diploweb.com La revue géopolitique
ISSN : 2111-4307

La guerre de l'information contre la France : anatomie d'une menace plurielle

jeudi 17 septembre 2026,par Alizéa-Maïwenn CIFTCISOY

Citer cet article / To cite this version :
Alizéa-Maïwenn CIFTCISOY, **La guerre de l'information contre la France : anatomie d'une menace plurielle**, *Diploweb.com : la revue géopolitique, 17 septembre 2026.*

Hum... Vous semblez apprécier le DIPLOWEB.COM. Nous vous en remercions et vous invitons à participer à sa construction.

Le DIPLOWEB.COM est LE media géopolitique indépendant en accès gratuit, fondé en l'an 2000. Nous vous proposons de participer concrètement à cette réalisation francophone de qualité, lu dans 190 pays. Comment faire ? Nous vous invitons à verser une participation à votre convenance par PayPal via **la page suivante** . Vous pouvez aussi rédiger un chèque à l'ordre du DIPLOWEB.COM et l'adresser à Diploweb.com, Pierre Verluise, 1 avenue Lamartine, 94300, Vincennes, France. Ou bien encore faire un virement bancaire en demandant un RIB à l'adresse expertise.geopolitique@gmail.com.

Avec 5 000€ par mois, nous pouvons couvrir nos principaux frais de fonctionnement et dégager le temps nécessaire à nos principaux responsables pour qu'ils continuent à travailler sur le DIPLOWEB.COM.
Avec 8 000€ par mois, nous pouvons lancer de nouveaux projets (contenus, événements), voire l'optimisation de la maquette du site web du DIPLOWEB.COM.

A-M Ciftcisoy retrace d'abord la généalogie des pratiques d'ingérence informationnelle et en mesure la mutation à l'ère numérique. Puis l'auteure analyse les trois grammaires contemporaines les plus significatives pour la France (Russie, Chine et Etats-Unis), avant d'en évaluer les risques systémiques pour la cohésion sociale, l'intégrité électorale et la souveraineté numérique du pays.

L'IDEE selon laquelle les mots sont une arme et que la guerre peut se mener par leur intermédiaire est loin d'être nouvelle. L'échelle de la confrontation informationnelle qui se déploie à l'ère du numérique et de la mondialisation l'est cependant. Longtemps circonscrite aux services de renseignement et à leurs opérations clandestines, la manipulation de l'information s'est progressivement diffusée vers des acteurs privés, des plateformes numériques et des réseaux transnationaux dont les intérêts, sans être toujours alignés sur ceux d'un État, produisent des effets stratégiquement comparables. Ces logiques d'ingérence informationnelle ne sauraient être appréhendées isolément : elles s'inscrivent dans un continuum plus large de guerre hybride, où la manipulation du champ informationnel, constitue un vecteur parmi d'autres pour affaiblir un adversaire sans jamais franchir le seuil de l'agression caractérisée. La France se trouve aujourd'hui exposée à une multitude de pressions informationnelles, dont les logiques, les finalités et les vecteurs diffèrent sensiblement selon leur origine. Cet article se propose, sans être pour autant exhaustif, de retracer la généalogie de ces pratiques d'ingérence informationnelle, d'en mesurer la mutation à l'ère numérique, puis d'en analyser les trois grammaires contemporaines les plus significatives pour la France, avant d'en évaluer les risques systémiques pour la cohésion sociale, l'intégrité électorale et la souveraineté numérique du pays.

Une illustration de la guerre de l'information

I. Généalogie et perdurance de la menace informationnelle

Loin de se cantonner aux fronts de bataille, la guerre informationnelle, malgré son appellation belliqueuse, vise, en tout temps, à **fragiliser et fragmenter les sociétés ennemies**, ou simplement adverses sur certains plans politiques. Afin d'en illustrer la perdurance temporelle et historique, la période de la Guerre froide (1947-1991) constitue un exemple particulièrement parlant. En effet, si la doctrine militaire russe intègre dès le XIXème siècle l'information comme une arme de déstabilisation de l'ennemi, elle connaît une certaine apogée à compter des années 1950. Le renseignement soviétique théorise et systématise ce qu'il appelle les « mesures actives » : un ensemble d'opérations clandestines combinant désinformation, faux documents, organisations-écrans et agents d'influence, destinées non pas à convaincre directement l'opinion occidentale, mais à **exploiter des contradictions déjà présentes dans les sociétés visées.** Tel est le cas de l'opération INFEKTION (ou « Denver » dans sa désignation est-allemande), conduite conjointement par le KGB et la Stasi est-allemande dans les années 1980. Le 17 juillet 1983, le quotidien indien *Patriot*, journal créé en 1962 avec le soutien du KGB et utilisé à des fins de désinformation, publie une lettre anonyme affirmant que le virus du sida serait issu de recherches américaines sur les

