La désinformation en Europe, état des lieux d'un champ de bataille hybride

Athénaïs Jalabert-Doury

Directrice du département Lutte informationnelle et influence de l'Institut d'études de géopolitique appliquée

18 novembre 2025

ISSN : 2739-3283

Comment citer cette publication :

Athénaïs Jalabert-Doury, *La désinformation en Europe, état des lieux d'un champ de bataille hybride,* Institut d'études de géopolitique appliquée, Paris, 18 novembre 2025.

66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org

Sommaire

Introduction 2
L'information, un nouveau champ de conflictualité en Europe 3
Une évolution structurelle de la mence 3
Une vulnérabilité européenne croissante 4
Étude d'un champ de bataille en mutation 6
Des acteurs multiples et des objectifs asymétriques 6
Des vecteurs parfois invisibiles mais efficaces 7
Quelle réponse européenne, entre souveraineté cognitive et résilience stratégiques ? 8
Entre prise de conscience et stratégie défensive 8
Vers une culture stratégique de l'influence et de la résilience à inventer 9
Conclusion 11
Bibliographie 12

Introduction

La désinformation au sein de l'espace européen constitue aujourd'hui un enjeu majeur pour la démocratie, 82 % des Européens estimant que les fausses informations représentent une menace pour le fonctionnement démocratique, et 77 % pour leur propre pays. Par ailleurs, les dernières élections européennes de juin 2024 ont offert à des acteurs étrangers, étatiques ou privés, l'opportunité de mener des campagnes d'influence massive, à l'instar du réseau *Doppelganger*. Marshall McLuhan avait anticipé que la troisième guerre mondiale pourrait être une guerre de l'information. Cette prédiction trouve un écho particulier aujourd'hui, alors que la notion de guerre cognitive, ou « bataille pour les esprits », occupe une place centrale dans la doctrine stratégique française et européenne, illustrant que l'influence psychologique agit sur la décision bien avant l'émergence d'un conflit armé direct.

L'Union européenne (UE) se trouve confrontée à une nouvelle réalité : l'information est à la fois une cible et un vecteur d'attaque. Ce contexte est accentué par l'intensification récente du flux informationnel sur les réseaux sociaux et sur internet, et désormais par le recours croissant à l'intelligence artificielle générative, qui ouvre la voie à un affrontement informationnel constant et de plus en plus difficile à contenir. Entre fausses informations, manipulation de récits historiques et diffusion de contenus clivants ou mensongers sur les réseaux sociaux, le champ informationnel est devenu un véritable espace de confrontation stratégique entre puissances. Ces attaques, souvent d'origine étatique ou non étatique, visent à affaiblir les sociétés européennes de l'intérieur, à éroder la confiance des citoyens envers leurs institutions et à fragmenter le débat public. La Russie, par exemple, a développé une doctrine de guerre hybride où la désinformation occupe une place centrale, au même titre que les actions militaires ou économiques.

Face à ces menaces, l'UE a progressivement reconnu sa vulnérabilité et cherche à mettre en place des dispositifs de sensibilisation et de riposte. Cependant, les effets de ces mesures restent fragmentés et parfois tardifs, dans un contexte également marqué par une polarisation politique croissante. La menace s'intensifiant et se diversifiant, il apparaît nécessaire que l'UE se dote d'une stratégie cohérente et résiliente afin de préserver sa souveraineté.

Quelles sont les principales menaces et quels moyens sont utilisés pour les mettre en œuvre ? Comment les campagnes de désinformation se déploient-elles sur le continent européen ? Quel est l'écosystème des acteurs européens déjà en place pour y faire face ? Enfin, quelles réponses l'UE peut-elle et doit-elle apporter pour protéger sa souveraineté ?

L'information, un nouveau champ de conflictualité en Europe

Une évolution structurelle de la menace

La désinformation constitue un élément central des campagnes d'influence orchestrées par des acteurs étatiques ou paraétatiques, souvent en complément d'autres moyens d'action tels que des opérations cyber ou des pressions diplomatiques. L'UE considère la Russie comme le principal acteur de ce type d'opérations, tandis que la Chine adopte une approche plus discrète, mais de plus en plus affirmée grâce à la consolidation de ses capacités. Le Service européen pour l'action extérieure (SEAE) cartographie notamment l'infrastructure technique des opérations FIMI (hébergeurs, proxys, domaines miroirs), principalement utilisées par la Russie et la Chine pour déstabiliser l'espace informationnel européen et celui de ses voisins.

