

Sciences Po Strasbourg

École

de l'Université de Strasbourg

# LA PROPAGATION DE LA DÉSINFORMATION À UN LARGE AUDITOIRE

## VECTEURS PHYSIQUES ET NUMÉRIQUES DE DIFFUSION DU DISCOURS DE DÉSINFORMATION

Ils ont rédigé ce rapport : Abd El Malek Océane, Bonnet Sarah, Corset Mathieu, Desponds Nérine, Falconnet Léo-Paul, Ghazi Tara, Nossent Louise, Perchine Zacharie, Perragin Adrien, Roudil Estelle.

Afin de propager la désinformation à une audience la plus large possible, les Etats ingérants utilisent plusieurs relais. Ces relais de désinformation peuvent être des intermédiaires influents au niveau national (1). Le contenu désinformationnel est également diffusé massivement par une utilisation efficace des outils numérique et une automatisation de cette diffusion (2). Enfin, les différentes techniques de propagation sont généralement croisées et la désinformation est diffusée via plusieurs vecteurs qui opèrent simultanément (3).

## 1. LA DIFFUSION PAR UN INTERMÉDIAIRE

En étant relayée par des intermédiaires divers qui disposent de la confiance de la population et d'une certaine autorité et/ou crédibilité, la désinformation peut atteindre un public le plus large possible. Le lien entre le relais de désinformation et sa source est souvent rendu explicite par le fait qu'il y ait un transfert d'argent. Pourtant, la motivation des intermédiaires n'est pas systématiquement d'ordre financier. Il peut s'agir de droits et de privilèges qui sont octroyés en échange de la diffusion de désinformation. Parfois même, un relais de désinformation peut avoir cette position sans en avoir conscience. Il peut par exemple être convaincu de la vérité du discours qu'il propage. Dans ce cas, sa motivation est d'ordre idéologique. Mais l'intermédiaire peut également être victime d'usurpation de son identité, dans ce cas son nom et son influence servent à la propagation d'un discours à son insu.

Ainsi, différentes sphères sont régulièrement les cibles de ceux qui cherchent des relais de désinformation. Parmi des individus crédibles et capables de transmettre le message à un grand nombre, on retrouve les sphères politiques et gouvernementales, les universités et le monde médiatique. Plus récemment, les influenceurs sur les réseaux sociaux sont également la cible d'États tentant de diffuser de fausses informations, notamment visant un public plus jeune.

## a. Les élus et sphères gouvernementales

Les élus sont des intermédiaires de choix lorsqu'il s'agit de véhiculer de fausses informations. En mesure d'orienter les décisions publiques ou les législations, ceux-ci sont en effet contactés par des États tiers à la recherche de plaidoyer en leur faveur au sein de diverses institutions. Leur influence peut être « achetée » financièrement, il est pourtant également possible que leur autorité soit utilisée à leur insu, notamment via l'usurpation de leur identité.

### L' « achat » des voix politiques par la corruption financière

La corruption par l'échange d'argent constitue une des méthodes « traditionnelles » de l'influence et de la désinformation. Elle est encore abondamment utilisée aujourd'hui. Le cas récent le plus emblématique est le scandale du Qatargate de 2022 au cours duquel l'eurodéputée grecque Eva Kailí, alors vice-présidente du Parlement européen, mais également Pier Antonio Panzeri, Président de la sous-commission des droits de l'Homme du Parlement entre janvier 2017 et juillet 2019 et d'autres acteurs de milieux proches des sphères décisionnelles (confédérations syndicales, organisations non-gouvernementales) [49] sont accusés d'avoir plaidé en faveur du Qatar, affirmant notamment son exemplarité en termes de droits des travailleurs. En parallèle étaient pourtant révélées les très mauvaises conditions de travail des ouvriers sur les chantiers de construction des infrastructures destinées à accueillir la Coupe du monde de football. En échange des voix de ces officiels, il apparaît que le Qatar leur a versé des sommes d'argent considérables. Plus d'un million d'euros en liquide ont en effet été saisis par la police fédérale belge en charge de l'enquête [50].

Le soutien financier peut d'ailleurs être accordé plus globalement à des partis politiques. Le Parlement européen mentionne ainsi de véritables « *relations de dépendances avec certains partis politiques européens* » notamment liés à leur financement et/ou à l'accord de prêt russes. Sont ainsi pointés du doigt des partis d'extrême droite, notamment l'AfD allemand et le RN français [51]. Le discours pro-russe de membres de ces deux partis semble ainsi lié, au moins en partie, à cette dépendance financière [52]. C'est ainsi via la corruption financière que les voix de diverses personnalités politiques peuvent être « achetées » et qu'il va être possible pour une puissante ingérante d'orienter le débat public.

[49] Jean-Philippe Leffief. « Qatargate » : ce que l'on sait des soupçons de corruption au Parlement européen ». *Le Monde*, 15 décembre 2022. [lien](#).

[50] Valentin Ledroit. « Qatargate : tout comprendre au scandale de corruption qui touche le Parlement européen ». *Touteurope.eu*, 3 octobre 2023. [lien](#).

[51] Parlement Européen. Proposition de résolution et résolution sur le Russiagate 8 février 2024.

[52] Romain Geoffroy et Maxime Vaudano. « Quels sont les liens de Marine Le Pen avec la Russie de Vladimir Poutine ? » *Le Monde*, 20 avril 2022. [lien](#).

## Usurper l'identité par le piratage : l'utilisation de l'influence des responsables politiques à leur insu

Il est également possible d'utiliser l'influence de personnalités politiques et de faire circuler de fausses informations en leur nom à leur insu. C'est ce que le rapport du réseau de journalistes Forbidden Stories montre dans son enquête sur l'entreprise israélienne de désinformation "Team Jorge"[53]. Leur rapport montre la capacité de l'entreprise à pirater et prendre le contrôle de messageries privées de responsables politiques (en l'occurrence de hauts responsables africains), notamment leurs adresses Gmail et leurs comptes Telegram. Il est alors non seulement possible d'avoir accès librement à tout le contenu relié à ces comptes (drive et carnet d'adresses), mais également d'usurper l'identité de la victime et d'envoyer des mails et messages à sa place et en son nom.

Cette technique aurait notamment été utilisée dans le contexte de l'élection kényane de 2022 [54]. Si une telle technique n'a, a priori, pas été utilisée à l'encontre de responsables européens jusqu'à aujourd'hui, il semble pourtant impératif d'avoir conscience de son éventualité et d'être préparés à la déstabilisation qui pourrait en résulter, notamment lors d'événements institutionnels clés tels que les élections.

## b. Les universités et la recherche

L'université est elle aussi le terrain d'action des stratégies d'influence étrangère et au sein de laquelle il est intéressant pour des puissances étrangères de diffuser de la désinformation, notamment dans le but de façonner une certaine image et une meilleure réputation étatique.

Plusieurs institutions européennes se sont saisies de la question et ont pointé du doigt ces influences. La Commission Européenne s'est notamment penchée sur la question des ingérences étrangères dans la recherche et l'innovation [55]. Au niveau national, différents organismes se sont également inquiétés de la situation, c'est le cas de la fondation suédoise pour la coopération internationale dans la recherche et l'éducation supérieure [56], ou encore le Sénat français qui a publié en septembre 2021 un rapport d'information [...] sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences [57].

[53] Cécile Andrzejewski. « "Team Jorge" : Révélations sur les manipulations d'une officine de désinformation ». Forbidden Stories (blog), 15 février 2023. [lien](#).

