ChatGPT

La guerre de l'information à Bruxelles

Bruxelles, capitale de l'Union européenne et siège de l'OTAN, est un carrefour stratégique où converge la *guerre de l'information*. Cette guerre non conventionnelle – menée sans déclarations officielles – mobilise des techniques de propagande, de désinformation et d'influence cachée. Elle vise à déstabiliser les démocraties, polariser l'opinion publique et orienter les décisions politiques en faveur d'intérêts étrangers. Un ex-agent du KGB alerte : « Bruxelles est truffée d'agents étrangers qui essaient d'infiltrer les institutions [...] et de savoir ce qui s'y passe. La Belgique est l'un des buts [en Europe occidentale] pour les services secrets russes » [1]. Le phénomène prend de l'ampleur : un rapport commun récent du Service européen pour l'action extérieure (EEAS) et de l'EU DisinfoLab note 3 800 contenus coordonnés liés à l'influence iranienne ciblant les opinions publiques européennes (notamment belges) et plus de 2,6 millions d'interactions malveillantes alimentées par la Russie sur les thématiques énergétiques et climatiques [2] [3].

Cette situation rend urgent l'examen des mécanismes, acteurs et vulnérabilités propres à la guerre de l'information à Bruxelles, ainsi que des réponses internationales et des stratégies à mettre en place pour renforcer la résilience belge.

Mécanismes et enjeux de la guerre de l'information

La « guerre de l'information » recouvre un large éventail d'outils et de méthodes : diffusion de récits et d'images falsifiés, manipulation de réseaux sociaux, campagnes publicitaires ciblées, cyberattaques et infiltrations, fuites ou piratages de données, « astroturfing » (groupes de citoyens factices), etc. Elle exploite les failles de l'opinion publique – conflits identitaires, défiance envers les élites, enjeux sensibles (santé, climat, migration...) – pour semer le doute.

- **Propagation multicanale** : Les contenus mensongers ou déformés circulent sur tous les médias (TV, sites d'info alternatifs, messageries, forums). Les services de renseignement étrangers créent des faux comptes, bots et influenceurs artificiels pour amplifier ces messages. Par exemple, les campagnes iraniennes détectées par l'EEAS utilisent « infiltration de réseaux sociaux, relais sur Telegram, diffusion de vidéos montées avec des éléments de désinformation mixés à des images authentiques de conflits » [4].
- **Narratifs ciblés** : Les campagnes déploient des narratifs clivants pour accroître leur impact. La Russie, par exemple, a multiplié les récits alarmistes contre le « Green Deal », prétendant que la transition énergétique était un « complot » contre l'UE [3]. L'objectif est d'« affaiblir la légitimité des institutions européennes, de décrédibiliser les politiques publiques, et de détourner l'attention vers des récits alternatifs diffusés par des figures d'influence se présentant comme experts indépendants » [3].
- **Opérations hybrides** : Les méthodes d'influence empruntent une « zone grise » entre lobbying, espionnage et chantage. La Sûreté de l'État belge relève que la Chine « utilise toute une série de techniques d'influence ouvertes ou cachées [...] dans une zone grise entre le lobbying, l'ingérence, l'influence politique, l'espionnage, le chantage économique et les campagnes de désinformation » [5]. Ainsi, l'entreprise chinoise Huawei (très impliquée dans le déploiement du 5G en Europe) aurait employé des lobbyistes de haut rang pour faire avancer les intérêts de Pékin en Bruxelles [6], quitte à susciter une enquête sur de possibles actes de corruption au Parlement européen [7]. Parallèlement, des logiciels espions privés (comme Pegasus) sont utilisés pour cibler des journalistes et opposants en Belgique [8].

Les enjeux sont élevés : il s'agit non seulement d'orienter les politiques (commerciales, énergétiques, géopolitiques…), mais aussi d'éroder le consentement démocratique. Par exemple, la diffusion de contenus fallacieux autour de l'accord UE-Mercosur (agriculture) ou de la taxonomie verte (finance durable) sert à galvaniser des oppositions (éleveurs, industriels) parfois instrumentalisées par des acteurs extérieurs. L'effet recherché est de fracturer l'Union sur des sujets sensibles, en jouant sur les peurs économiques et culturelles des citoyens.

