SÉNAT DE BELGIQUE

La lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique

RAPPORT D'INFORMATION

19 avril 2024

COLOPHON

Le texte peut être téléchargé à l'adresse suivante:
http://www.senat.be

Deze tekst is ook in het Nederlands beschikbaar.

Secrétariat de la commission du Renouveau démocratique, de la Citoyenneté et des Affaires internationales
comcivitas@senate.be
02/501 71 11

Éditeur responsable:
Gert Van der biesen, secrétaire général du Sénat
Place de la Nation 1, 1009 Bruxelles

Cette publication n'a qu'une valeur informative. Bien qu'elle ait été rédigée avec le plus grand soin,
ni le Sénat ni ses services ne sauraient être tenus pour responsables de son contenu.

Dépôt légal: D/2025/3427/1

La lutte contre les ingérences de puissances étrangères visant à saper les fondements de l'état de droit démocratique

RAPPORT D'INFORMATION

19 avril 2024

Rapport fait au nom de la commission du Renouveau démocratique, de la Citoyenneté et des Affaires internationales

Rapporteurs:
M. Coenegrachts, Mme Ryckmans en M. Freches

Composition du comité d'avis:
Président: Rodrigue Demeuse
Membres:
N-VA: Andries Gryffroy, Freya Perdaens, Nadia Sminate
Ecolo-Groen: Rodrigue Demeuse, Chris Steenwegen, Farida Tahar
Vlaams Belang: Adeline Blancquaert, Bob De Brabandere, Guy D'haeseleer
PS: Philippe Courard, Latifa Gahouchi, Laurent Léonard
MR: Véronique Durenne, Gregor Freches
CD&V: Kris Poelaert, Orry Van de Wauwer
Open Vld: Steven Coenegrachts, Willem-Frederik Schiltz
PVDA-PTB: László Schonbrodt, Ayse Yigit
Vooruit: Ludwig Vandenhove

SÉNAT DE BELGIQUE

Session de 2023-2024
19 avril 2024
Dossier n° 7-344

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

Dossier parlementaire:
7-344/1: Demande d'établissement d'un rapport d'information
7-344/2: Rapport fait au nom de la commission
7-344/3: Constatations et recommandations adoptées par la commission
7-344/4: Auditions

TABLE DES MATIÈRES

I. MOT D'INTRODUCTION 7

II. CONSTATATIONS 9

I. Cadre légal

II. Discussion générale 10

III. RECOMMANDATIONS 27

IV. AUDITIONS 37

LES RAPPORTS D'INFORMATION DU SÉNAT: 39
https://www.senate.be/rapportsdinformation

I. MOT D'INTRODUCTION

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

L'un des moyens souvent utilisé pour une telle ingérence est la désinformation. C'est la raison pour laquelle le présent rapport d'information peut être considéré comme une suite logique du rapport sur les infox (*fake news*) (doc. Sénat, no 7-110/1 à 4). Pour autant, l'ingérence étrangère ne se limite pas à la manipulation d'informations par le biais des médias traditionnels et des réseaux sociaux, ni à la manipulation de données sur internet. Elle inclut également l'utilisation abusive de la technologie à des fins de déstabilisation, comme les cyberattaques, le piratage informatique (*hacking*) ou le recours à l'intelligence artificielle, aux vidéos hypertruquées (*deepfakes*), aux logiciels espions (*spyware*), aux armées de trolls et aux bots. L'ingérence étrangère peut aussi se traduire par le financement secret de partis politiques, d'hommes d'affaires ou autres. Enfin, elle peut passer par la coercition économique ou par une volonté de déstabiliser la société civile, par exemple par l'intermédiaire d'universités, d'organisations non gouvernementales (ONG), de groupements religieux ou de la diaspora.

Par tous ces moyens, les instigateurs d'ingérence tentent de perturber le débat démocratique au sein de la société, de fausser ou manipuler des élections et de polariser la société afin de nuire à la cohésion de la société en tentant de la rendre ingouvernable.

L'objectif du présent rapport d'information, à savoir la lutte contre les ingérences qui visent à miner les États de droit démocratiques, revêt donc une grande importance dans le contexte politique actuel. Il s'agit de veiller à ce que nos élections demeurent libres et intègres, que les droits humains individuels continuent à être respectés, que les instances démocratiques et que les États respectant les principes de l'état de droit puissent continuer à exercer leurs missions de manière viable.