[54] *Ibid.*

[55] UE, « Tackling R&I Foreign Interference: Staff Working Document », 2022. [lien](#).

[56] Stefan Östlund, Tommy Shih, et Albin Gaunt. « Responsible Internationalisation: Guidelines for Reflection on International Academic Collaboration ». STINT, The Swedish Foundation for International Cooperation in Research and Higher Education, 2020. [lien](#).

[57] André Gattolin. « Rapport d'information (...) sur les influences étatiques extra-européennes dans le monde universitaire et académique français et leurs incidences ». Direction de l'information légale et administrative, Sénat, 2021. [lien](#).

C'est particulièrement la restriction de la liberté académique qui inquiète. Celle-ci se remarque dans le cas d'une dépendance financière des chercheurs à un État tiers, mais également dans le cadre de pressions quant à l'accès au territoire étudié, par exemple via l'attribution de visas.

### **Le financement étranger des universités et de la recherche, source de remise en question de la liberté académique**

Tous les rapports cités précédemment décrivent un paramètre commun : le lien entre le financement étranger des universités et la dépendance académique qui peut en résulter.

La problématique touche d'abord les chercheurs financés par une puissance étrangère. Le risque pour ces chercheurs de transformer le discours, les focus académiques voire le résultat des recherches est ainsi avéré dans le cas d'une dépendance financière à un État tiers pour la tenue des travaux de recherches.

Or, les financements étrangers abondent dans les universités européennes. La Chine est ainsi l'un des États qui finance le plus de recherches en Europe et a ainsi développé le programme « 1000 talents », exclusivement destiné à recruter des chercheurs étrangers dans des domaines scientifiques clés [58]. C'est ainsi 203 projets de recherche en République tchèque dont le financement provient exclusivement de sources chinoises. En Autriche, 284 universitaires voient également leurs recherches financées exclusivement par la Chine. Pour autant, il faut noter que le phénomène est hétérogène à travers l'Europe, en Slovaquie par exemple, moins d'une vingtaine d'universitaires sont concernés [59]. Cette dépendance financière serait rendue possible par une relative insuffisance des ressources budgétaires allouées aux chercheurs dans le contexte européen [60]. Les pays occidentaux investissent des moyens relativement importants par rapport au reste du monde. Pourtant, de fortes disparités persistent, c'est ainsi les pays anglo-saxons et d'Europe du Nord qui dotent le mieux leurs universités, tandis qu'en Europe continentale et du sud, les dépenses sont beaucoup plus restreintes [61].

---

[58] Aneta Zachová, Laura Miraglia, Pekka Vanttinen, et Sofia Mandilara. « L'ingérence croissante de la Chine au sein des universités européennes ». Euractiv, 1 décembre 2022. [lien](#).

[59] *Ibid.*

[60] *Ibid.*

[61] Julian Garritzmann. « Higher Education Funding across the Globe ». Education International, 15 mai 2024. [lien](#).

Toujours en termes d'influence financière, certaines universités, particulièrement au Royaume-Uni, sont assez largement dépendantes des inscriptions d'étudiants étrangers, notamment chinois. Les universités britanniques accueillent ainsi « davantage d'étudiants chinois que le reste de l'Europe combiné » [62]. C'est ainsi une quinzaine d'universités britanniques qui tire de l'inscription d'étudiants chinois dans leur établissements plus d'un cinquième de leurs revenus [63]. Cette dépendance crée une fois de plus une difficulté à résister aux pressions chinoises, et se manifeste par de l'auto-censure et par une forte réticence des chefs universités à émettre des critiques à l'égard du gouvernement chinois.

### **L'attribution des visas comme moyen matériel de création de dépendance**

D'autres moyens peuvent créer une dépendance des universités et chercheurs à un pays tiers. La Chine utilise par exemple sa capacité à délivrer (ou à refuser) des visas pour entrer sur son territoire comme un moyen de s'assurer une non critique du régime, ou encore pour se garantir la non évocation de thèmes sensibles, tels que le Tibet ou le Xinjiang et les Ouïghours, Taiwan, ou encore les manifestations de la place Tian'anmen. Cette politique de restriction d'accès au territoire vise surtout les spécialistes de la Chine dont le travail requiert de se rendre dans leur pays d'étude [65].

Finalement, la dépendance des universités et des chercheurs européens à un État-tiers, qu'elle soit financière ou non, est un terreau fertile pour la propagation de désinformation au sein de la sphère universitaire.

**La désinformation dans le cadre universitaire prend souvent la forme d'une « auto-censure » des chercheurs quant aux thèmes abordés et aux conclusions données.**

---

[62] Charles Parton. « China-UK Relations: Where to Draw the Border Between Influence and Interference? » Royal United Services Institute for Defence and Security Studies, février 2019. [lien](#).

[63] Paul Charon et Jean-Baptiste Jeangène Vilmer. Les opérations d'influences chinoises - Un moment machiavélien. Editions Des Equateurs, 2024.

[64] Ingrid D'Hooghe, Annemarie Montulet, Marijn de Wolff, et Frank N. Pieke. « Assessing Europe-China Collaboration in Higher Education and Research ». Leiden Asia Centre, 2018. [lien](#).

[65] Amaury Renaudie. « La stratégie d'influence chinoise dans le monde universitaire français ». Enderi, 28 juillet 2023. [lien](#).

## c. Les médias et professionnels de l'information

Les médias et les professionnels du journalisme sont le relais de l'information par excellence. Plusieurs devoirs lient les journalistes, selon les modalités notamment décrites dans la Déclaration de Munich de 1971 [66]. Le journaliste doit ainsi « *Respecter la vérité, quelles qu'en puissent être les conséquences pour lui-même, [...]. Rectifier toute information publiée qui se révèle inexacte* ». Il doit également « *S'interdire [...] de recevoir un quelconque avantage en raison de la publication ou de la suppression d'une information* » et « *n'accepter de directives rédactionnelles que des responsables de la rédaction* ».

Ces précautions érigées à la base même du métier de journaliste sont le reflet du pouvoir potentiel d'une information erronée diffusée via les médias. Il y apparaît également que des personnes tierces pourraient être effectivement tentées d'influencer le discours médiatique.

### La captation de journalistes en échange d'argent

Il arrive pourtant que des médias soient la cible d'ingérences étrangères et se transforment en relais de désinformation. En témoigne l'affaire M'Barki documentée notamment par l'enquête « Story Killers » menée par un consortium de journalistes européens pour Forbidden stories [67].

Début février 2023, Rachid M'Barki, figure historique de BFMTV, diffuse ainsi plusieurs contenus qui n'ont au préalable pas suivi le cursus habituel de validation par la rédaction. Parmi les propos qui questionnent se trouve notamment l'utilisation inhabituelle au sein du paysage médiatique français de l'expression « *Sahara marocain* », mais aussi des informations en lien avec la Russie et sa diaspora d'oligarques à Monaco qui risquerait des difficultés économiques en lien avec des sanctions de l'UE contre la Russie. Des propos attaquant l'ancien procureur général du Qatar, Ali Bin Fetais Al-Marri ont également été diffusés. Ce qui interroge alors, c'est l'incohérence du contenu de ces brèves par rapport à la ligne éditoriale de la chaîne. Il apparaît finalement que R. M'Barki aurait diffusé ces contenus en réponse à une demande du lobbyiste Jean-Pierre Duthion, lui-même a priori mandaté par l'entreprise Team Jorge, selon l'enquête de Forbidden Stories. Si les liens financiers sont encore flous aujourd'hui, il semble bien qu'il y ait eu des versements d'argent [68].