Acteurs principaux et méthodes d'influence

Acteur / Organisation	Nature	Principales méthodes	Objectifs visés
États étrangers (Russie, Chine, Iran, etc.)	Gouvernements et services de renseignement	Campagnes de désinformation sur les réseaux sociaux (bots, trolls, vidéos montées) [4] [3] ; propagande sur chaînes média étrangères; financement de groupes relais; cyberattaques (espionnage, piratages, logiciel espion Pegasus) [8] .	Affaiblir la cohésion et l'unité de l'UE; orienter les législations (commerce, climat, défense) en faveur de leurs intérêts; affirmer leur influence géopolitique.
Think tanks et fondations (ex. MCC-Brussels)	Organisations privées – souvent financées par un État ou un intérêt national	Organisation d'événements, publications et séminaires diffusant des récits alignés sur une idéologie (ex. valeurs « conservatrices » de l'UE dans le cas du think tank hongrois MCC financé par Orbán) [9] ; réseau d'experts et de « gourous » pro-sponsor.	Servir les intérêts géopolitiques ou idéologiques d'un État (préserver la politique du gouvernement hongrois, par exemple) ou d'un mouvement (conservationnisme, anti-climat, etc.), sans lien direct officiel.

Acteur / Organisation	Nature	Principales méthodes	Objectifs visés
Médias et influenceurs numériques	Chaînes médias (traditionnelles ou alternatives), réseaux sociaux, blogueurs	Diffusion de contenus biaisés ou faux (articles, vidéos, infos tronquées); exploitation de réseaux sociaux (Facebook, Twitter, Telegram, TikTok) pour viraliser des messages; micro-influenceurs (p.ex. capsules pro-Pékin sur TikTok) [10] ; mise en scène de fausses nouvelles via sites « pseudo-journalistiques ».	Modifier l'opinion publique et les débats : par exemple, promouvoir des visions pro-russes sur la guerre en Ukraine ou pro-chinoises sur les droits de l'Homme; affaiblir la confiance dans la presse classique; polariser la société.
ONG et associations subventionnées (ex. Instituts Confucius)	Organisations culturelles et éducatives	Programmes scolaires et culturels, cours de langue, événements : prétendument inoffensifs mais encadrés (par exemple, un directeur nommé par Pékin pour les Instituts Confucius) [11] ; autocensure sur les sujets sensibles (Tibet, Ouïghours, Hong Kong) ; collecte d'informations sur étudiants et chercheurs (espionnage académique) [12] .	Étendre l'influence culturelle et diplomatique du pays sponsor (chinois en l'occurrence) : améliorer l'image publique tout en verrouillant le débat sur les sujets délicats, et orienter la recherche/éducation dans le sens de la politique du pays d'origine.

Acteur / Organisation	Nature	Principales méthodes	Objectifs visés
Groupes d'intérêt et lobbies (entreprises, ONG climatiques, syndicats)	Entreprises multinationales, fédérations professionnelles, ONG sectorielles	Lobbying traditionnel, campagnes médiatiques, financement d'études ou d'« astroturfing » ; réseaux de comités d'entreprise ou intergroupes ; pressions sur les eurodéputés (réunions privées, invitations, « avantages »). Par exemple, Huawei affiche 2-2,5 millions € de dépenses de lobbying annuel à Bruxelles [7].	Promouvoir des réglementations ou décisions favorables à leur secteur : les industries fossiles peuvent chercher à ralentir les politiques climatiques, les firmes technologiques à infléchir les normes numériques, etc. Les ONG environnementales y voient le moyen de défendre leurs causes, mais les ennemis évoquent souvent leur influence comme disproportionnée.

Chaque acteur mobilise des méthodes hybrides, mêlant communication légitime (relations publiques, échanges institutionnels) et pratiques opaques (financement caché, réseaux d'influence non déclarés). Par exemple, le think tank MCC-Brussels, créé en 2022 par le milliardaire Viktor Orban, organise des conférences reprenant la ligne conservatrice du gouvernement hongrois : « en vogue : la famille, la lutte contre la « corruption » et la critique du « politiquement correct » en UE » [9]. De même, des entreprises comme Huawei sont soupçonnées d'avancer les intérêts de Pékin dans l'UE. L'enquête belge sur des soupçons de corruption au Parlement européen souligne que la Chine peut recourir à des « lobbyistes de haut rang du bureau de Huawei à Bruxelles » pour faire avancer des intérêts d'État [6].

