van buitenlandse inmenging, terwijl tegelijkertijd wordt vastgehouden aan open standaarden en competitieve marktwerking (63).

3) Evaluatie en limieten van de genomen maatregelen

79. Door de aanzienlijke toename van de middelen voor de inlichtingendiensten en de geleidelijke afname van de terroristische dreiging zijn in de afgelopen jaren

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

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

ont permis de dégager les moyens nécessaires pour la contre-ingérence. À cela s'ajoute une meilleure coordination des branches civile et militaire des services de renseignement. La situation est globalement satisfaisante de ce point de vue, notamment si on la compare avec celle qui prévalait il y a une quinzaine d'années (64).

80. L'identification des auteurs de (cyber)attaques est difficile: l'attribution d'un événement unique est relativement simple, mais lorsque des éléments sont partagés de façon organique, il est très difficile de les tracer. Au mieux, il est possible de remonter à l'origine de ce type de désinformation, mais comment faire lorsqu'elle est propagée de façon organique (65)?

81. Les opérations d'ingérence agissent au niveau cognitif et ne sont pas directement assimilables à des contraintes. C'est précisément parce qu'elles se situent au niveau cognitif qu'il est également difficile d'évaluer directement leur efficacité (66).

*
* *

(64) M. Michel Liégeois, professeur, Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain.
(65) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*
(66) Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*

de benodigde middelen vrijgemaakt om inmenging te bestrijden. Bovendien is de coördinatie tussen de civiele en de militaire tak van de inlichtingendiensten verbeterd. Vanuit dit oogpunt is de situatie over het algemeen bevredigend, met name in vergelijking met zo'n vijftien jaar geleden (64).

80. De toewijzing van (cyber)aanvallen is moeilijk: het toewijzen van een individuele gebeurtenis is relatief eenvoudig, maar wanneer items organisch worden gedeeld, wordt het zeer moeilijk om ze te traceren. In het beste geval is het misschien mogelijk om de oorsprong van dit soort desinformatie te achterhalen, maar hoe ga je om met de organische verspreiding ervan (65)?

81. Inmengingsoperaties werken op het cognitief niveau en zijn niet onmiddellijk gelijk te stellen aan dwanghandelingen. Net omdat ze zich op het cognitief niveau afspelen, is het ook moeilijk om de doeltreffendheid ervan direct te beoordelen (66).

*
* *

(64) De heer Michel Liégeois, *professor*, *Institut de sciences politiques Louvain-Europe (ISPOLE)*, *UCLouvain*.
(65) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*
(66) Mevrouw Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR*, *Queen Mary University of London.*

PARTIE II: RECOMMANDATIONS

I. CONCEVOIR ET METTRE EN ŒUVRE DES STRATÉGIES D'ALERTE ET DE RÉDUCTION DES RISQUES

A. Information/sensibilisation

1. Pour se prémunir contre les ingérences, il est nécessaire 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, quels que soient sa fonction, son niveau ou son grade, d'une «conscience situationnelle»: il s'agit 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.

2. 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.

3. Il est indispensable de ne pas se fier uniquement à la vérification des faits (*factchecking*) et à la démystification (*debunking*), mais aussi d'œuvrer à un changement plus large de mentalité. L'approche doit également viser à développer, en misant considérablement sur l'enseignement, l'esprit critique, l'éducation aux médias et la résilience face à la désinformation, moyens efficaces de contrer les mécanismes d'ingérence.

4. La résilience sociétale face à l'ingérence repose sur notre propre comportement. À cet égard, on peut considérer plusieurs groupes de personnes ou institutions.

   a) On pense, en particulier, aux mandataires politiques et aux fonctions publiques. Faire preuve de transparence en matière d'intérêts financiers, expliciter les éventuels conflits d'intérêts, disposer de codes éthiques et de registres de transparence sont autant de moyens de contribuer à cette résilience.

   b) Vu l'importance de la sécurité des connaissances, il importe de prendre des initiatives visant à préserver les universités de toute ingérence.