[66] « Charte de déontologie de Munich ». CFDT Journalistes. [lien](#).

[67] Cécile Andrzejewski. « "Team Jorge" : Révélations sur les manipulations d'une officine de désinformation ». Forbidden Stories (blog), 15 février 2023. [lien](#).

[68] Ouest France. « Soupçons d'ingérence à BFMTV. « J'étais manipulé » : Rachid M'Barki aurait reconnu avoir été payé ». 19 janvier 2024, sect. BFMTV. [lien](#).

L'entreprise « Team Jorge » avait notamment été impliquée dans l'affaire de Cambridge Analytica et a pour clients des États, des entreprises et de riches individus, répartis a minima dans une soixantaine de pays. C'est ainsi un total d'une douzaine de sujets problématiques qui ont été diffusés par R. M'Barki, au profit notamment du Qatar et du Maroc, mais également d'intérêts privés russes.

Parmi les raisons qui semblent motiver un journaliste à enfreindre la charte de déontologie de son métier, Laurent Esquenet, député et vice-Président de la Commission de lutte contre les ingérences étrangères en 2023 [69] estime qu'une certaine précarisation du métier de journaliste pourrait expliquer l'appât que représente la diffusion de désinformation en échange de sommes d'argent conséquentes. Pourtant, pour le député européen Serguey Lagodinsky [70], bien que les financements soient une partie du problème, l'éthique des journalistes serait également en partie responsable. Il insiste enfin sur la nécessité de structures organisées de journalistes pour faire face aux tentatives d'ingérences étrangères.

### **Les risques liés à la propriété étrangères de médias européens**

Un autre risque de diffusion de désinformation au sein des médias européens réside dans la possession par des États tiers d'actions dans les capitaux de médias européens. La plupart des États européens établissent ainsi des limites à la possession étrangère d'un média. La Grèce limite par exemple la propriété par des non-résidents à 25% du capital pour une chaîne de télévision et à 49% pour le capital d'une compagnie de radio. En Italie, la loi sur la télévision privée interdit plus largement aux ressortissants extra-communautaires de prendre des actions dans le capital de chaînes de télévision, à moins qu'un accord bilatéral ne les y autorise. Une forte disparité réglementaire entre les États européens transparaît donc. Jusqu'à très récemment, le Royaume-Uni ne fixait ainsi aucune limitation aux participations étrangères. Pourtant en mars 2024, le Daily Telegraph frôle la faillite et une offre de rachat du fonds privé IML, possédé par le cheikh Mansour Ben Zayed, de la famille régnante d'Abou Dabi, et vice-président des Emirats arabes unis, fait scandale. Les inquiétudes se multiplient. Fraser Nelson, rédacteur en chef du *Spectator* estime ainsi que [71] :

**« Si les gouvernements se mettent à posséder un journal, que ce soit le gouvernement britannique, ou un gouvernement européen ou arabe, la liberté de la presse serait mortellement compromise. »**

[69] Propos confiés lors d'un entretien réalisé par notre équipe le 18 octobre 2024

[70] Dans une interview accordée à Euractiv pour le rapport « The state of media freedom in Europe, challenges and protections », 30 novembre 2024 [lien](#)

[71] Eric Albert. « Le Royaume-Uni interdit l'acquisition de journaux par des États étrangers ». Le Monde, 15 mars 2024. [lien](#).

En réaction, le gouvernement britannique a modifié la loi qui empêche désormais toute acquisition d'un journal ou d'un magazine par un « *État étranger* » et par des « *agents de gouvernements étrangers qui opèrent à titre privé* » [72]. Un cas effectif d'ingérence de ce type a par ailleurs été rapporté par une étude pour le projet MapInfluenCE [73] en République tchèque. Ainsi, en 2015, la société chinoise CEFC20 a obtenu des actions dans l'entreprise Empresa Media. Grâce à ces dernières, la société s'est garantie l'accès à une chaîne de télévision (TV Barrandov) et à plusieurs magazines. L'enquête a révélé que cette acquisition a eu un impact profond sur le discours des médias de l'entreprise quant à la Chine qui ont dès lors commencé à n'évoquer ce pays que sous un angle positif et élogieux.

## d. Les influenceurs

Plus récemment, les influenceurs actifs sur divers réseaux sociaux se sont imposés en tant que nouvelle sphère à fort pouvoir de dissémination d'informations. Dotés de communautés d'internautes qui les suivent en général de manière très régulière et qui leur accordent une certaine confiance, les influenceurs ont en effet un fort pouvoir d'orientation de l'opinion de ceux qui les suivent. Enfin, ils permettent de cibler une catégorie de la population souvent plus jeune par rapport aux intermédiaires décrits précédemment (figures politiques, universités, presse traditionnelle).

Cette confiance accordée par une communauté à un internaute est ainsi un vecteur très efficace pour la diffusion de désinformation. Les influenceurs sont en effet régulièrement approchés par des acteurs désireux de propager de la désinformation.

### La désinformation par des influenceurs rémunérés

Dans le contexte de la crise du Covid-19, plusieurs influenceurs européens (notamment le youtubeur français Léo Grasset, détenteur de la chaîne « Dirty Biology » et Sami Ouladitto détenteur du compte Instagram « Et ça se dit médecin » ou encore l'allemand Mirko Drostchmann) ont été démarchés par l'entreprise russe Fазze pour dénigrer le vaccin Pfizer au profit de Spoutnik V [74]. Il était notamment demandé d'affirmer que le vaccin russe avait un taux de mortalité bien inférieur au Vaccin Pfizer. Là encore, l'entreprise a proposé des sommes d'argent conséquentes en échange de la diffusion de son message par les influenceurs. Il faut noter qu'il ne s'agit pas d'une simple demande de publicité ou de promotion, mais bien d'une tentative malhonnête d'influence de l'opinion.

[72] amendement de l' « Enterprise Act 2002 » par le « Digital Markets, Competition and Consumers Act 2024 »

[73] Ivana Karásková, Tamás Matura, Richard Q. Turcsányi, et Matej Šimalčík. « Central Europe for Sale: The Politics of China's Influence ». Association for International Affairs (AMO), 16 avril 2018. [lien](#).

[74] Courrier international. « Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée ». 26 mai 2021. [lien](#).

En témoignent par exemple les instructions envoyées aux influenceurs. Dans les mails reçus, était notamment soulignée l'importance de faire passer le message comme incarnant leur « propre point de vue indépendant ». Le mail demandait également explicitement à ce que l'entreprise Fazze ne soit pas mentionnée et que l'audience ne s'aperçoive pas qu'il s'agissait d'un contenu sponsorisé – payé par un tiers. Le but global de l'opération était donc explicitement que le message « *apparaisse comme un conseil à votre audience* » [75]. Il est donc clair que l'entreprise est consciente qu'il ne s'agissait pas simplement de faire simplement de la publicité pour un produit mais bien d'influencer l'opinion via des informations erronées – la mortalité prétendue moins élevée du vaccin russe. Des techniques similaires sont utilisées par le régime chinois qui propose des rémunérations financières ou d'autres avantages matériels, par exemple des voyages en Chine dans des hôtels de luxe [76].

### **La désinformation via des influenceurs idéologiquement convaincus**

Par ailleurs si certains profils d'influenceurs sont susceptibles de céder à de telles demandes en raison des profits potentiels, d'autres sont d'abord poussés par des motivations idéologiques [77]. Selon le chercheur Paul Charon, c'est notamment l'adhésion aux thèses soutenues par le Parti Communiste chinois ou par la Russie, ou encore une convergence des deux sur la base d'anti-américanisme qui va pousser des influenceurs à adopter un discours désinformationnel, qui frôle parfois le complotisme, en lien en particulier avec la Chine ou la Russie.