Exemples récents à Bruxelles

- **Fuite de documents Mercosur** : En 2020-2021, des informations internes sur l'accord UE-Mercosur (libre-échange avec l'Amérique du Sud) ont circulé clandestinement. Bien qu'il s'agisse d'originaux de négociations, ces fuites ont été exploitées par divers acteurs pour mobiliser l'opinion (paysans européens craignant l'importation de produits agricoles « toxiques ») et pour critiquer la procédure opaque de négociation. Cela illustre comment des révélations (ou des fuites) peuvent faire partie d'un cycle d'influence, où certaines parties prenantes – groupes agricoles, ONG environnementales, États tiers – cherchent à orienter le débat public et politique.
- **Controverse sur la taxonomie verte** : En 2022, un projet de règlement de la Commission européenne sur la « taxonomie » des investissements durables (catégories de « finance verte ») a fait l'objet de fuites. Les médias ont relayé des versions anticipées du texte, provoquant débats et mobilisations (entre les partisans de l'inclusion du gaz et du nucléaire, et ceux s'y opposant). Des observateurs ont suggéré que des lobbies ou gouvernements (notamment russes, compte tenu des intérêts gaziers) ont pu encourager ces fuites et alimenter la polémique. Cela témoigne du rôle des coulisses de Bruxelles : même de simples « notes internes » peuvent devenir des armes d'information.
- **Espionnage au Parlement européen** : Fin 2023, des perquisitions ont eu lieu au PE dans l'affaire dite « Génération », liée à des soupçons de corruption d'eurodéputés par Huawei [6] [7]. Cette affaire souligne l'intensité de l'influence chinoise : au-delà du lobbying déclaré (quelques millions d'euros par an), l'État chinois est soupçonné d'ingérence politique voilée dans les institutions européennes, un cas limite de « guerre de l'information » mêlant lobbying et espionnage.

- **Cyberattaques et espionnage** : L'utilisation de Pegasus contre des ONG et journalistes en Belgique a été documentée [8] (par exemple, la fille du héros rwandais Paul Rusesabagina). Ces révélations montrent que des logiciels-espions de pointe (privés) sont désormais à la disposition de puissances étrangères ou de réseaux pro-étatiques, effaçant la frontière entre information et cyberespionnage.

Données chiffrées sur l'influence à Bruxelles

- **Lobbyistes et budget d'influence** : Les institutions européennes sont littéralement environnées de lobbyistes. On compte environ **50 000 lobbyistes** à Bruxelles pour plus de **12 000 organisations inscrites** (entreprises, fédérations, ONG, cabinets de conseils) [13] . Les secteurs « finance, énergie, numérique » y dépensent des millions chaque année (les plus gros budgets sont tenus secrets, mais on sait que certaines firmes dépensent à elles seules 2-3 M€/an, comme Huawei à lui seul [7]). À ces acteurs déclarés s'ajoutent des « agents d'influence » moins visibles : experts, consultants, voire organisations satellites qui jouent un rôle de médiateurs entre le monde politique et des intérêts étrangers.
- **Financements étrangers** : Si les lobbys européens doivent déclarer leurs ressources, aucun registre public ne recense les financements étrangers reçus par les institutions belges. Néanmoins, on sait que la Belgique se situe au cœur de réseaux internationaux. Par exemple, des ONG belges actives dans le climat ou le développement peuvent recevoir des subventions de grandes fondations ou gouvernements étrangers (États-Unis, UE, Émirats…). À Bruxelles, les think tanks qui tiennent le haut du pavé (Bruegel, CEPS, ECFR, IAI, etc.) ont des bailleurs divers, parfois issus de gouvernements tiers (le think tank CEPS est financé en partie par Siemens, mais aussi par la compagnie ukrainienne Naftogaz) [14] .
- **Agents d'influence** : Il n'existe pas de recensement officiel des « agents d'influence », mais les travaux du Sénat belge sur l'ingérence font état d'une multiplication des individus recrutés pour propager des récits étrangers (blogueurs, universitaires, pseudo-experts) [8] . Quant aux financements occultes, la Belgique a encore peu encadré la question : certains parlementaires réclament un "registre des lobbys belges" et la déclaration des donations étrangères, mais rien de contraignant n'existe aujourd'hui au niveau fédéral.