DEEL II: AANBEVELINGEN

I. WAARSCHUWINGS- EN RISICOBEPERKINGSSTRATEGIEËN ONTWIKKELEN EN IMPLEMENTEREN

A. Voorlichting/bewustmaking

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

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

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

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

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

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

c) Il importe de mener 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.

Ces campagnes visent à les informer des risques d'espionnage numérique et à leur donner des conseils pratiques pour renforcer leur sécurité en ligne, comme recourir au chiffrement de bout en bout, mettre régulièrement à jour les logiciels et éviter les liens et annexes suspects.

d) Il convient d'organiser régulièrement des campagnes de formation au sein des instances publiques et des entreprises privées, ainsi que pour les citoyens, afin de favoriser un changement de mentalité. Cela concerne également les ministres et les conseillers.

e) Des programmes éducatifs dans les écoles, misant sur l'enseignement de la gestion de l'information et de l'esprit critique, sont nécessaires, en particulier à destination des jeunes, car ces derniers sont particulièrement ciblés par les plateformes de réseaux sociaux.

5. Il s'impose de mettre systématiquement en œuvre des mesures concrètes, telles que de fréquents *briefings* de sécurité lors d'interactions avec des partenaires étrangers, afin de promouvoir des améliorations.

6. Ceci passe par un renforcement de la communication entre la Sûreté de l'État (VSSE) et les acteurs académiques, scientifiques et politiques.

a) Pour ce qui est des secteurs académiques et de la recherche, l'Académie de recherche et d'enseignement supérieur (ARES) et le *Vlaamse Interuniversitaire Raad* (VLIR), ainsi que les établissements de recherche et d'enseignement supérieur, doivent opérationnaliser les mesures suivantes:

− soutenir le renforcement de la cybersécurité au sein des établissements;

− mettre en place un bureau consultatif au niveau fédéral qui pourrait agréger les informations issues des différents services publics pour éclairer les universités sur les risques de certaines collaborations.

b) Pour ce qui concerne les mandataires politiques, un *briefing* de sensibilisation à la sécurité et aux

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

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

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

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

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

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

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

− de versterking van de cybersecurity binnen de instellingen ondersteunen;

− een adviesbureau op federaal niveau oprichten dat de informatie van de verschillende overheidsdiensten kan samenbrengen om universiteiten te adviseren over de risico's van bepaalde samenwerkingsverbanden.

b) Wat de politieke mandatarissen betreft, zou de VSSE aan het begin van elke zittingsperiode een

risques d'ingérence devrait être organisé par la VSSE au début de chaque mandature, comme cela a été proposé aux parlementaires européens, et ce à tous les niveaux de pouvoir (y compris au niveau local).

B. Communication

7. Nous recommandons aux autorités publiques et aux entreprises de médias sociaux de 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.

8. En particulier en période électorale, il convient d'instaurer un code de bonne conduite pour les partis politiques et les candidats.

9. On pourrait envisager 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. Nous recommandons de créer en Belgique, à l'image de ce qui est réalisé aux Pays-Bas, un point de contact entre certains services publics spécifiques et les associations des diasporas. Un tel point de contact pourra développer des programmes de sensibilisation et d'éducation aux médias et à l'information à destination des diasporas et des minorités de notre pays, afin de renforcer leur résilience. Cela permettra aux autorités publiques de rester bien informées de la situation au sein de ces communautés et de détecter et combattre plus efficacement l'intimidation, les menaces et l'ingérence. Cette initiative servira de base au soutien et à la protection offerts aux communautés concernées.

11. Afin de réduire les effets d'une influence extérieure, les pouvoirs publics doivent contribuer à la transparence et à la confiance sur les plateformes existantes en encourageant le dialogue, le débat et la discussion avec les citoyens.

12. Dans la mise au jour des ingérences étrangères, les organes de presse et d'information peuvent être des alliés précieux, comme lanceurs d'alerte et moyennant le respect des clauses de responsabilité.

briefing moeten organiseren om hen bewust te maken van de mogelijke gevaren voor de veiligheid en de risico's van inmenging, zoals ook werd voorgesteld voor de Europese parlementsleden, en dat op alle bevoegdheidsniveaus (met inbegrip van het lokale niveau).