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

Le présent rapport d'information entend apporter sa pierre à l'édifice. C'est ainsi que, dans un premier volet, il énonce une série de constatations qui dressent un état des lieux du phénomène en tant que tel. Les dangers et les points d'attention, tels qu'ils ont été exposés par les vingt-six personnes qui ont pris la parole lors des auditions, y sont aussi

mentionnés. Dans un second volet, le rapport formule des recommandations à destination de l'ensemble des citoyens et des pouvoirs publics qui doivent permettre de cerner et de combattre plus efficacement ce phénomène qui se développe généralement sous les radars.

Le président,
Rodrigue DEMEUSE

Les rapporteurs,
Steven COENEGRACHTS
Hélène RYCKMANS
Gregor FRECHES

II.

CONSTATATIONS

I. CADRE LEGAL

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));

   - 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].

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

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 contre-mesures nationales, les motivations et objectifs des agresseurs et les effets des algorithmes.

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].

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

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).

II. DISCUSSION GENERALE

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 désinformatione[15].

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, Sûreté de l'État (VSSE).
12. M. Dirk Janvier, commissaire divisionnaire, SGRS.
13. Rapport annuel de la Sûreté de l'État, 2019, p. 18.
14. Mme Sofia Collignon, *lecturer* (professeure adjointe), *School of politics and IR, Queen Mary University of London.*
15. M. Dirk Janvier, commissaire divisionnaire, SGRS.

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].

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].

    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

16. M. Dirk Janvier, commissaire divisionnaire, SGRS.
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. M. Kenneth Lasoen, *lector intelligence and security,* Département des Sciences politiques, *Universiteit Antwerpen.*

(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 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:

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).

- 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 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:

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.*
25. M. Kristof Clerix, journaliste d'investigation, *Knack.*

- 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].

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 la cyberintrusion

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 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].

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

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].

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 dés-

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.*
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.*

Data Breach
Cyber Attack

information, 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.

    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

39. Mme Sofia Collignon, *lecturer (assistant professor)*, *School of politics and IR, Queen Mary University of London.*
40. Raphaël Kergueno, *senior policy officer, Transparency International EU.*
41. M. Dirk Janvier, commissaire divisionnaire, SGRS.
42. Lutz Güllner, *Head of Strategic Communications, European External Action Service* (EEAS).

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 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 anglosaxon 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 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

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

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 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 parfois, et le sera sans doute de plus en plus à l'avenir, opérée par des

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.*
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.*

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 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

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.*
52. M. Kristof Clerix, journaliste d'investigation, *Knack.*
53. M. Kristof Clerix, journaliste d'investigation, *Knack.*

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 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 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,

54. Mme Ivana Karásková, *European China Policy Fellow, Mercator Institute for China Studies.*
55. De heer Gert Vercauteren, directeur a.i., *OCAD.*
56. De heer Lutz Güllner, *Head of Strategic Communications, EEAS.*
57. M. Peter Lanssens, directeur de l'analyse, VSSE.
58. Comité permanent R: Rapport d'activités 2020, p. 22 et suiv.

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 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'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.

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

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 cyber-sécurité 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 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 cyber-

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

sécurité 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 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].

63. Prof. dr. Alexander Mattelaer, *vice dean research, Brussels School of Governance, Vrije Universiteit Brussel.*
64. M. Michel Liégeois, professor, 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.*

STOP
PIRACY
copyright
all rights reserved

III.

RECOMMANDATIONS

I. CONCEVOIR ET METTRE EN ŒUVRE DES STRATEGIES D'ALERTE ET DE REDUCTION 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.

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 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.

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 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. 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 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.

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.

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 CLES DE LA LUTTE CONTRE LES INGERENCES

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 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 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.

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 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.

spam
malware
adware
VIRUS ALERT !
detected
spyware
attack
phishing

IV.

AUDITIONS

Le compte rendu des auditions est publié dans le doc. Sénat, no 7 344/4. Les personnes et organismes suivants ont été auditionnés:

Le 9 janvier 2023
- Mme Sofia Collignon, *lecturer (assistant professor), School of politics and IR, Queen Mary University of London;*
- M. Kenneth Lasoen, chargé de cours «Intelligence et sécurité», Département de sciences politiques, *Universiteit Antwerpen*;
- le professeur Alexander Mattelaer, vice-doyen «recherche», *Brussels School of Governance, Vrije Universiteit Brussel*.

Le 27 janvier 2023
- M. Dirk Janvier, commissaire divisionnaire, Service général du renseignement et de la sécurité (SGRS);
- M. Peter Lanssens, directeur de l'analyse, Sûreté de l'État (VSSE).

Le 6 février 2023
- Mme Ivana Karásková, *European China Policy fellow, Mercator Institute for China Studies*;
- M. Michel Liégeois, professeur, et M. Tanguy Struye de Swielande, professeur, Institut de sciences politiques Louvain-Europe (ISPOLE), UCLouvain.