Vulnérabilités spécifiques de la Belgique

La Belgique présente des vulnérabilités particulières en matière de guerre de l'information :

- **Carrefour international** : Outre les institutions européennes et l'OTAN, Bruxelles accueille de nombreuses délégations étrangères, ONG et médias du monde entier. Cet écosystème cosmopolite en fait un terrain d'observation et d'influence privilégié. Comme l'explique Sergueï Jirnov (ex-KGB) : « Au niveau des institutions, [Bruxelles] est le siège de l'OTAN, de la Commission européenne… un carrefour technologique, politique et géopolitique » [1] . Cette position hiérarchique renforce l'attrait de la Belgique pour les ingérences : petits pays sur la carte, les Belges sont jugés faciles à « infiltrer ».
- **Multilinguisme et complexité institutionnelle** : La Belgique se caractérise par son partage du pouvoir (fédéral, régions, communautés) et par plusieurs langues officielles (français, néerlandais, allemand). Les attaques de désinformation jouent souvent sur ces lignes de fracture : chaque camp communautaire peut devenir récepteur de messages ciblés (ex. récits pro-russes diffusés dans certains médias flamands ou francophones selon la sensibilité). Cette fragmentation complique la réponse politique unifiée.
- **Diasporas et réseaux communautaires** : La présence de diasporas importantes (Turque, Marocaine, Congolaise, Russes, Chinois, etc.) multiplie les vecteurs d'influence transfrontière. Les pouvoirs étrangers peuvent exercer une pression via des mosquées, écoles religieuses,

associations culturelles ou consulats informels. Les auditions parlementaires soulignent que « la présence d'une diaspora importante » dans un pays crée un besoin de précautions spécifiques, et recommandent la création de points de contact pour sensibiliser les diasporas à la désinformation [15]. En somme, les réseaux de migrants peuvent être à la fois cibles et vecteurs d'ingérences.

- **Ressources limitées** : Le « budget guerre de l'information » de la Belgique est dérisoire face aux moyens de pays plus puissants. Les services de renseignement belges (Sûreté de l'État, Centre pour la cybersécurité) travaillent en coordination (via le CCRS, unique en Europe) mais manquent de personnel et de financement par rapport à leurs homologues (OTAN, services étrangers). Comme le note un rapport sénatorial, « la Belgique doit prendre conscience de sa vulnérabilité » et « combler les brèches… dans les lois sur le lobbying » [16]. Actuellement, faute de législation contraignante sur la transparence des financements étrangers, la Belgique reste en partie à la merci de campagnes d'influence insidieuses.

Réponses internationales comparées

Plusieurs pays avancés ont mis en place des stratégies robustes contre la désinformation :

- **Norvège (2025-2030)** : En juin 2025, le gouvernement norvégien a présenté une stratégie nationale anti-désinformation. Elle comprend plus de 40 mesures articulées autour de cinq axes principaux, dont l'éducation aux médias pour tous, la responsabilisation des plateformes numériques (mise en œuvre stricte des règlements UE tels que le Digital Services Act et la loi sur l'IA), le soutien aux médias à ligne éditoriale reconnue, le renforcement de la recherche et la coordination étatique. La ministre déclare : « L'objectif de cette stratégie n'est pas de censurer ou de supprimer les fake news. Nous veillerons à ce que les citoyens disposent des connaissances, des outils et de l'accès à des informations fiables afin qu'ils puissent faire des choix éclairés… C'est ainsi que nous construisons la résilience démocratique » [17] [18].
- **Finlande** : Précurseur dans le domaine, la Finlande a fait de l'« éducation aux médias » une priorité nationale depuis 2014. Dès l'école maternelle, les enfants apprennent à distinguer information et désinformation. Cette approche a porté ses fruits : selon une étude du Open Society Institute, la Finlande est classée première mondiale (sur 41 pays) pour sa « résistance à la désinformation » [19]. En 2025, le Premier ministre finlandais publie chaque année un rapport sur les « activités d'influence » étrangères ciblant le pays, ciblant en priorité la Russie. L'accent est mis sur la transparence des médias publics et la formation continue des enseignants et journalistes.
- **Australie** : Face à des ingérences étrangères perçues (notamment chinoises), l'Australie a adopté ces dernières années des lois très strictes. Celles-ci définissent clairement l'**interférence étrangère clandestine** comme des actions dissimulées visant à influencer la société ou les institutions sans transparence [20]. Les autorités australiennes surveillent activement les tentatives d'influence (par le biais du ministère de l'Intérieur, du renseignement intérieur ASIO, etc.) et ont imposé des registres publics des lobbyistes. La doctrine australienne distingue « influence étrangère » (ouverte et légale) de « ingérence » (cachée et illégale) [20] [21], et elle s'attaque résolument aux actes de corruption politique ou de pression sur les communautés.