## **Enfin, il faut insister sur le fait que les différents intermédiaires décrits sont généralement les maillons d'une chaîne plus complexe.**

Les cas d'interférences ne se cantonnent pas à l'utilisation d'un seul intermédiaire. Au contraire, dans une recherche d'efficacité des campagnes de désinformation, c'est en général plusieurs intermédiaires issus de sphères différentes qui sont approchés simultanément. Par ailleurs, toujours en vue d'une propagation large et rapide, plusieurs moyens numériques de renforcer la propagation de désinformation existent et sont vecteurs d'une distribution massive de cette dernière.

---

[75] Courrier international. « Des influenceurs français approchés pour dénigrer le vaccin Pfizer, la Russie soupçonnée ». 26 mai 2021. [lien](#).

[76] Interview de Paul Charon par Jérémie André. « Chine : désinformation, manipulations et agents d'influence sur les réseaux sociaux ». *Le Point*, 17 février 2024. [lien](#)

[77] *Ibid.*

## 2. LES TECHNIQUES NUMÉRIQUES DE PROPAGATION MASSIVE DE DÉSINFORMATION

Avec l'évolution des outils numériques, les campagnes de désinformation s'appuient sur des techniques sophistiquées pour massifier leur propagation. Automatisation de la diffusion, optimisation du référencement et exploitation de l'espace publicitaire sont autant de moyens utilisés pour manipuler les perceptions et amplifier des récits fallacieux. Le numérique est devenu l'outil majeur de la lutte informationnelle, qui est l'ensemble d'actions visant à garantir une supériorité sur l'adversaire par l'usage de l'information. Cette partie explore ainsi les principales techniques numériques utilisées pour propager la désinformation.

### a. L'automatisation massive de la diffusion de désinformation par les bots

Les bots sont des comptes automatisés actifs sur les réseaux sociaux. Ils exécutent en majorité des tâches répétitives et prédéfinies et sont un large vecteur de propagation de désinformation en ligne. Les premiers bots développés étaient relativement simplistes. Leur tâche était notamment de poster différents liens de spams sur le plus de plateformes possibles, mais les comptes étaient souvent peu crédibles et le message final peu soigné, ce qui les rendait faciles à détecter. À l'inverse, les « *social bots* » sont des programmes plus sophistiqués qui reproduisent les comportements humains afin de gagner la confiance d'autres utilisateurs en ligne. Une fois cette confiance acquise, ces bots peuvent diffuser de la désinformation qu'il sera plus difficile pour un utilisateur de détecter et de se méfier [78].

Le phénomène est de très grande ampleur. Ainsi, en 2017 sur le total des comptes présents sur Twitter, jusqu'à 15% étaient en réalité des bots [79]. Selon Imperva, une filiale de Thalès, c'est 16 % du trafic internet mondial qui est généré par des bots. Autour de moments politiques cruciaux, la part de trafic générée par des bots grimpe encore. Durant le premier impeachment de D. Trump par exemple, c'est plus de 30% des tweets générés en lien avec ce thème qui étaient publiés par des bots [80].

[78] Susan Morgan. « Fake news, disinformation, manipulation and online tactics to undermine democracy ». *Journal of Cyber Policy*, 2 janvier 2018. [lien](#)

[79] Onur Varol, Emilio Ferrara, Clayton A. Davis, Filippo Menczer, et Alessandro Flammini.

« Online Human-Bot Interactions: Detection, Estimation, and Characterization », 27 mars 2017.

[lien](#).

[80] Michael Rossetti et Tauhid Zaman. « Bots, disinformation, and the first impeachment of U.S. President Donald Trump ». *PLOS ONE*, 8 mai 2023. [lien](#).

La manière dont fonctionne la diffusion de désinformation à partir des bots est double. D'une part, par la publication massive de fausses informations, les bots amplifient la part de désinformation présente sur les réseaux sociaux. Celle-ci est donc plus fréquente sur les fils d'actualité des utilisateurs. Par ailleurs, une même information, diffusée de manière coordonnée par plusieurs bots, a plus de chances de devenir une « tendance » que l'algorithme du réseau social va souvent lui-même mettre en avant. Les bots eux-mêmes participent au « succès » d'une publication en la partageant et en lui ajoutant des « likes ». D'autre part, l'abondance de désinformation sur les réseaux sociaux a également un rôle dissimulateur. C'est-à-dire que les informations légitimes vont avoir moins de chances d'être vues par les utilisateurs du fait de la surabondance de fausses informations qui « prennent la place » des premières [81].

Par ailleurs, si les bots sont initialement programmés par des humains, la place de l'intelligence artificielle dans ces réseaux est croissante et permet un développement encore supérieur en termes de quantité de rapidité, et finalement en termes d'efficacité.

Très récemment, c'est dans le cadre des élections présidentielles croates que le phénomène a été pointé du doigt. Un grand réseau de bots a été découvert par le Centre for Information Resilience [82]. De nombreux faux comptes diffusant des messages pro-russes, anti-UE et anti-OTAN, en concordance avec les propos du président Zoran Milanovic dont la réélection n'est pas assurée, ont ainsi été mis en lumière. Ces algorithmes avaient une activité significativement supérieure à la moyenne, avec parfois plus de cent publications par jour. Nombre d'entre eux étaient dotés de photos de profil générées par IA. Dans cet exemple, la volonté d'atteindre une audience le plus large possible est très perceptible. Les bots publiaient effectivement dans au moins six langues différentes (anglais, français, espagnol, italien, serbe et croate) [83].

Finalement, si la place du numérique tend à prendre de l'ampleur, l'activité humaine dans ce cadre n'est pas négligeable pour autant. Plusieurs études ont ainsi montré que l'efficacité des bots est d'autant plus grande lorsqu'elle est étroitement couplée à une activité ou supervision humaine. Certains parlent de « cyborg », pour décrire ce mode d'action mi-humain mi-robot [84].

---

[81] Michael Rossetti et Tauhid Zaman. « Bots, disinformation, and the first impeachment of U.S. President Donald Trump ». PLOS ONE, 8 mai 2023. [lien](#).

[82] Centre for Information Resilience. « Disinformation Campaign Uncovered by Researchers Ahead of Croatian Presidential Run-Off », 8 janvier 2025. [lien](#).

[83] Starcevic, Seb. « Russian Bots Boosted NATO Critic Ahead of Croatian Election, Researchers Say ». POLITICO, 9 janvier 2025. [lien](#).

[84] *Ibid.*

## b. L'optimisation du référencement du contenu

Pour que les campagnes de désinformation atteignent leur plein potentiel, une optimisation minutieuse du référencement des contenus sur les moteurs de recherche, les réseaux sociaux et d'autres plateformes numériques est cruciale. Ce référencement consiste à améliorer la visibilité des messages dans les résultats de recherche ou les fils d'actualité des utilisateurs, souvent par le biais de mots-clés stratégiques ou d'algorithmes de classement spécifiques. Ces actions peuvent être menées par des acteurs étatiques ou privés, qui adaptent continuellement leur stratégie pour contourner les mécanismes de modération ou tirer parti des changements dans les algorithmes des plateformes.