L'opération *Doppelganger* illustre ce phénomène : ce réseau de sites « miroirs » imitant des médias européens, destiné à diffuser des récits pro-Poutine, a été lancé en 2014 et continue ses activités depuis le début de la guerre en Ukraine en 2022, par le biais d'achats d'annonces, de clonage de pages et de relais sur X et Telegram. En Pologne, lors des élections de mars et avril 2025, 279 publications identifiées ciblaient explicitement le débat électoral : des analyses d'*EU DisinfoLab*, de chercheurs OSINT et de Meta ont démontré qu'il s'agissait de l'une des campagnes russes les plus persistantes. De même, le cas « Voice of Europe » en mars 2024 a montré que l'Autriche a condamné un site internet accusé d'avoir rémunéré des responsables politiques dans plusieurs États membres afin d'influencer l'opinion contre l'aide à l'Ukraine, juste avant les élections européennes, illustrant la convergence entre médias, financement et politique.

La Chine, de son côté, renforce ses capacités à travers des réseaux tels que « *Spamouflage* », associés à des acteurs liés à l'État, selon Meta, et opérant via des campagnes multi-canaux. Si la qualification et la quantification des opérations demeurent parfois hypothétiques, la France, via VIGINUM, a répertorié 77 opérations de désinformation russes entre 2023 et 2025, révélant une pression ciblée en réponse au soutien français à l'Ukraine. En janvier 2025, une enquête de *Graphika* a recensé un appel explicite de la Chine à renverser le gouvernement espagnol après les inondations, sous couvert de faux comptes d'ONG, illustrant la montée en puissance de la Chine et l'usage direct de l'information à des fins politiques.

La manipulation informationnelle est aujourd'hui un concept central de la guerre hybride, en particulier dans la doctrine militaire russe. Plus largement, la guerre hybride s'inscrit désormais dans une logique de guerre cognitive, où l'esprit et l'attention deviennent des cibles prioritaires. L'OTAN définit la guerre cognitive comme une attaque sur la rationalité et la prise de décision, exploitant des vulnérabilités humaines et sociotechniques. Bien que les chercheurs

peinent à établir une définition unique, tous s'accordent sur son impact stratégique au sein des démocraties.

Pour y répondre, les démocraties mettent en œuvre des instruments institutionnels de contre-récits, tels que l'*East StratCom Task Force* et l'*EUvsDisinfo*, systèmes d'alerte et de sanction FIMI issus de la coopération UE-OTAN. Ces dispositifs visent à répertorier, exposer et dissuader les opérations hostiles, tout en fournissant des outils aux États membres. En France, la doctrine interarmées de lutte informationnelle et d'influence (L2I) de 2021 formalise l'action dans l'espace informationnel et le cyberespace, intégrant détection, caractérisation et appui à la Stratcom dans la planification opérationnelle. Cet « armement cognitif » se déploie également au sein des institutions diplomatiques et civiles, ainsi que dans la recherche académique, qui analyse les schémas narratifs hostiles afin de prévenir et de sensibiliser.

Le contexte socio-technologique renforce l'intensité et l'efficacité de ces opérations, avec la multiplication des contenus sur les plateformes numériques, les systèmes de recommandation algorithmiques optimisant l'engagement et les coûts de production et diffusion réduits. Des études montrent que les fausses informations circulent plus rapidement et plus loin que le vrai, et que la charge émotionnelle ou morale des messages accroît leur viralité, particulièrement en politique. Ces mécanismes constituent des leviers puissants pour les acteurs d'influence.

L'usage massif des réseaux sociaux pour s'informer, notamment chez les 16-24 ans, accentue cette vulnérabilité. Au Royaume-Uni, une étude d'Ofcom (2024) indique que 88 % des 16-24 ans s'informent en ligne, dont 82 % via les réseaux sociaux, tandis que les médias traditionnels, jouant un rôle de filtre, touchent majoritairement un public de plus de 55 ans, réduisant la résilience aux manipulations dans le débat public.

Pour y remédier, le règlement européen sur les services numériques (DSA) constitue un outil majeur de gestion des risques systémiques liés à la désinformation. La Commission européenne a engagé des procédures formelles contre X, pour la transparence publicitaire et l'accès aux chercheurs, et contre TikTok, pour les risques pesant sur les processus démocratiques et les systèmes de recommandation, après avoir déjà relevé des infractions contre X en juillet 2024. Ces actions réglementaires témoignent de la volonté institutionnelle de garantir modération, traçabilité des annonces et accès aux données.