B. Communicatie

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

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

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

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

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

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

C. Recherche

13. Lorsque la désinformation est diffusée de façon organique, la première chose à faire est toujours d'en identifier la source. Il est capital de retracer la désinformation jusqu'à sa source, *a fortiori* lorsqu'il apparaît que des acteurs étatiques étrangers en sont à l'origine.

    Nous recommandons à cette fin de dégager des moyens pour mener de nouvelles études sur la détection, l'analyse et la résilience, afin d'obtenir une vision plus claire du phénomène. Ces moyens doivent être octroyés aussi bien aux services de sécurité concernés qu'aux universités.

    Le renforcement de notre protection contre les menaces nécessite une double approche. D'une part, il faut investir dans la technologie afin d'améliorer la sécurité. D'autre part, il faut opérer un changement culturel permettant à la Belgique de prendre conscience de sa vulnérabilité.

    À cet égard, nous devons en priorité combler les brèches et remédier aux lacunes existant dans les lois actuelles sur le *lobbying*, ainsi qu'analyser les vulnérabilités administratives et sociétales, les initiatives et contre-mesures nationales, les motivations et objectifs des agresseurs et les effets des algorithmes.

14. Il est essentiel de développer constamment les techniques permettant de détecter les textes écrits par des robots et les images générées par intelligence artificielle. Nous recommandons que l'autorité fédérale, en concertation avec les Régions, y affecte en permanence des moyens matériels et humains.

15. L'analyse ciblée des potentiels acteurs d'ingérence, que ce soient des pays déjà reconnus pour leur ingérence (Russie, Chine, Turquie, Qatar, Maroc, Israël), des entreprises (*TikTok*) ou des communautés de la diaspora, revêt une grande importance. Elle aide les pouvoirs publics à approfondir leurs connaissances et à étendre leurs possibilités d'action.

16. Il convient de mener des études afin d'élaborer éventuellement 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. Cela peut passer par une collaboration étroite entre les services de sécurité et les services de renseignement nationaux

C. Onderzoek

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

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

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

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

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

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

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

qui permettra d'établir s'il existe véritablement une intention de servir des intérêts étrangers.

D. Mesures répressives

17. Il est important de poursuivre le développement de notre cybercapacité nationale. Nous recommandons d'accroître les investissements existants. En outre, il convient de renforcer la coopération avec les pays partenaires afin d'organiser des formations en cybernétique et d'échanger les expertises.

18. Afin de limiter l'impact des opérations d'information étrangères, il convient de prendre une initiative similaire à celle de l'Union européenne (UE) pour interdire certains canaux spécifiques de propagande étrangère. Cela réduit leur portée et leur influence.

19. Au microniveau, une approche efficace de l'ingérence étrangère par le biais d'internet consiste à en identifier systématiquement les manifestations, à les analyser et à les traiter de manière proactive. Cela passe par la suppression des contenus trompeurs, la réfutation des fausses informations et la communication proactive d'informations factuelles sur l'importance de la démocratie et des droits humains afin de réduire la propagation de l'ingérence.

II. TRANSPARENCE

A. Médias sociaux

20. Nous recommandons, au niveau européen, le développement d'un mécanisme visant à une réglementation plus stricte et à des exigences de transparence pour les contenus en ligne relatifs à des questions politiques. Cela suppose que les plateformes soient tenues d'identifier les comptes de médias sociaux et les publicités en lien avec des opérations d'influence.

B. Responsables politiques

21. Un délai de carence dans l'embauche de responsables politiques, hauts fonctionnaires et autres dirigeants par des entreprises (publiques) étrangères, combiné à des règles de transparence plus strictes et à la publication des partenariats, constitue une mesure effective pour empêcher que les élites politiques, économiques et culturelles soient influencées par des intérêts étrangers.

22. Les zones grises constituent un terreau fertile pour l'ingérence et doivent par conséquent être limitées.

en inlichtingendiensten om te bepalen of er sprake is van een daadwerkelijke intentie om buitenlandse belangen te dienen.