Une première méthode clé, mentionnée par VIGINUM dans son rapport technique de février 2024 sur le réseau numérique de propagande prorusse Portal Kombat [85], est l'optimisation du référencement sur les moteurs de recherche par le biais d'une promotion SEO (Search Engine Optimization [86]). Le SEO correspond à ce que l'on appelle le « *référencement naturel* », c'est-à-dire l'ensemble des manipulations reconnues pouvant aider à ce qu'un site soit plus visible sur un moteur de recherche. Lorsque l'on fait référence à ce terme, il s'agit essentiellement de manipulations qui sont autorisées. Pour figurer sur Google, un site doit par exemple se référer aux *Essentiels de la recherche* [87], qui forment les principes fondamentaux nécessaires à l'apparition des contenus sur le moteur.

Parmi ces essentiels, il y a premièrement des exigences techniques, ainsi que des règles concernant le spam. Ces dernières visent à lutter contre certaines méthodes abusives, qui peuvent également booster le référencement, comme l'emploi massif de textes ou liens cachés [88] (texte blanc sur fond blanc, caché derrière une image, opacité zéro, etc.). L'amélioration du SEO est à l'inverse recommandée, puisque cela renvoie au troisième et dernier principe, qui concerne les bonnes pratiques clés, le but étant de permettre aux moteurs de recherche et aux utilisateurs de trouver plus facilement les sites pertinents.

Pour autant, VIGINUM montre que l'emploi des techniques SEO constitue également un levier important pour l'optimisation du référencement des contenus désinformateurs sur les moteurs de recherche. Effectivement, l'enquête révèle que les différents sites de l'écosystème de désinformation russe « pravda » semblent bénéficier d'une telle optimisation. Concrètement, les manipulations SEO correspondent à l'utilisation de mots-clés stratégiques, ou encore à la création de « liens entrant » ou « backlinks » pour augmenter la crédibilité du site.

[85] Secrétariat général de la défense et de la sécurité nationale. « Portal Kombat : un réseau structuré et coordonné de propagande prorusse », 12 février 2024. [lien](#).

[86] Google Search Central. « Bien débuter en référencement naturel (SEO) : principes de base ». [lien](#).

[87] Google Search Central. « Essentiels de la recherche Google ». [lien](#).

[88] Google Search Central. « Règles concernant le spam dans la Recherche sur le Web Google ». [lien](#).

Les backlinks sont des liens hypertextes émanant de sites web externes et qui renvoient vers des pages précises d'autres sites. Essentiels pour le référencement naturel, ils sont interprétés par les moteurs de recherche comme des votes de confiance, renforçant la visibilité et la crédibilité d'un contenu. Dans le cadre de la désinformation, ils deviennent des outils stratégiques pour amplifier la diffusion de contenus trompeurs. Les acteurs malveillants créent en général des réseaux de sites interconnectés, ou exploitent des plateformes légitimes pour générer ces liens. Cela leur permet alors de manipuler les algorithmes des moteurs de recherche et de donner une apparence de fiabilité à leurs contenus. En multipliant ces liens entrants, ils augmentent les probabilités pour les informations mensongères d'être mieux classées dans les résultats de recherche, atteignant ainsi un public plus large, tout en brouillant la distinction entre vérité et désinformation.

Une autre technique qui mérite toute notre attention est la saturation du référencement. Basée sur un concept assez simple, cette méthode consiste à saturer un espace médiatique, avec des articles ou des posts, dans le but de noyer les contenus indésirables aux yeux de la puissance qui ingère. Ce mode d'action a notamment été documenté par les organismes membres [89] du projet européen CrossOver [90], qui visait à surveiller et analyser les algorithmes des plateformes en ligne pour lutter contre la désinformation. Leur rapport de février 2023 [91] concernant l'influence de la Chine dans le traitement médiatique du Xinjiang sur Google News pour les internautes francophones belges, est à ce titre édifiant. Parmi les parties prenantes de cette investigation se trouve CheckFirst, une start-up finlandaise spécialisée dans le développement de logiciels et de méthodes de lutte contre la désinformation. Lors de l'entretien qu'il nous a accordé, son CEO Guillaume Kuster explique que :

## **A la suite de la publication d'un rapport d'Amnesty International sur les droits humains en Chine et les Ouïghours, la Chine a déployée d'importants moyens pour noyer les contenus francophones traitant du sujet.**

En effet, le rapport montre que pour les utilisateurs belges francophones, c'est 13% des sources Google analysées entre le 1er février 2022 et le 1er février 2023, reliées au mot clés « Xinjiang », qui furent produites par des médias contrôlés par le gouvernement chinois.

---

[89] EU DisinfoLab, the Dutch-language media outlet Apache, the French media education association Savoir Devenir, and the Finnish start-up Check First.

[90] EU DisinfoLab. « Past Project: CrossOver ». [lien](#).

[91] CheckFirst. « Are State-Controlled Chinese sources trying to dominate Xinjiang coverage on Google News? », 22 février 2023. [lien](#).

Sur la période, 209 organismes ont également couvert ce sujet sur Google News. Or sur cet ensemble, les six plus gros médias sous contrôle chinois ont été auteurs à eux seuls de 27% des articles francophones sur le Xinjiang. Le contenu de ces articles était lui consacré à des aspects dénués de lien avec la question des droits humains, comme le tourisme ou l'agriculture. Cet exemple témoigne de la capacité de diffusion massive dont disposent certaines puissances comme la Chine, et donc du risque associé quant au référencement du contenu, avec une possibilité de dilution des contenus européens fiables au milieu des vagues de désinformation étrangères.

### c. L'achat d'espace publicitaire

L'achat d'espace publicitaire est parfois une composante des campagnes de désinformation, permettant d'amplifier leur portée et de cibler des audiences spécifiques de manière précise. Cette méthode exploite les outils marketing mis à disposition par les plateformes numériques pour maximiser l'exposition des contenus manipulateurs.

Ceux qui désinforment identifient des segments de population selon des critères tels que l'âge, la localisation, les centres d'intérêt ou les comportements en ligne. Ces publicités sont intégrées dans le flux des utilisateurs, rendant leur caractère manipulateur difficile à détecter.

Par exemple, pour attiser les tensions autour du sujet israélo-palestinien, des campagnes de désinformation pour le compte de la Russian Internet Agency, la société de désinformation liée à Wagner, a dépensé près de 35 000€ de publicité pour rendre leurs contenus plus visibles, incluant des achats de likes et d'abonnés. Ici, pour dissimuler leur origine, les campagnes publicitaires recourent souvent à des comptes fictifs ou des entreprises-écrans [92].

Le Règlement pour la transparence et le ciblage des publicités politiques, adopté en 2024, s'inscrit dans la stratégie globale et normative de l'Union européenne de lutte contre la désinformation et les ingérences étrangères. Le règlement exige que la publicité à caractère politique soit clairement étiquetée, permettant aux citoyens de voir pourquoi ils ont été ciblés, qui a parrainé la publicité, combien cela a coûté et à quelles élections ou référendums elle se rapporte. Le parrainage de publicités provenant de l'extérieur de l'UE est interdit pendant la période de trois mois précédant les élections. En réaction, Google a choisi d'interdire la publicité politique en Europe sur ses plateformes, estimant le règlement européen trop compliqué à appliquer [94].

[92] Leloup, Damien. « Graffitis d'étoiles de David : des liens établis avec d'autres opérations d'ingérence en Europe ». Le Monde, 15 août 2024. [lien](#).

[93] Parlement européen. « L'essentiel de la plénière 26-29 février 2024 - Session plénière Strasbourg », 22 février 2024. [lien](#).