L'essor de l'IA générative, avec les deepfakes et la re-textualisation, a amplifié la confusion pour les utilisateurs. La France a publié une évaluation de VIGINUM sur la menace informationnelle liée à l'IA, identifiant des abus et proposant des contre-mesures telles que détection, marquage et coopération public-privé. À l'échelle européenne, des travaux expérimentaux (JRC) attestent de l'efficacité du prebunking, qui sensibilise via de courtes vidéos, et du debunking, qui démystifie des croyances jugées fausses. Ces recherches soulignent également l'importance de plans éducatifs coordonnés et standardisés à l'échelle de l'UE.

Une vulnérabilité européenne croissante

Face à la multiplication des campagnes d'influence étrangères, l'une des principales fragilités de l'UE réside dans la polarisation politique et la défiance croissante envers les institutions démocratiques. L'Eurobaromètre 102, publié à l'automne 2024, révèle que 82 % des Européens considèrent la désinformation comme une menace pour la démocratie, et 71 % estiment qu'elle

affecte directement la vie politique de leur pays. Les acteurs malveillants exploitent cette baisse de confiance publique en diffusant des récits anti-UE, anti-OTAN ou anti-vaccins.

Une vulnérabilité supplémentaire réside dans l'inégalité entre citoyens quant à la capacité d'évaluer la fiabilité des sources, autrement dit la littératie médiatique, alors même que les campagnes de désinformation continuent de se multiplier. Selon le Reuters Digital News Report 2024, seulement 23 % des Européens déclarent faire confiance aux médias en ligne, avec des écarts très marqués selon les pays.

Cette fragilité est renforcée par la dépendance de l'UE aux grandes plateformes numériques américaines, où l'essentiel du trafic informationnel transite par Google, Meta, X, TikTok et YouTube, dont les algorithmes privilégient l'engagement émotionnel au détriment de la qualité de l'information. Des recherches du *Massachusetts Institute of Technology* (MIT) montrent que les fausses informations circulent en moyenne six fois plus vite que les vraies sur X, en raison de l'architecture même des systèmes de recommandation. À cette dépendance technologique s'ajoute une saturation informationnelle : le citoyen européen est exposé en permanence à un flux continu de contenus contradictoires, non hiérarchisés ni filtrés. L'individu est ainsi confronté principalement à des opinions proches des siennes, favorisant la radicalisation et la fragmentation du débat public.

L'intelligence artificielle générative a introduit une nouvelle dimension à ces vulnérabilités. Elle permet de produire en masse des textes persuasifs, ainsi que des images et vidéos falsifiées, à faible coût et avec un réalisme croissant. L'ONG *EU DisinfoLab* alertait dès 2023 sur l'usage d'avatars numériques fictifs pour commenter en ligne, simuler une opinion publique et légitimer de faux experts. VIGINUM, en 2025, a publié un rapport détaillant l'intégration d'images générées par IA dans des campagnes russes ciblant la France et l'Allemagne, rendant leur détection quasi impossible.

Par ailleurs, les deepfakes politiques se multiplient et représentent une menace particulière à l'approche des scrutins : en Slovaquie, en septembre 2023, un enregistrement audio falsifié circulant sur Facebook et Telegram a semé le doute quelques jours avant les élections législatives, déstabilisant le débat démocratique. Des scénarios similaires ont été observés lors des élections européennes de 2024 et des présidentielles en Pologne en 2025. L'IA peut même générer de faux profils d'experts et des publications à caractère scientifique, ou simuler des interventions médiatiques, ouvrant ainsi la voie à une industrialisation de la désinformation.

Aujourd'hui, l'IA générative offre un éventail de possibilités quasi-réalistes, accentuant la défiance des sociétés envers l'information et renforçant les vulnérabilités démocratiques en Europe.

Étude d'un champ de bataille en mutation

Des acteurs multiples et des objectifs asymétriques

L'écosystème de la désinformation dans l'espace européen se caractérise par une diversité d'acteurs aux objectifs variés, souvent asymétriques, exploitant les vulnérabilités sociales, politiques et technologiques des États membres. Parmi les acteurs étatiques, la Russie demeure un acteur central, notamment via l'*Internet Research Agency* (IRA), tandis que d'autres puissances déploient des stratégies d'influence moins directes mais ciblées. La Chine, par exemple, utilise des plateformes comme TikTok pour diffuser des narratifs pro-gouvernementaux et anti-occidentaux, tandis que l'Iran mène des campagnes portant sur des sujets tels que les droits de l'homme et la politique au Moyen-Orient.