D. Repressieve maatregelen

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

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

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

II. TRANSPARANTIE

A. Sociale media

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

B. Politici

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

22. Inmenging gedijt in de schemerzone, daarom moet de schemerzone beperkt worden. Hiertoe moeten

À cet effet, il importe d'élaborer au plus vite des directives déontologiques plus claires en matière d'indemnités, de voyages, de repas, de cadeaux, etc. Pour éviter que les zones grises ne donnent lieu à des abus, il est important de disposer de lignes directrices précises et strictes et d'un code de conduite contraignant et assorti de sanctions en cas de non-respect. Des codes de déontologie devraient être établis dans chaque parlement à cet effet. Ces règles pourraient entre autres imposer une obligation de signalement de contacts étrangers bien définis, ainsi qu'un registre des cadeaux d'affaires et même des voyages offerts.

Dans le respect de l'autonomie des parlements, ces règles doivent en outre être harmonisées au maximum entre les assemblées et instances du pays.

Nous recommandons dans ce cadre l'instauration d'un registre de transparence, à l'image de celui qui existe au niveau de l'UE. Il s'agit d'une base de données répertoriant toutes les organisations qui agissent (ou tentent d'agir) pour influencer les activités législatives et politiques de l'UE. Lorsqu'une personne est approchée par une tierce partie, elle peut toujours vérifier dans ce registre si cette organisation est légitime et quel est son objectif. Un tel registre peut contribuer à ce que chacun sache clairement qui est à l'origine d'une certaine action de *lobbying*.

23. Il faut prévoir un cadre strict pour les investissements étrangers, à l'attention des dirigeants d'entreprises, en particulier lorsque l'acquisition d'infrastructures critiques ou stratégiques est en jeu.

    Il faut clarifier les règles et procédures applicables aux acquisitions étrangères et investir dans un système de filtrage des investissements étrangers qui identifie les secteurs stratégiques sensibles, qui évalue les risques potentiels et qui examine les acquisitions en fonction de l'évaluation de la menace pour la sécurité nationale.

24. Il faut identifier les technologies sensibles et renforcer leur protection, tout en veillant à ne pas nuire à la collaboration internationale en matière de recherche et développement.

25. La transparence du financement des partis politiques et des campagnes médiatiques dans le cadre

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

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

Wij bevelen binnen dit kader aan om een transparantieregister op te zetten zoals ook de EU er één heeft. Het betreft een databank waarin alle organisaties vermeld worden die zich bezighouden met het (trachten te) beïnvloeden van de wetgevende en politieke activiteiten van de EU. Wie benaderd wordt door een derde partij, kan steeds in dit register nagaan of het hier om een legitieme organisatie gaat en wat haar oogmerk is. Dit kan helpen om het voor iedereen duidelijk te maken wie er achter een bepaalde lobbyactie zit.

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

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

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

25. De transparantie van de partijfinanciering en mediacampagnes naar aanleiding van verkiezingen

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.

C. ONG, lobbyistes, etc.

26. Il convient d'élaborer une législation qui limite le financement étranger de campagnes politiques ou impose des obligations de transparence aux lobbyistes, sans aller cependant aussi loin que le *Foreign Agents Registration Act* aux États-Unis. Le législateur national est libre d'adopter des lois plus strictes que les normes internationales. 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.

27. 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.

28. 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.

29. Le financement et la représentation étrangers en matière de *lobbying* doivent être plus transparents. Il est nécessaire que des mesures législatives soient adoptées à cette fin au niveau européen. 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.

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

C. Ngo's, lobbyisten, enz.

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

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

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

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

III. ACTIONS JURIDIQUES

A. Niveau national

30. Il faut, à court terme, examiner avec le monde universitaire la manière dont on peut mettre fin aux revendications de droit d'auteur hostiles (les «*hostile copyright claims*»). Il y aurait lieu d'élaborer une procédure de révision rapide pour les fausses accusations de plagiat, afin d'éviter que des informations légitimes présentant un intérêt sociétal soient retirées d'internet à tort. Une telle mesure doit être prise à l'échelon européen, dès lors que les droits d'auteur sont régis par une directive européenne.

31. Pour relever efficacement le défi que posent les opérations de renseignement étrangères, nous recommandons que les services appropriés reçoivent un mandat clair pour ce faire. En outre, ces services doivent être dotés des compétences juridiques nécessaires pour pouvoir agir avec rigueur et détermination.