[94] Le Monde. « Google va cesser de diffuser des publicités politiques dans l'ensemble de l'Union européenne ». 15 novembre 2024. [lien](#).

Il est également à noter que la désinformation est aussi un business lucratif. D'après une étude de NewsGuard et Comscore, la désinformation représente 2,6 milliards de dollars de revenus publicitaires estimés versés aux diffuseurs chaque année par les annonceurs [95].

En conclusion, l'automatisation joue un rôle central dans la propagation à grande échelle de la désinformation. Il est possible de créer, publier et partager des contenus faux ou trompeurs à une vitesse et à une ampleur qui seraient impossibles à atteindre manuellement.

### 3. LES MÉTHODES DE DÉSINFORMATION CROISÉES

Au-delà d'une désinformation que l'on pourrait considérer comme « classique », où les fausses informations relayées vont servir à promouvoir une vision méliorative de la puissance qui ingère, une nouvelle tendance se développe. En effet, si ce type de désinformation est toujours pratiqué, nous remarquons qu'il s'agit de plus en plus pour les puissances étrangères de déstabiliser en profondeur les sociétés visées, plutôt que d'y inséminer leurs idéologies. Vincent Couronne, fondateur du média de fact checking Les Surligneurs, nous parlait ainsi d'un « *phénomène nouveau* » apparu il y a quelques années. Ce dernier se caractérise par une moindre place accordée aux sujets pro-russe ou pro-chinois par exemple, pour privilégier des narratifs visant à exacerber des fractures déjà existantes au sein des sociétés européennes.

Pour cette désinformation qui vise à accentuer les clivages internes, les canaux de diffusion tels que les intermédiaires d'influence ou les réseaux numériques sont bien sûr mobilisés. Toutefois, il existe également d'autres modes opératoires, qui sont particulièrement prisés et efficaces pour relayer ce type de désinformation. Effectivement, un nouveau champ de techniques, consistant à combiner des méthodes de désinformation classiques avec des pratiques issues d'autres domaines d'action, semble en plein essor. Nous explorerons ici les spécificités de ces techniques contemporaines, que nous définirons comme « techniques de désinformation croisées ».

---

[95] NewsGuard, et ComScore. « Advertising on Misinformation », 23 août 2021. [lien](#).

Qu'entendons-nous donc par techniques de désinformation croisées et pourquoi les définir ainsi ? Au cours de nos recherches, il est apparu essentiel d'accorder une place à ce type de techniques dans le rapport. De fait, elles étaient mentionnées de manière récurrente comme élément important de la désinformation contemporaine, que ce soit au travers des rapports institutionnels sur la désinformation, par des médias de fact-checking ou des personnalités politiques. Bien que systématiquement évoquées comme des méthodes bien particulières, ces techniques ne faisaient pas l'objet d'une définition spécifique dans les différentes sources consultées. Et pour cause, il est assez difficile de les classer dans les catégories de désinformation déjà existantes.

En quelque sorte à la croisée des chemins entre divers domaines d'action, ces techniques reposent sur la « *création d'évènements qui n'existent pas* » [96], qui vont venir servir d'appuis au développement d'un narratif ensuite relayé sur les canaux précédemment évoqués. Concrètement, cela signifie que :

**Avant de diffuser sa fausse information, la puissance étrangère va orchestrer la réalisation d'une action tangible pour les sociétés européennes, qui va constituer une sorte de preuve pour les discours qui vont être émis.**

Cela s'appuie dans plusieurs cas sur une action de terrain, comme avec les graffitis d'étoiles de David à Paris en novembre 2023 [97], orchestrés par un réseau de désinformation russe, en vue de pousser un narratif de montée de l'antisémitisme en France. Cette illusion d'événements réels offre aux désinformateurs la capacité à susciter de plus fortes émotions chez le public cible, qui va être témoin sur le terrain d'une réalisation concrète de ce qu'il peut lire en ligne, le poussant à valider la fausse information.

Avec ces techniques croisées, il y a donc toujours une action qui vient s'ajouter à la diffusion de la désinformation. Nous avons remarqué que cette action pouvait prendre diverses formes, en s'appuyant sur différents domaines et registres. Nous avons identifié trois domaines d'action en particulier, dont les méthodes sont parfois empruntées, puis croisées avec une diffusion plus classique. Ainsi, nous nous focaliserons tout d'abord sur l'utilisation de moyens d'action issus du répertoire de l'action collective ; pour ensuite aborder l'amplification et le détournement d'événements directement sur les réseaux en ligne ; et enfin analyser l'emploi de méthodes étant initialement associées au lobbying.

---

[96] Citation de Laurent Esquenet, lors de l'entretien réalisé par notre équipe le 18 octobre 2024

[97] Maxime Tellier. « Derrière les tags d'étoiles de David à Paris, un vaste réseau de désinformation russe ». *Franceinfo*, 26 janvier 2024. [lien](#).

## a. L'utilisation des moyens d'action issus du répertoire de l'action collective

Le concept de répertoire de l'action collective, développé par l'historien et sociologue Charles Tilly en 1984, renvoie au « *stock limité de moyens d'action à la disposition des groupes contestataires, à chaque époque et dans chaque lieu* » [98]. Ces moyens d'action sont utilisés par les acteurs contestataires, afin de faire retentir leurs mouvements sociaux et de se faire entendre. L'utilisation de ces méthodes peut constituer un levier particulièrement puissant dans la légitimation de fausses informations. En effet, étant habituellement mobilisés par les différents acteurs de la société civile pour appuyer leurs revendications, de telles actions orchestrées par une puissance qui opère une ingérence peuvent alors passer pour des opérations de groupes militants.

C'est notamment ce qu'il s'est passé à Paris en octobre 2023, avec les graffitis d'Etoiles de David. Le 30 octobre, dans un contexte de tensions faisant suite à l'attaque du Hamas en Israël le 7 octobre et à la réponse du gouvernement israélien à Gaza, une soixantaine d'Etoiles de David ont été taguées au pochoir dans le 14ème arrondissement de Paris. Cette information est immédiatement reprise et relayée par l'ensemble des médias français, de médias israéliens et internationaux. Dans les lignes du journal The Times of Israël, on peut alors lire le témoignage du Président de l'Union des Etudiants Juifs de France, Samuel Lejoyeux : « Cet acte de marquage rappelle les procédés des années 30 et la Seconde Guerre mondiale qui ont conduit à l'extermination de millions de juifs » [99]. Le Parquet de Paris ouvre une instruction dès le 31 octobre, et les responsables politiques commentent les faits. La Première ministre de l'époque, Elisabeth Borne, réagit avec les mots suivants : « *Au nom du gouvernement, je condamne avec une fermeté absolue ces agissements ignobles [...] s'en prendre à quelqu'un parce qu'il est juif, [...] c'est s'en prendre à l'âme même de la République* » [100].

Il y a donc un très fort retentissement médiatique et institutionnel, avec l'identification initiale de ces graffitis comme des actes antisémites, émanant supposément d'individus ou de groupes contestataires locaux. Cette première analyse n'est pas étonnante, puisque taguer des symboles ou slogans est un moyen d'action régulièrement employé dans les mouvements sociaux contestataires quels qu'ils soient [101]. Le 6 novembre, une semaine après l'événement, VIGINUM annonce qu'il s'agit finalement d'un acte d'ingérence russe. Grâce à son enquête, le service met en lumière le lien entre les graffitis et le dispositif russe RRN (Recent Reliable News).

[98] Cécile Péchu. « Répertoire d'action ». *Dictionnaire des mouvements sociaux*, 2009. [lien](#).