Les acteurs non étatiques sont également nombreux : militants idéologiques, trolls, fermes à clics ou influenceurs jouent un rôle déterminant. Leurs motivations peuvent être politiques, religieuses, idéologiques ou financières. Dans certains cas, des États sont soupçonnés de soutenir ces groupes non étatiques, qui disposent souvent de stratégies de communication sophistiquées et de compétences technologiques avancées, rendues possibles par des financements importants.

Les objectifs de ces campagnes sont multiples et parfois interconnectés. Elles visent d'abord à affaiblir la cohésion sociale et politique en exploitant les divisions internes d'un État, fragilisant ainsi les sociétés démocratiques. La polarisation des débats publics, l'amplification des opinions extrêmes et la réduction de la confiance des citoyens envers les institutions contribuent à créer un climat de méfiance généralisé, affectant aussi bien les médias et les entreprises que les relations interpersonnelles. Ces campagnes cherchent également à semer le doute et la confusion, en exploitant les biais cognitifs et en diffusant des informations contradictoires ou fausses, rendant difficile la distinction entre le vrai et le faux. Enfin, elles visent à influencer les processus décisionnels en orientant l'opinion publique et en affectant les politiques nationales et internationales. Pour atteindre ces objectifs, les acteurs combinent différentes tactiques : manipulation émotionnelle, exploitation des biais cognitifs et utilisation de technologies avancées pour influencer l'information.

À titre d'exemple, durant la pandémie de COVID-19, une étude de *SpringerLink* (2024) a montré que l'exposition à la désinformation sur les vaccins était associée à une baisse significative de l'acceptation vaccinale dans l'UE. Des sites tels que « The Exposé » ont diffusé des articles prétendant que les vaccins pouvaient provoquer le SIDA, des infections à l'herpès ou certains cancers. Ces informations, largement partagées, y compris par l'ancien président brésilien Jair Bolsonaro, ont été démenties par des experts en santé publique. YouTube a ainsi supprimé plus de 30 000 vidéos contenant des informations erronées ou trompeuses sur les vaccins au cours des six mois précédant mars 2021. Un rapport du *Center for Countering Digital Hate* (CCDH) a également montré que la majorité des informations erronées sur le

COVID-19 provenaient de seulement 12 individus, surnommés le « disinformation dozen », dont les audiences cumulées atteignaient jusqu'à 59 millions de personnes sur diverses plateformes.

Les acteurs de la désinformation disposent ainsi d'un avantage asymétrique : bien que leurs ressources soient limitées, ils peuvent atteindre rapidement un large public grâce à l'usage de bots, de deepfakes et de narratifs émotionnels, contournant les stratégies traditionnelles de régulation de l'information. La difficulté d'attribution des attaques ou des campagnes complique par ailleurs la mise en place de réponses efficaces. Cette asymétrie est renforcée par la vulnérabilité cognitive des populations, peu sensibilisées à détecter et à réagir face à ces manipulations.

Des vecteurs parfois invisibles mais efficaces

La désinformation au sein de l'UE ne se déploie pas uniquement à travers de grandes campagnes orchestrées par des États, mais aussi via des vecteurs plus diffus, parfois quasi invisibles, conférant un avantage stratégique considérable à ses auteurs. L'information circule dans des espaces numériques fragmentés et en constante évolution, brouillant les frontières entre sources fiables et sources manipulées.

Les réseaux sociaux demeurent le principal vecteur de diffusion des narratifs manipulés. Leur viralité repose sur des algorithmes favorisant les contenus engageants, qui suscitent d'abord l'émotion ou l'indignation. Selon le *Reuters Institute Digital News Report* 2023, plus de 54 % des Européens s'informent régulièrement via les réseaux sociaux, avec une majorité provenant des jeunes générations. Parallèlement, les messageries chiffrées, telles que Telegram ou WhatsApp, jouent un rôle croissant. Leur cryptage protège les contenus des regards extérieurs et de la régulation, facilitant la circulation de messages manipulables, y compris conspirationnistes, et rendant leur surveillance complexe. Pendant la pandémie de COVID-19, de nombreuses études ont montré que Telegram servait de canal privilégié pour diffuser des rumeurs sur l'inefficacité ou la dangerosité des vaccins, accompagnées de visuels facilement interprétables de manière erronée. Ces messageries échappent en outre aux règles de modération appliquées par l'UE aux plateformes comme Meta ou X.