32. Nous recommandons de rationaliser le processus de passage d'un «dossier de renseignement» vers un «dossier judiciaire», de sorte que la transition se déroule sans accroc dès que des preuves suffisantes d'une infraction ont été récoltées. L'efficacité s'en trouve accrue dès lors que l'information est transmise plus aisément au parquet, ce qui permet de prendre plus rapidement des mesures plus efficaces.

33. Il convient de vérifier si la nouvelle réglementation en matière d'ingérence et d'influence offre des garanties suffisantes pour garantir une approche efficace et l'imposition de sanctions.

B. Niveau international

34. Nous recommandons d'utiliser un large éventail d'angles sous lesquels aborder la question de l'ingérence étrangère, étant donné qu'elle affecte tous les aspects de notre société. La définition employée à la fois par l'UE et l'Organisation du Traité de l'Atlantique Nord (OTAN) doit servir de guide à cet égard.

35. En cas d'ingérence flagrante de pays partenaires, les autorités devront avant tout faire preuve de discrétion. Cela signifie que la question devra être traitée avec la prudence nécessaire en évitant d'éveiller l'attention des médias.

III. JURIDISCHE ACTIES

A. Nationaal

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

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

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

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

B. Internationaal

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

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

36. Pour lutter efficacement contre l'ingérence étrangère, il est essentiel de combiner démantèlement et réglementation. Cela inclut l'identification de méthodes permettant de mettre fin à des situations spécifiques, ce qui constitue souvent un grand défi, et pas seulement sur le plan juridique. Différents instruments peuvent être mis en œuvre sur le plan numérique, y compris la législation européenne sur les services numériques, dont les principaux fondements sont la transparence et la responsabilité.

37. Nous recommandons que la Belgique entame 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.

38. Le règlement sur les services numériques (*Digital Services Act* – DSA) qui vient d'être adopté impose des obligations en matière de transparence des algorithmes dans les médias sociaux et de signalement des contenus nuisibles. Il s'agira toutefois d'évaluer rapidement la pertinence de ce règlement.

39. Pour assurer une bonne gouvernance algorithmique, il importe de fournir un cadre qui soit démocratiquement acceptable. En y associant non seulement les dirigeants politiques, les responsables de la stratégie de sécurité, mais également les citoyens, on se donne les conditions pour qu'il fonctionne bien.

40. La situation est similaire au sujet de la nouvelle directive NIS2 et de la proposition de règlement européen sur la cyberrésilience (connue sous le nom de «*Cyber Resilience Act*»). 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.

IV. RENFORCER LES ACTEURS CLÉS DE LA LUTTE CONTRE LES INGÉRENCES

A. Au plan national

41. 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

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

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

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

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

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

IV. DE BELANGRIJKSTE ACTOREN IN DE STRIJD TEGEN INMENGING ONDERSTEUNEN

A. Nationaal

41. Analoog naar het Franse voorbeeld is het van groot belang om het werkterrein van de inlichtingendiensten (en dus ook de Cel voor financiële

des informations financières (CTIF)) avec la plus grande précision et de définir celui-ci de manière approfondie.

42. La détection plus efficace des interférences nécessite un nouveau renforcement de notre appareil de renseignement, en termes tant de capacité en personnel que de ressources de travail.

43. Nous recommandons de relever les défis organisationnels en procédant à une évaluation approfondie des besoins spécifiques pour faire face aux formes nouvelles d'ingérence facilitées par les réseaux sociaux, l'intelligence artificielle, les technologies *spyware*. Une amélioration de nos services spécialisés doit tenir compte non seulement des besoins en personnel, en forte croissance, mais aussi de la capacité d'absorption afin de garantir l'efficacité des services. Outre le fait de prévoir des moyens suffisants, nous recommandons aussi de définir une stratégie claire, reposant sur des priorités et des objectifs précis, afin de garantir un fonctionnement efficient et ciblé. Les procédures d'engagement de personnel doivent prendre davantage en compte les exigences et les sensibilités propres des différentes fonctions au sein de chaque organe de sécurité. Il sera possible ainsi de prévoir de manière adéquate les moyens humains et matériels nécessaires pour pouvoir détecter, surveiller et contrer les phénomènes en constante évolution.