[99] The Times of Israël, « Stars of David Spray-Painted on Buildings in Paris, Heightening Fears among Jews ». 31 octobre 2023. [lien](#).

[100] Le Monde. « Des étoiles de David taguées en Ile-de-France : enquête ouverte, Elisabeth Borne dénonce des « agissements ignobles » ». 31 octobre 2023. [lien](#)

[101] Anny Bloch-Raymond. « Tags, graffs et fresques murales : revendications identitaires, expressions communautaires? (San Francisco Strasbourg) », *Agora débats/jeunesses*. [lien](#).

En effet, les experts retracent la diffusion de 2589 posts polémiques sur les graffitis, par un réseau de 1095 bots associés à l'opération de désinformation RRN [102]. Un des éléments les plus édifiants du lien entre cette action et l'ingérence russe est la primo-diffusion de certains de ces posts, près de 48h avant la première publication authentique des tags. De son côté, le Tribunal judiciaire de Paris annonce dans son communiqué de presse avoir identifié un couple auteur des faits, ayant déjà quitté la France. L'analyse de leurs conversations téléphoniques, ainsi que celle d'un autre couple de moldave ayant agi de manière similaire quelques jours auparavant, permet de penser que ces deux couples auraient agi sous la commande d'une même tierce personne [103]. La suite des investigations établira la responsabilité d'Anatoli Prizenko, un homme d'affaires moldave connu pour son engagement pro-russe, et qui reconnaît son implication [104].

## **Un événement de terrain, assimilable à une action collective authentique, peut donc décupler la force d'impact de la désinformation.**

Ici, cet événement a profondément touché la population française, bien que le démasquage de l'opération d'ingérence n'ait pris qu'une semaine. Si le cas des Etoiles de David à Paris demeure à ce jour le plus emblématique de cette méthode émergente, les acteurs de lutte contre la désinformation ont pu identifier d'autres cas en Europe.

A ce titre, l'ONG EU DisinfoLab parle de « potentielles opérations hybrides » comme tactiques employées dans la campagne de désinformation russe Doppelgänger, à laquelle se rattache l'opération RRN [105]. EU DisinfoLab renvoie alors vers Meta, qui identifie plusieurs cas assimilables aux méthodes de désinformation croisées. Effectivement, son Rapport sur les menaces adverses du deuxième trimestre 2024 [106] met en lumière l'implication d'un réseau russe lié à la diffusion de posts sur les Etoiles de David dans d'autres opérations. Bien que la plupart d'entre elles sont plutôt à ranger dans la catégorie de l'amplification et du détournement d'événements réels, que nous allons voir ensuite, sont également citées certaines techniques relevant du répertoire de l'action collective, comme l'organisation et l'incitation en ligne à des manifestations physiques contre le soutien à l'Ukraine en Allemagne, France ou Pologne. Lors de ces manifestations sont également distribués des flyers, permettant d'accéder aux boucles Telegram de ces opérations. Le répertoire de l'action collective constitue ainsi une nouvelle ressource pour les désinformateurs, avec un large panel de moyens d'action dans lequel ils peuvent se servir.

[102] Représentation Permanente de la France auprès de l'OSCE. « Russie - Nouvelle ingérence numérique russe contre la France », 9 novembre 2023. [lien](#).

[103] Parquet du Tribunal Judiciaire de Paris. « Communiqué de presse de la procureure de la République », 7 novembre 2023. [lien](#).

[104] Jacques Pezet et Elsa de La Roche Saint-André. « Anatoli Prizenko, commanditaire présumé des étoiles de David taguées dans Paris, prétend que l'action visait à «soutenir» les Juifs ». *Libération*, 8 novembre 2023. [lien](#).

[105] EU DisinfoLab. « What Is the Doppelgänger Operation? List of Resources », 30 octobre 2024. [lien](#).

[106] Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, et Mike Dvilyanski. *Adversarial Threat Report*, 2024. [lien](#).

## b. L'amplification et le détournement en ligne d'événements réels

Il s'agissait ici de la forme la plus représentative et la plus palpable de la désinformation croisée, avec la création d'actions de terrain qui vont susciter des émotions et des réactions intenses au sein des sociétés européennes.

Toutefois, l'appui de la désinformation sur un acte tangible n'implique pas forcément que ce dernier ait été orchestré par la puissance qui s'ingère, ni même nécessairement qu'il soit de terrain. Pour revenir à la citation de Laurent Esquenet, il parle d'un nouveau type de désinformation qui s'appuie sur « la création d'événements qui n'existent pas ». Or, s'il cite les Etoiles de David en exemple, il évoque également l'affaire des punaises de lit à Paris en septembre 2023. On pourrait alors se dire qu'il ne s'agit pas de création ici, puisqu'il y avait effectivement des problèmes de punaises de lit à Paris. Toutefois, on a pu remarquer par la suite que la panique médiatique avait été largement disproportionnée vis-à-vis de la situation réelle. En cause, une polémique « artificiellement amplifiée » par la Russie sur les réseaux sociaux, comme l'expliquait le ministre français délégué à l'Europe du moment, Jean-Noël Barrot [107].

L'amplification et le détournement d'événements existants peut constituer un problème distinct, puisqu'un phénomène authentique va servir de base à la construction d'un édifice mensonger tout autour. Nous pouvons alors considérer qu'il s'agit là aussi, de manière différente, de créer quelque chose qui n'existe pas, en donnant à l'événement initial une ampleur complètement déconnectée de sa réalité. Il s'agit d'une autre manière de croiser la désinformation avec le réel, qui ne nécessite cette fois-ci pas forcément d'engager de moyens d'action sur le terrain, le phénomène étant déjà existant. L'enjeu pour les désinformateurs est alors de l'exploiter à profit.

L'amplification en ligne d'événements réels ou tangibles pour les populations européennes est précisément la forme de désinformation croisée à laquelle on peut assimiler les cas soulignés par Meta dans le Rapport Q2 2024 [108]. Ces rapports trimestriels sur les méthodes adverses ont un but bien précis, identifier des « Coordinated Inauthentic Behavior (CIB) » et les réseaux qui y sont liés. En tant que géant du web et gestionnaire de plateformes en ligne, la multinationale se concentre sur l'aspect numérique de la désinformation. Nous pouvons justement reprendre un exemple qui se passe entièrement en ligne, mais qui simule l'expression d'une partie de la population moldave.

[107] Le Figaro. « France: la psychose des punaises de lit a été « amplifiée » par Moscou, affirme le ministre délégué à l'Europe ». 1 mars 2024. [lien](#)

[108] Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, et Mike Dvilyanski. Adversarial Threat Report, 2024. [lien](#).

Meta nous apprend ainsi que le troisième réseau CIB russe identifié dans le rapport Q2 2024 a promu une pétition pour l'abolition du vote par correspondance en Moldavie, dont on ne sait pas vraiment si elle est indépendante ou non. Cette pétition d'apparence authentique et présente sur la plateforme en ligne openPetition est relayée par les comptes de ce réseau, qui diffusent également des posts pro-russes ou des critiques du gouvernement moldave. Bien qu'entièrement numérique, la pétition constitue tout de même un élément concret, qui vient renforcer le narratif pro-russe déjà poussé par les leviers plus classiques de désinformation, tels les posts cités à l'instant. A travers cet exemple assez spécifique, nous nous rendons compte que le phénomène associé n'a pas forcément besoin d'être physique, mais doit toutefois renvoyer à une action tangible et créatrice d'effets dans la société, comme c'est le cas avec la pétition.