Le phénomène cognitif lié à la viralité émotionnelle joue également un rôle central : les individus partagent davantage ce qui suscite une réaction émotionnelle que ce qui repose sur des faits. David Colon, dans *La guerre de l'information* (2019), souligne que la vérité est souvent reléguée au second plan, tandis que l'indignation et la peur accélèrent la diffusion. Une étude de *Vosoughi, Roy et Aral* (2018, Science) a montré que les fausses informations sur Twitter circulaient six fois plus vite que les informations vérifiées, précisément parce qu'elles généraient davantage de réactions émotionnelles. Dans le contexte européen, cela s'est illustré lors de la crise migratoire de 2015, lorsque des rumeurs virales sur des agressions attribuées à des réfugiés se sont propagées en Allemagne sur Facebook et WhatsApp, alimentant un climat de peur et de polarisation politique.

L'émotion agit ainsi comme une véritable monnaie d'échange informationnelle. Les récentes campagnes de désinformation russes et chinoises exploitent cette logique en diffusant des récits simplistes mais percutants, souvent accompagnés de contenus visuellement marquants. En suivant les « trends », c'est-à-dire les contenus populaires sur les réseaux sociaux, ces

campagnes produisent des visuels, mèmes ou vidéos courtes, adaptés aux formats réguliers des plateformes et conçus pour un impact maximal.

La manipulation de l'information, couplée aux transformations numériques, a provoqué un basculement structurel. La désinformation n'est plus ponctuelle, mais permanente. Les démocraties européennes se trouvent désormais au cœur de guerres de récits continues, où les lignes de front sont difficiles à identifier et fluctuent selon l'actualité : crises sanitaires, guerre en Ukraine, défense européenne, élections, migrations ou enjeux climatiques. Par exemple, des vidéos virales publiées sur TikTok durant la guerre en Ukraine ont été manipulées ou sorties de leur contexte, influençant significativement la perception du conflit. L'*OTAN StratCom COE* a identifié une campagne systématique de faux comptes sur TikTok et X visant à discréditer les autorités ukrainiennes et à accentuer la fatigue des opinions publiques occidentales.

Sur une autre thématique, avant les élections européennes de 2024, le *European Digital Media Observatory* a observé une recrudescence de narratifs manipulés autour du climat énergétique et des sanctions contre la Russie, visant à présenter l'UE comme affaiblie par ses propres décisions. Cette guerre des récits instaure un flux informationnel permanent, rendant difficile la distinction entre narratifs étatiques stratégiques et dynamiques organiques de polarisation sociale.

Quelle réponse européenne, entre souveraineté cognitive et résilience stratégique ?

Entre prise de conscience et stratégie défensive

Depuis une décennie, l'UE et ses États membres ont progressivement pris conscience de l'enjeu que représente la désinformation et la menace informationnelle, considérées à la fois comme des défis sociétaux et sécuritaires. Cette prise de conscience a été renforcée par une succession d'événements marquants : les campagnes de désinformation russes lors de la crise ukrainienne de 2014, l'ingérence dans les élections américaines de 2016 qui a servi d'alerte mondiale, la pandémie de COVID-19 illustrant l'ampleur des effets de la prolifération massive de fausses informations, et plus récemment le conflit israélo-palestinien.

L'UE a mis en place des instruments institutionnels et opérationnels pour lutter contre ces menaces. L'*East StratCom Task Force,* créé en 2015 au sein du Service européen pour l'action extérieure (SEAE), constitue le premier pilier de cette approche. Sa mission principale est de détecter et analyser les campagnes de désinformation via la plateforme publique *EUvsDisinfo*, qui documente depuis plusieurs années des milliers de cas de récits mensongers. Cependant, les moyens humains et financiers demeurent limités : en 2020, seulement 16 personnes y étaient affectées, selon le Parlement européen. Néanmoins, cette structure a permis d'établir une veille

institutionnelle solide à l'échelle européenne et de sensibiliser les acteurs aux enjeux géopolitiques de l'information.

Au niveau national, certains États membres ont renforcé leurs dispositifs, notamment la France avec le Service de l'Information du Gouvernement (SIG), créé en 2021, qui centralise les capacités de communication stratégique et assure un suivi renforcé des campagnes de désinformation. Le service VIGINUM a été spécifiquement mis en place pour lutter contre les manipulations de l'information provenant de l'étranger.

Parallèlement, l'UE a adopté un cadre juridique et réglementaire avancé. Le *Digital Services Act* (DSA), entré en vigueur en 2022, impose aux grandes plateformes numériques, notamment les « Very Large Online Platforms » telles que Meta, X ou TikTok, des obligations renforcées en matière de transparence algorithmique, de retrait de contenus illicites et de lutte contre la désinformation. Ce règlement complète le code de bonnes pratiques sur la désinformation, apparu en 2018 et renforcé en 2022, signé par les principales plateformes afin de limiter la monétisation des fausses informations et de signaler les contenus douteux. La Commission européenne a également lancé des mesures préventives à l'approche des élections européennes de 2024, fondées sur la coopération avec les États membres et les plateformes pour détecter les discours hostiles. Enfin, la législation émergente sur l'intelligence artificielle, notamment le projet de règlement *AI Act*, intègre des dispositifs visant à encadrer l'usage de l'IA générative afin de prévenir les risques liés aux deepfakes et aux manipulations automatisées.