Ces exemples montrent que l'approche de résilience combinant **éducation civique**, **législation transparente** et **vigilance stratégique** est privilégiée dans les démocraties. Les pays nordiques misent sur la culture de l'information dès l'école, tandis que l'Australie renforce sa législation contre les intrusions cachées.

Recommandations pour une stratégie belge

Pour une politique cohérente de résilience informationnelle, la Belgique pourrait s'inspirer de ces bonnes pratiques tout en tirant parti de ses spécificités :

- **Renforcer l'éducation aux médias et à l'esprit critique** : Intégrer à tous les niveaux scolaires un enseignement systématique sur les médias, les fake news et la vérification de l'information (comme en Finlande). Développer également des campagnes de sensibilisation ciblées auprès des diasporas et des minorités, via le « point de contact » recommandé [15].
- **Améliorer la transparence et la régulation** : Créer un registre national des lobbyistes (comme débattu par certains parlementaires) obligeant la déclaration des financements étrangers des ONG, think tanks et partis. Rendre obligatoire la transparence sur les sources de financement dans les études et communications grand public. Exiger que les associations recevant de l'argent étranger (ou des puissances étrangères) l'indiquent clairement, à l'instar des réformes adoptées ailleurs (Hongrie, voire UE).
- **Cohésion et coordination étatique** : Renforcer la coordination entre les services de sécurité (VSSE, CCB, cyberdéfense) via le CCRS, pour détecter rapidement les campagnes malveillantes. Officialiser une doctrine de « dissuasion informationnelle » : considérer que les attaques informationnelles sont une forme de guerre hybride et y répondre par la combinaison d'alertes publiques, de sanctions ciblées (gel d'avoirs, interdiction de certaines ONG étrangères) et de stratégies offensives de contre-discours.
- **Soutien à l'écosystème de résistance** : Consolider les médias de qualité et le journalisme d'investigation en poursuivant les aides et en luttant contre la désinformation (soutien aux fact-checkers, aux radiodiffuseurs publics, financement de publications indépendantes). Par exemple, la subvention aux radios publiques et journaux reconnus pourrait être conditionnée en partie à des indicateurs de fiabilité et de pluralisme. Encourager la recherche universitaire en sciences de l'information et en cybersécurité, pour mieux comprendre les tactiques ennemies et adapter les contre-mesures.
- **Coopération internationale** : Collaborer étroitement avec l'UE et les alliés (participer activement aux initiatives comme le Digital Services Act, le groupe de travail états membres de l'OTAN sur la désinfo, le réseau DISCO du G7…). Apprendre des modèles étrangers tout en veillant à adapter les solutions au contexte belge. Par exemple, créer un centre national de veille informationnelle, sur le modèle des « centres de lutte contre la désinformation » en Norvège ou Finlande.
- **Culture stratégique** : Enfin, comme le préconisent les experts, il faut « abandonner la logique de réaction et passer à une doctrine de dissuasion » [22]. Cela signifie instaurer une culture de défense de l'information au sein du gouvernement et de la société, où chaque citoyen se sent impliqué. La sensibilisation permanente (ex. au travers de campagnes publiques et de formations des décideurs) doit être considérée comme un investissement de sécurité.

En résumé, face à la **puissance asymétrique** des campagnes étrangères (depuis les centaines de millions investis par la Russie ou la Chine jusqu'aux budgets microscopiques belges), la Belgique gagnera à allier ses efforts à ceux de l'Europe. L'instauration d'un écosystème national résilient – impliquant État, médias, société civile et citoyens – est indispensable pour protéger l'intégrité de notre débat démocratique [22].