Dans ce rapport, Meta fait à plusieurs reprises le lien entre ce qui est publié sur Facebook ou Instagram et des événements réels. On se retrouve alors dans une configuration plus similaire à celle concernant l'affaire des punaises de lit. Le troisième réseau CIB suscite de nouveau notre intérêt, puisque c'est aussi celui-ci qui se trouve derrière les manifestations contre le soutien à l'Ukraine déjà évoquées. En effet, le réseau est à l'origine d'actions de terrain, puisque certaines pages ou groupes en ligne associés, qui se présentent de façon mensongère comme des soutiens aux ukrainiens, revendiquent l'organisation de certaines manifestations qui visent en réalité à développer une opinion contre l'aide à l'Ukraine. Ce fut notamment le cas du groupe Telegram « Ukrainian European Front », qui avait créé une page Facebook directement repérée et supprimée par les services de Meta. L'implication russe dans les manifestations en physique a également été mise en avant par les services d'investigation du journal *Le Monde* [109].

Mais au-delà des manifestations dans l'espace public, qui relève plutôt du répertoire de l'action collective, il est intéressant de remarquer que l'amplification des événements réels en ligne est un élément central dans le mode d'action de ce réseau. Le rapport de Meta met l'accent sur ce point, puisque les actes de terrain (manifestations, stickers, graffitis, etc.) sont ensuite repris sur les différents réseaux sociaux avec des photos ou vidéos, ainsi que sur des « pages d'informations », qui tâchent de faire croire à des manifestations authentiques. A noter que la vision amplificatrice constitue une sorte de matrice, dont s'imprègne l'action réelle. Dans l'exemple soulevé par *Le Monde*, à Paris, les auteurs, qui ne sont que trois, se fondent dans une manifestation concernant la réforme des retraites, détournant alors une manifestation réelle afin de créer une illusion de masse et d'augmenter l'impact des images relayées.

---

[109] Thomas Eydoux et Margaux Farran. « How Russia Is Staging Fake Protests in Europe to Discredit Ukraine ». *Le Monde*, 7 mai 2023. [lien](#)

Ainsi, si l'on peut établir une distinction entre désinformation croisée se référant au répertoire de l'action collective et désinformation croisée via l'amplification d'évènements réels qui ne sont pas nécessairement créés par la puissance qui s'ingère, ce dernier exemple nous montre que ces deux formes de désinformation peuvent être combinées dans le but de maximiser l'impact.

### **c. La désinformation croisée en déploiement vers d'autres champs d'activités, tels que le lobbying**

Suite à cette analyse de la désinformation croisée et des manières dont elle se manifeste la plupart du temps, il apparaît clairement qu'elle repose systématiquement sur la création de quelque chose qui n'existe pas. Si les formes et techniques peuvent différer, un point commun à tous les cas étudiés est la mise en œuvre d'une illusion de réel à travers des évènements tangibles, qu'ils soient orchestrés, amplifiés ou détournés par les désinformateurs. Ce fil directeur semble particulièrement bien fonctionner avec les phénomènes de terrain, qui touchent plus directement les sociétés. Toutefois, bien que les exemples renvoient souvent à des actes issus du répertoire de l'action collective, à l'amplification en ligne de phénomènes réels, ou aux deux en même temps, ce type de désinformation s'étend également à d'autres domaines d'activités.

Nous remarquons ainsi que de récentes techniques de désinformation vont venir piocher dans le répertoire d'action du lobbying. Dans son rapport INGE 2 [110], la Commission spéciale du Parlement européen sur l'ingérence étrangère et la désinformation cite certains risques d'ingérence liés au manque de réglementation des activités de lobbying. En revanche, il n'est pas question dans le rapport de l'appropriation de certaines techniques de lobbying par les désinformateurs de pays tiers. Or, ces croisements se développent. C'est ce que mettent en avant les journalistes d'investigation de Forbidden Stories dans l'enquête « Story Killers » sur la désinformation. A travers l'étude des techniques contemporaines employées par l'officine de désinformation israélienne Team Jorge, ils soulignent la proposition par l'agence de créer des ONG afin de servir de relais aux idées à diffuser. Dans un podcast France Inter [112], Frédéric Métézeau, journaliste Radio France infiltré pendant l'enquête, revient sur cette proposition, nous décrivant une situation que l'on peut sans aucun doute identifier comme de l'astroturfing.

[110] Parlement européen. « Rapport sur l'ingérence étrangère dans l'ensemble des processus démocratiques de l'Union européenne, y compris la désinformation », 15 mai 2023. [lien](#).

[111] France Inter, « Story Killers, la dernière enquête de Forbidden Stories ». 16 février 2023. [lien](#).

Cette technique de désinformation et d'influence doit son nom au sénateur Lloyd Bentsen, qui la définit en 1985 par « l'astroturf » (gazon synthétique), en opposition au terme « grass-roots » qui renvoie à des mouvements de base citoyenne. Elle vise à créer de toute pièce quelque chose de réel (une association, un mouvement, etc.), qui va servir à relayer des idées dans le but d'influencer un public [112]. Cela rejoint en tout point le fil directeur des cas de désinformation croisée étudiés jusqu'ici. Cette méthode n'est pas nouvelle, puisqu'elle est définie dès 1985. Pour autant, c'est une technique habituellement associée à l'activité des lobbies industriels. Il est donc intéressant de voir que certaines agences de désinformation aux ressources conséquentes, telles que la Team Jorge, se mettent à reprendre des méthodes de lobbying dans leur catalogue de techniques.

En somme, il apparaît que l'ensemble des méthodes croisées forme dans sa globalité un type de désinformation émergent et récent, qui tend à se développer davantage.

### **Si les cas les plus emblématiques de désinformation croisée sont caractérisés par une action de terrain assortie d'une amplification en ligne, il ne faut pas mettre de côté le déploiement vers d'autres secteurs actuellement à l'œuvre.**

La reprise de l'astroturfing dans des campagnes de désinformation en est un bon exemple, qui invite les acteurs de lutte à rester vigilant quant à la possibilité d'investissement de nouveaux domaines d'activités par les désinformateurs. La désinformation croisée constitue aujourd'hui un élément fondamental des stratégies d'ingérence hybrides des Etats tiers, qui peut même venir se confondre dans des cas extrêmes avec l'action directe d'un gouvernement. C'est ainsi ce que relève la commission spéciale INGE 2 dans son rapport au sujet des migrants déplacés à la frontière polonaise par les autorités biélorusses. Au-delà de l'ingérence physique, le rapport met en avant l'aspect de désinformation, avec un flux migratoire alimenté par la Biélorussie visant entre autres à exploiter le sujet majeur de division qu'est la migration au sein de l'Union européenne [113].

Il convient donc d'accorder une attention toute particulière à ce type de désinformation en plein développement, qui se manifeste sous diverses formes et qui présente un risque considérable de déstabilisation et de renforcement des clivages au sein des sociétés européennes.

---

[112] France Inter « L'astroturfing, la grande illusion de l'opinion », 25 janvier 2024. [lien](#).

[113] *ibid.*

# CONFRONTATIONS EUROPE



## ***Confrontations - Bruxelles***

Avenue des Arts 46

1000 Bruxelles

## ***Confrontations - Paris***

Avenue de Versailles 77

75016 Paris



@confrontations



@ConfrontationsEurope



[www.confrontations.org](http://www.confrontations.org)



[communication@confrontations.org](mailto:communication@confrontations.org)

**Confronter les idées, construire l'Europe**