Malgré ces avancées, l'opérabilité de ces dispositifs reste limitée. L'UE est critiquée pour sa réactivité jugée trop lente face à la rapidité des campagnes de désinformation, lesquelles exploitent la viralité des réseaux sociaux. Une infox peut atteindre des millions de personnes en quelques heures, tandis que la réaction institutionnelle est souvent tardive et conditionnée par la complexité de la coordination politique entre États membres, organes de l'UE et acteurs privés. Cette coordination reste inégale : certains États, comme la Finlande ou les pays baltes, investissent massivement dans la lutte informationnelle, tandis que d'autres hésitent à mobiliser des moyens significatifs, fragmentant la résilience globale.

Le cadre juridique demeure également flou, le DSA et le code de bonnes pratiques reposant largement sur la coresponsabilité avec les plateformes privées, laissant place au lobbying et à l'interprétation des GAFAM. Ces acteurs conservent une position dominante dans la régulation des flux d'information, soulevant des questions de souveraineté européenne. Peut-on envisager une capacité d'action autonome tant que le champ informationnel dépend largement des plateformes et algorithmes non européens ? Par ailleurs, les initiatives de fact-checking et d'éducation aux médias, bien qu'existantes et en développement, restent dispersées et peu visibles pour le grand public.

Vers une culture stratégique de l'influence et de la résilience à inventer

Le véritable défi pour les années à venir réside dans la construction d'une véritable culture stratégique de l'influence et de la résilience, au-delà de la simple dotation d'outils défensifs pour contrer la désinformation. Il ne s'agit plus seulement de réagir, mais de structurer une approche proactive et préventive, capable de renforcer la cohésion interne des sociétés européennes et de consolider une autonomie stratégique européenne.

L'éducation des citoyens à la résilience informationnelle constitue un levier essentiel. Des enquêtes montrent que la vulnérabilité à la désinformation est corrélée au niveau de littératie médiatique et de confiance envers les institutions. Selon le *Reuters Institute* (2023), seuls 37 % des Européens déclarent faire confiance aux médias d'information, chiffre en forte baisse sur les cinq dernières années. Cette méfiance favorise la circulation de récits mensongers, souvent émotionnels et viraux, au détriment des discours institutionnels. Une solution consiste à intégrer l'éducation aux médias dès l'école, comme l'a expérimenté la Finlande depuis 2016 avec son programme national *Media Literacy*, associant enseignants, journalistes et chercheurs pour développer l'esprit critique face aux fausses informations. Les résultats sont probants : la Finlande est régulièrement classée comme l'État européen le plus résilient face à la désinformation, selon le *Media Literacy Index*.

La société civile joue également un rôle central dans ce combat. Des ONG, telles que EU *DisinfoLab*, traquent et exposent les campagnes de désinformation, comme l'opération *Indian Chronicles* en 2020, qui révélait un vaste réseau de faux médias pro-indien ciblant les institutions européennes. Par ailleurs, les réseaux de fact-checking coordonnés par l'*European Digital Media Observatory* (EDMO) permettent de mutualiser les expertises d'universitaires, de journalistes et d'acteurs technologiques. Ces initiatives montrent que la société civile peut constituer un écosystème de vigilance efficace, qui gagnerait à être davantage soutenu par les pouvoirs publics.

Il est également nécessaire d'aller au-delà de la seule défense et d'instaurer une gouvernance stratégique centralisée de la lutte informationnelle. Une telle stratégie pourrait s'articuler autour d'une doctrine européenne de la résilience informationnelle et de l'influence. La Russie a formalisé dès 2013 une doctrine informationnelle offensive avec la doctrine Gerasimov, alors que l'UE conserve une approche défensive, marquée par la crainte d'atteindre à la liberté d'expression. L'objectif n'est pas de censurer les citoyens, mais de produire des récits mobilisateurs capables de renforcer la légitimité des institutions démocratiques. Bruno Tertrais écrivait en 2021 : « L'influence n'est pas un gros mot : elle constitue une arme de souveraineté dans un monde de rivalités systémiques. » L'UE pourrait développer une stratégie narrative centrée sur ses valeurs fondamentales (démocratie, État de droit, solidarité) et les traduire en politiques de communication cohérentes, tant pour ses citoyens que pour ses partenaires internationaux.