44. Il faut aussi investir davantage dans le renforcement de la capacité de contre-renseignement (CI) et dans les services de sécurité. Il est crucial de soutenir davantage la lutte contre le terrorisme, qui bénéficie depuis peu d'une attention prioritaire, et de faire face aussi aux menaces émergentes telles que le contre-espionnage.

45. Le renforcement de la lutte contre la corruption est aussi essentiel, car elle constitue un indicateur clair de risque d'ingérence. Cette lutte s'organise également, et de plus en plus, au niveau européen, avec les demandes du Parquet européen. Nous recommandons en outre 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.

46. Nous recommandons la mise en place d'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

informatieverwerking (CFI)) zo nauwkeurig mogelijk af te bakenen en grondig te definiëren.

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

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

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

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

46. We bevelen aan om een nauwere samenwerking te stimuleren tussen technologiebedrijven, die na *screening* (of via een federaal bestek) als «veilig» worden bestempeld, alsook cybersecurity-experts en overheidsinstanties om voortdurend de nieuwste

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. Cela pourrait donner lieu, entre autres, à des mises à jour régulières des protocoles de sécurité et à l'identification des vulnérabilités des systèmes d'exploitation mobiles, par exemple aux logiciels espions tels que *Pegasus*.

47. Nous recommandons de laisser l'espace nécessaire 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*). Un grand nombre de médias traditionnels et d'organisations ont déjà développé diverses initiatives dans ce domaine. L'objectif est de confronter les informations fausses ou manipulées à des faits vérifiés.

48. En Belgique, la coordination et la concertation entre les divers 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.

49. Pour accroître l'efficacité, il faut une coopération plus étroite entre les différents 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.

spyware-technologieën en -methoden te monitoren en tegen te gaan. Dit kan onder meer resulteren in regelmatige *updates* van beveiligingsprotocollen en het identificeren van kwetsbaarheden in mobiele besturingssystemen, bijvoorbeeld in spionagesoftware zoals *Pegasus*.

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

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

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

B. Au plan international

50. Le cadre européen est un cadre tout à fait important pour la prévention des ingérences et la protection des enjeux stratégiques de l'Europe et de chacun des pays membres. Nous plaidons pour une collaboration étroite avec les instances européennes afin de ne pas laisser la seule responsabilité et l'entière autonomie d'action aux États membres.

51. En outre, nous recommandons que les pays européens mettent 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.

52. 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.

53. Au-delà de l'ingérence qui vise directement la Belgique, il est important de tenir compte aussi des entreprises qui sont vulnérables face à l'ingérence, *a fortiori* si celles-ci travaillent avec des données ayant une valeur stratégique. Cela pourrait donc, par extension, être préjudiciable à la Belgique.

    Pour lutter contre l'ingérence économique, il faut veiller à renforcer la résilience de notre économie, de notre société et de nos territoires.

54. La menace internationale exige aussi une réponse internationale 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

B. Internationaal

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

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

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

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

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

54. Ook de internationale dreiging vereist een eensgezind internationaal antwoord. Daarom is een blijvende samenwerking met overkoepelende strategische actoren van groot belang. Voorbeelden hiervan zijn het intensiveren van de samenwerking met bestaande internationale organisaties, zoals de Verenigde Naties, de NAVO en de Organisatie voor veiligheid en samenwerking in Europa (OVSE), om gezamenlijke initiatieven te ontwikkelen ter

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.

55. Nous recommandons que les organisations internationales et les gouvernements fassent pression sur les entreprises qui développent et vendent les logiciels espions afin de garantir la transparence et de les rendre responsables juridiquement.

bevordering van democratische stabiliteit en het voorkomen van inmenging. Dit omvat ook een constructieve diplomatieke benadering op zowel nationaal als Europees niveau, waarbij politici van zowel de meerderheid als de oppositie betrokken worden.

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

Imprimerie centrale – Centrale drukkerij