Le 27 février 2023
- M. Étienne Soula, *research analyst, Alliance for Securing Democracy* (ASD);
- M. Kristof Clerix, journaliste d'investigation au *Knack*.

Le 13 mars 2023
- le Dr. Luca Ferro, professeur assistant en droit international, *Vrije Universiteit Brussel*;
- M. Lutz Güllner, chef de division «Communication stratégique», Service européen pour l'action extérieure (SEAE).

Le 31 mars 2023
- 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), Parlement européen;
- M. Maxime Lebrun, directeur adjoint en recherche et analyse au Centre européen d'excellence pour la lutte contre les menaces hybrides.

Le 14 avril 2023
- M. Eric Snoeck, directeur général de la police judiciaire fédérale, Office central pour la répression de la corruption (OCRC);
- M. Gert Vercauteren, directeur *a.i.*, Organe de coordination pour l'analyse de la menace (OCAM);
- M. Philippe de Koster, président, Cellule de traitement des informations financières (CTIF).

Le 26 mai 2023
- M. Raphaël Kergueno, *senior policy officer, Transparency International EU*;
- M. Miguel De Bruycker, directeur général, Centre pour la cybersécurité Belgique (CCB).

Le 5 juin 2023

- M. Guy De Pauw, CEO et cofondateur, *Textgain*;
- Mme Ksenia Iliuk, experte en communication stratégique et cofondatrice de *LetsData*.

Le 19 juin 2023

- M. Paul Van Tigchelt, chef de cabinet adjoint, cabinet du vice-premier ministre et ministre de la Justice, chargé de la Mer du Nord, M. Van Quickenborne;
- M. Eric Kalajzic, directeur du Centre d'études de sécurité et de défense, Institut royal supérieur de défense (IRSD);
- M. Christopher Houtkamp, senior research fellow - responsable du programme *Connected Security (Sécurité connectée), Clingendael - the Netherlands Institute of International Relations.*

Le 20 novembre 2023

- M. Étienne Klein, directeur de recherche, Commissariat à l'énergie atomique et aux énergies alternatives (CEA);
- M. Samuel Profumo, directeur gestion des données, Radio-télévision belge de la Communauté française (RTBF).

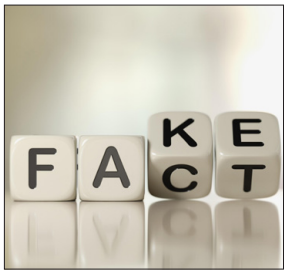
LES RAPPORTS D'INFORMATION DU SÉNAT

Tous les rapports d'informations sont disponibles sur le site :
https://www.senate.be/rapportsdinformation

LÉGISLATURE 2019 - 2024

La nécessaire modernisation de notre système démocratique en complétant la démocratie représentative par une participation accrue des citoyens dans la prise de décisions aux différents niveaux de pouvoir ainsi qu'au sein de la société

(dossier 7-117) - adopté le 18 juin 2021

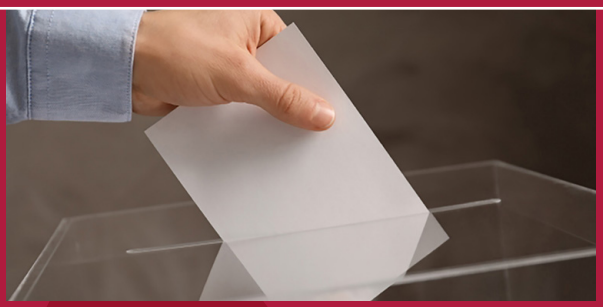


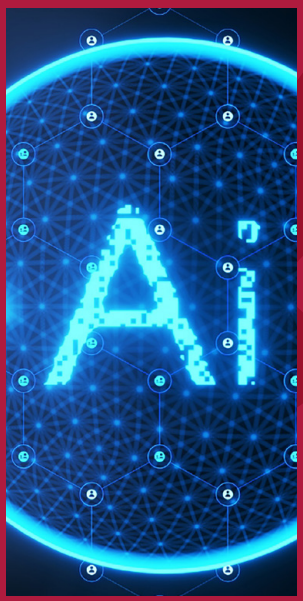
Rapport d'information concernant la nécessaire collaboration entre l'autorité fédérale et les Communautés en matière de lutte contre les infox (fake news)

(dossier 7-110) - adopté le 19 novembre 2021

Rapport d'information concernant le droit à l'autodétermination corporelle et la lutte contre les violences obstétricales

(dossier 7-245) - adopté le 15 janvier 2024




AI

DEMOCRACY

COMPUTER ERROR DETECTED
ERROR