L'UE finance déjà des programmes de formation à la communication stratégique pour les diplomates et les communicants institutionnels, notamment via le réseau StratCom du SEAE. L'OTAN a également développé un *StratCom Centre of Excellence* à Riga, proposant analyses et formations pratiques pour renforcer les capacités des États membres.

Instaurer une culture européenne de l'influence suppose de combiner trois dimensions : la résilience sociétale par l'éducation et la sensibilisation, la vigilance partagée via un écosystème associant société civile, institutions et chercheurs, et enfin l'offensive narrative par une stratégie politique coordonnée. Dans un monde où « l'espace informationnel est devenu un véritable champ de bataille, où la guerre cognitive fait rage et où la désinformation est une arme utilisée de manière décomplexée », comme le souligne Olivia Pénichou, directrice de la Délégation à l'information et à la communication de la Défense (DICoD) du ministère français des Armées, la souveraineté cognitive ne pourra être atteinte qu'en considérant l'influence non comme une menace pour la démocratie, mais comme l'un de ses instruments essentiels.

Conclusion

La désinformation n'est plus un phénomène marginal, mais constitue un véritable champ de conflictualité stratégique, où l'information elle-même devient à la fois une cible et un instrument utilisé par des acteurs étatiques et non étatiques pour affaiblir la cohésion nationale, fragmenter le débat public et réduire la confiance des sociétés envers les institutions démocratiques. Des épisodes récents, tels que l'opération *Doppelganger* ou les campagnes multi-canaux de la Chine via le réseau *Spamouflage*, illustrent que les campagnes d'influence peuvent atteindre des millions d'individus en quelques heures, exploitant la viralité des algorithmes. L'information devient ainsi un champ opérationnel où l'esprit et l'attention des populations sont ciblés bien avant tout conflit armé direct.

Face à cette menace structurelle et multidimensionnelle, l'UE dispose d'outils institutionnels et législatifs prometteurs (l'*East StratCom Task Force*, *EUvsDisinfo*, VIGINUM), ainsi que les régulations émergentes sur l'intelligence artificielle, mais leur efficacité demeure limitée par des contraintes de coordination politique, de moyens humains et financiers, ainsi que par la dépendance aux plateformes numériques étrangères. La fragmentation des initiatives, la rapidité des campagnes de désinformation et la saturation du flux informationnel exposent particulièrement les sociétés, et notamment les jeunes, à une vulnérabilité accrue. L'émergence de l'IA générative, capable de produire des contenus massifs et quasi réalistes, accentue cette fragilité et complique encore la distinction entre information véridique et manipulation.

Le défi pour l'UE consiste donc, au-delà de la simple défense, à construire une véritable souveraineté cognitive européenne. Cela implique une approche holistique de la menace, combinant éducation aux médias et résilience informationnelle, le renforcement des capacités de la société civile et des réseaux de fact-checking. L'aspect politique est primordial, à la fois pour assurer la coordination des décisions et pour impulser une doctrine européenne de l'influence centrée sur la résilience sociétale, la vigilance collective et l'offensive narrative. Cette approche permet de constituer une base stratégique coordonnée, garantissant à la fois la cohésion interne et la souveraineté de l'UE face aux ingérences étrangères.

L'information n'est donc plus seulement un vecteur communicationnel classique, mais un véritable champ de conflictualité, où les capacités à protéger, analyser, sensibiliser et influencer deviennent essentielles à la souveraineté.

Bibliographie

Brennen, J. S., Simon, F., Howard, P. N., & Nielsen, R. K. (2021). *Types, sources, and claims of COVID-19 misinformation.* Reuters Institute for the Study of Journalism.

Center for Countering Digital Hate (CCDH). (2021). *The Disinformation Dozen.* CCDH Report.

Centre européen de sécurité et de stratégie. (n.d.). *Souveraineté cognitive et résilience stratégique : l'Europe face à l'impact des réseaux sociaux.* https://www.centre-europeen-securite-strategie.eu/post/souveraineté-cognitive-et-résilience-stratégique-l-europe-face-à-l-impact-des-réseaux-sociaux

CLEMI. (n.d.). *Programme européen DE FACTO : comprendre et lutter contre la désinformation.*https://www.clemi.fr/europe-et-international/programme-europeen-de-facto-comprendre-et-lutter-contre-la-desinformation

Colón, D. (2019). *La guerre de l'information.* Paris : CNRS Éditions.