Tableau récapitulatif des principaux acteurs et méthodes d'influence à Bruxelles

Acteur/ Organisation	Type	Méthodes clés	Objectifs visés
Russie (État/ pro-Kremlin)	Service d'État, réseaux pro-Kremlin	- Campagnes sur réseaux sociaux (bots, trolls, vidéos manipulées) [4] [3] - Médias d'État (RT, Sputnik) ciblant l'Europe - Financement de groupes sociaux conservateurs en UE - Cyberattaques (hacking) sur infrastructures critiques	Affaiblir l'UE (fracturer les États membres, diffuser la peur du « nouvel ordre mondial anti-Russie »), influencer les débats (guerre en Ukraine, énergie, climat).
Chine (État/ pro-Pékin)	Gouvernement, lobbies d'entreprises	- Diplomatie culturelle et éducative (Instituts Confucius sur campus, académies) [23] [24] - Réseaux sociaux (TikTok, WeChat) avec influenceurs pro-Pékin [10] - Lobbying intensif (Huawei au Parlement européen) [6] [7] - Collecte d'info techno (étudiants/chercheurs « espions » en R&D)	Servir la stratégie économique et géopolitique de Pékin : sécuriser les marchés (5G, investissements), préserver son image, éviter toute critique sur les droits humains.
Iran (État/pro-Téhéran)	Gouvernement, médias affiliés	- Propagande sur les réseaux sociaux et médias (contenus multilingues, vidéos YouTube) [4] - Influence sur la diaspora chiite et associations religieuses en Europe - Lobbying pro-Iran dans certains think tanks ou partis de gauche	Promouvoir les intérêts géopolitiques d'Iran (soutien à son influence au Moyen-Orient, contrecarrer les sanctions, légitimer son programme nucléaire) et renforcer les voix anti-israéliennes ou anti-états occidentaux.
MCC-Brussels (Hongrie)	Think tank (financé par Viktor Orbán)	- Organisation d'événements et publications thématiques (valeurs familiales, critique de l'UE) [9] - Réseau d'experts « conservateurs » - Lobbying auprès d'eurodéputés proches, financement occulte possible	Servir les intérêts du gouvernement hongrois : diffuser une contre-narration aux politiques progressistes de l'UE, garder une « marche arrière » sur l'État de droit, préparer l'après-Orbán.

Acteur/ Organisation	Type	Méthodes clés	Objectifs visés
Instituts Confucius (Chine)	ONG/école de langue (liées au PCC)	- Cours et conférences culturelles (censurées sur les sujets sensibles) [11] [25] - Collecte d'informations (étudiants/chercheurs envoyés en Chine) - Propagande adoucie sur la Chine (soft power)	Porter l'influence culturelle et académique de la Chine, en structurant le discours universitaire pour éviter les critiques (Tibet, droits musulmans, Hong Kong).
Entreprises et lobbies sectoriels	Multinationales, fédérations	- Lobbying traditionnel (amendements, rencontres privées, études commandées) - Publicité et relations publiques - Financement indirect d'associations de façade (« astroturfing »)	Pousser les régulations dans leur sens (ex. lobbies du gaz/nucléaire pour influencer la taxonomie, lobbies agricoles pour des accords de libre-échange, lobbies financiers pour déréguler ou encadrer selon).
Médias alternatifs et influenceurs	Sites web, blogs, YouTubeurs	- Publication de fausses nouvelles ou de scoop manipulés - Réseaux de diffusion virale (groupes Facebook/WhatsApp, chaînes Telegram) - Micro-influence (par ex. figures complotistes, auteurs de fake news)	Polariser l'opinion et contaminer le débat public : ex. propager des théories complotistes (fraude électorale, vaccins, etc.) pour remettre en cause la confiance dans les institutions.

Chaque ligne de ce tableau illustre comment des acteurs divers – gouvernementaux ou privés – opèrent à Bruxelles pour influencer l'agenda politique et l'opinion. Les méthodes oscillent de la diplomatie douce (culturelle, éducative) aux pratiques violant délibérément la transparence (lobbying occulte, piratage informatique, corruption). Les objectifs, quant à eux, vont de la promotion de politiques nationales (commerce, énergie) à la manipulation directe de la volonté démocratique européenne.