Colón, D. (2021). *La guerre de l'information : Les États à la conquête de nos esprits.* Tallandier.

Commission européenne. (n.d.). *Countering information manipulation.* https://commission.europa.eu/topics/countering-information-manipulation_en

Cour des comptes européenne. (2021). *Rapport spécial 09/2021 : La désinformation concernant l'UE : un phénomène sous surveillance mais pas sous contrôle.* https://www.eca.europa.eu/fr/Pages/DocItem.aspx?did=59182

DisinfoLab, EU. (2023). *The Rise of AI-Generated Disinformation.* Bruxelles : EU DisinfoLab.

EU DisinfoLab. (n.d.). *Reports and investigations on disinformation networks.* https://www.disinfo.eu/

Eurobaromètre 102. (Automne 2024). *Public Opinion on Disinformation and Democratic Trust in the EU.* Bruxelles : Commission européenne.

European Commission. (2022). *Digital Services Act (DSA).* Bruxelles : Commission européenne.

European Digital Media Observatory (EDMO). (n.d.). *Resources and analyses on disinformation in Europe.*https://edmo.eu/

European Digital Media Observatory (EDMO). (2024). *Election Monitoring Report 2024.* Bruxelles : EDMO.

European External Action Service (EEAS/SEAE). (2024). *FIMI Infrastructure Mapping : Russian and Chinese Operations.* Bruxelles : SEAE.

European Union. (2018, 2022). *Code of Practice on Disinformation.* Bruxelles : Commission européenne.

European Union. (2022). *Digital Services Act (DSA).* Bruxelles : Commission européenne.

Finberg, D. (2022). *Media Literacy Index.* Open Society Institute.

Galeotti, M. (2016). *Hybrid war or gibridnaya voina? Getting Russia's non-linear military challenge right.* Mayak Intelligence. https://ecfr.eu/article/commentary_hybrid_war_or_gibridnaya_voina/

Graphika. (2025, janvier). *Chinese Disinformation and Political Influence Operations in Europe.* Graphika Research Report.

Jeangène Vilmer, J.-B. (2020). *La guerre informationnelle.* CNRS Éditions.

Massachusetts Institute of Technology (MIT). (2024). *Social Media Misinformation and Algorithmic Spread.*Cambridge, MA : MIT.

Meta. (2025). *Spamouflage and Chinese Influence Networks.* Meta Research.

NATO Strategic Communications Centre of Excellence (NATO StratCom COE). (2022). *Russian Influence Operations in Ukraine.* Riga : NATO StratCom COE.

NATO StratCom Centre of Excellence. (n.d.). *Publications on disinformation and strategic communications.*https://www.stratcomcoe.org/

Ofcom. (2024). *Online News Consumption among 16–24 Year Olds in the UK.* Londres : Ofcom.

Petrov, A. (2022). *Information Wars : State and Non-State Actors in Disinformation Campaigns.* Springer.

Ravailhe, N. (2023). *Guerre cognitive et stratégies d'influence dans l'Union européenne.* CR451. https://cr451.fr/guerre-cognitive-et-strategies-dinfluence-dans-lunion-europeenne-par-nicolas-ravailhe/

Reuters Institute. (2023). *Digital News Report 2023.* Oxford : Reuters Institute for the Study of Journalism.

SpringerLink. (2024). *Disinformation in the COVID-19 Pandemic.* SpringerLink.

StratCom Task Force – European External Action Service (EEAS). (n.d.). *Reports on foreign information manipulation and interference (FIMI).* https://www.eeas.europa.eu/eeas/strategic-communications-and-information-analysis_en

Tertrais, B. (2021). *L'influence, une arme de souveraineté dans un monde de rivalités systémiques.* Paris : Fondation pour la Recherche Stratégique.

Tertrais, B. (2023). *Les opérations d'influence : arme de guerre moderne ?* Institut Montaigne. https://www.institutmontaigne.org/publications/les-operations-dinfluence-arme-de-guerre-moderne

VIGINUM. (2025). *Évaluation de la menace informationnelle liée à l'IA.* Paris : Service de l'Information du Gouvernement, France.

Voice of Europe. (2024, mars). *Report on Political Influence in Austria and Europe.* Vienne : VOE.

Vosoughi, S., Roy, D., & Aral, S. (2018). *The spread of true and false news online. Science*, 359(6380), 1146–1151.

Institut
EGA

ISSN : 2739-3283

Institut d'études de géopolitique appliquée
66 avenue des Champs-Élysées, 75008 Paris
Courriel : secretariat@institut-ega.org
Site internet : www.institut-ega.org