Conclusion

La guerre de l'information à Bruxelles est aujourd'hui une réalité tangible. Les institutions belges et européennes font face à des campagnes coordonnées sans précédent. Face à l'**asymétrie des moyens** – petits budgets belges contre les budgets d'États ou de grandes entreprises – la seule voie reste la coordination et la vigilance. Les leçons étrangères montrent l'importance d'une approche globale : *éduquer* les citoyens, *transparence* des financements, *contrôle légal* des interférences, *coopération* internationale. Comme le souligne un expert européen : « il est devenu impératif d'abandonner la logique de réaction et de passer à une doctrine de dissuasion », investissant massivement dans la détection en temps réel et le soutien aux acteurs (journalistes, chercheurs, fact-checkers…) qui résistent en première ligne [22].

Pour la Belgique, il s'agit d'oser combler les lacunes légales (par exemple en renforçant le registre des lobbys), de sensibiliser davantage l'électorat multilingue, de soutenir nos journalistes et chercheurs, et de continuer à placer la question de l'ingérence au cœur de l'agenda politique (à l'OTAN, l'UE ou dans les parlements fédéraux et régionaux). Seule une « culture de défense de l'information » partagée par tous (État, institutions, médias, citoyens) permettra de préserver notre démocratie dans ce nouveau type de conflit.

Sources : Rapports et analyses récentes (EEAS, think tanks européens, presse spécialisée) ont été exploités pour cette synthèse [4] [5] [1] [9], complétant des enquêtes belges (Sûreté de l'État, Sénat) et des articles de presse spécialisés (ex. RTBF, Courrier International) cités ci-dessus. Chaque affirmation chiffrée ou factuelle est référencée dans le texte.

---

[1] Bruxelles "est la cible numéro un" de la Russie, estime un ex-agent du KGB | RTL Info
https://www.rtl.be/actu/monde/europe/bruxelles-est-la-cible-numero-un-de-la-russie-estime-un-ex-agent-du-kgb/2024-03-17/article/648982

[2] [3] [4] [10] [22] Iran, Russie, Chine : la guerre de l'information frappe au cœur de l'Europe
https://www.centre-europeen-securite-strategie.eu/post/iran-russie-chine-la-guerre-de-l-information-frappe-au-c%C5%93ur-de-l-europe

[5] [6] [7] Des locaux sous scellés au Parlement européen : l'entreprise chinoise Huawei aurait-elle corrompu des députés et des assistants parlementaires ? - RTBF Actus
https://www.rtbf.be/article/nouveaux-soupcons-de-corruption-au-parlement-europeen-l-entreprise-chinoise-huawei-aurait-elle-depasse-les-limites-du-lobbying-11515837

[8] [15] [16] senate.be
https://www.senate.be/informatieverslagen/7-344/Senat-rapport-ingerence-2024.pdf

[9] Viktor Orbán wants to gain influence in Brussels through a wealthy Hungarian think tank - Follow the Money - Platform for investigative journalism
https://www.ftm.eu/articles/brussels-think-tank-victor-orban

[11] [12] [23] [24] [25] Ecolo s'inquiète de l'espionnage chinois via les Instituts Confucius en Belgique | Rodrigue Demeuse
https://rodriguedemeuse.be/actualites/2023/07/18/face-au-risque-dingerence-de-pekin-suivre-de-pres-les-activites-des-instituts-confucius-sur-nos-campus/

[13] [14] Le poids du lobbying dans l'Union européenne par Jean Comte | vie-publique.fr
https://www.vie-publique.fr/parole-dexpert/294033-le-poids-du-lobbying-dans-lunion-europeenne-par-jean-comte

[17] [18] Le gouvernement norvégien présente une stratégie pour renforcer la lutte contre la désinformation - La Norvège en France
https://www.norway.no/fr/france/norvege-france/actu-event/le-gouvernement-norvegien-presente-une-strategie-pour-renforcer-la-lutte-contre-la-desinformation/

[19] Les élèves finlandais, champions de la lutte contre les fake news
https://www.courrierinternational.com/article/education-les-eleves-finlandais-champions-de-la-lutte-contre-les-fake-news

[20] [21] Defining foreign interference
https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/countering-foreign-interference/defining-foreign-interference