armes biologiques menées à Fort Detrick. D'abord resté relativement confidentiel, ce récit est réactivé en 1985 par le journal soviétique *Literaturnaya Gazeta*, donnant ainsi **l'illusion de deux sources indépendantes se corroborant mutuellement**. L'opération atteint son apogée en septembre 1986. À l'occasion du sommet du Mouvement des non-alignés à Harare, la Stasi diffuse une brochure reprenant les thèses du biologiste est-allemand Jakob Segal, qui prétend démontrer, sous couvert d'une caution pseudo-scientifique, que le virus aurait été créé par manipulation génétique. Le récit se propage alors largement en Afrique avant de gagner la presse occidentale : le 29 octobre 1986, le *Sunday Express* britannique en publie à son tour une version, bientôt suivie par une quarantaine d'articles à travers le monde au début de l'année1987. Si l'opération est officiellement abandonnée en août 1987 sous la pression diplomatique américaine, ses effets se révèlent durables : en 1992, 15 % des Américains considèrent encore plausible l'hypothèse d'une origine délibérée du virus. Cette persistance illustre la remarquable capacité de tels récits, une fois installés dans l'espace public, à **survivre à leur démenti et à s'ancrer durablement dans l'imaginaire collectif**.

Si l'opération INFEKTION relevait d'une désinformation savamment orchestrée en coulisses par un service de renseignement, une autre catégorie d'opérations psychologiques s'est déployée, tout au long du XXe siècle, à visage découvert : celle des émissions de propagande radiophonique directement adressées aux troupes ennemies, dont « Hanoi Hannah » demeure l'incarnation la plus connue pour la génération de la guerre du Vietnam, mais qui s'inscrit dans une filiation remontant à la Seconde Guerre mondiale.

« Hanoi Hannah », de son nom véritable Trịnh Thị Ngọ, ne doit pas sa notoriété à sa seule fonction de propagandiste, mais bien davantage à l'efficacité paradoxale de la méthode qu'elle mit en œuvre. Recrutée en 1955 par la *Voix du Vietnam* en raison de sa maîtrise de la langue anglaise, elle devient, à compter de 1965, l'une des voix les plus reconnaissables de la propagande nord-vietnamienne à destination des troupes américaines. Trois fois par jour, ses émissions conjuguaient appels à la désertion, comptes rendus de pertes militaires et informations soigneusement sélectionnées. Leur efficacité, cependant, ne procédait pas tant du mensonge que de **l'insertion habile de faits avérés au sein d'un récit à visée propagandiste**. En relayant des événements que le commandement militaire américain s'efforçait de minorer, voire de taire, telles que le massacre de My Lai (1968), Hanoi Hannah parvenait à brouiller la frontière entre désinformation et information. La figure d'Hanoi Hannah ne surgit pas *ex nihilo* : elle prolonge une tradition inaugurée durant la Seconde Guerre mondiale par plusieurs voix chargées, par ondes courtes, d'éroder le moral de l'adversaire. Dans le Pacifique, le programme japonais « Zero Hour » popularise la figure composite de « Tokyo Rose », incarnée notamment par Iva Toguri d'Aquino. Sur le théâtre européen, Mildred Gillars (« Axis Sally ») et William Joyce (« Lord Haw-Haw ») animent des émissions comparables pour l'Allemagne nazie. Le conflit coréen reproduit ce schéma avec « Seoul City Sue », dont les émissions se signalent par la lecture macabre des plaques d'identification de soldats américains tombés au combat. Tel est, précisément, le paradoxe constitutif de la propagande radiophonique : pour emporter l'adhésion, il n'est nul besoin qu'elle soit vraie dans son intégralité, il suffit qu'elle le soit assez pour ébranler la confiance accordée à la source adverse. La voix de l'« ennemi » peut ainsi acquérir une crédibilité d'autant plus grande que la parole officielle américaine perd, quant à elle, la sienne. Hanoi Hannah illustre en cela un principe fondamental de la guerre psychologique : il ne s'agit pas seulement de persuader l'adversaire d'une contre-vérité, mais de **rendre suspecte, à ses yeux, la vérité qui lui parvient de son propre camp**.

> Fracturer le tissu social afin d'y faire prospérer des narratifs favorables à l'émetteur.

Ce que ces cas, en dépit de leurs contextes distincts, mettent en lumière de façon convergente, c'est

la porosité constante entre propagande d'État et velléités d'influences étrangères. Ils illustrent également les limites structurelles de ce type d'entreprise : les études postérieures s'accordent à souligner que l'effet démoralisateur recherché demeurait largement inférieur aux ambitions de leurs commanditaires, les auditoires militaires ayant davantage consommé ces émissions comme un divertissement teinté d'ironie que comme une source d'endoctrinement effectif, signe que l'arme radiophonique, si elle a occupé une place centrale dans l'arsenal de la guerre psychologique du XXe siècle, n'a jamais suffi, à elle seule, à emporter l'adhésion ou le déchirement interne qu'elle visait. Cette limite partage peut-être des convergences avec les opérations contemporaines.

Il ne s'agit plus tant, désormais, d'emporter l'adhésion et la conviction profonde des populations visées, que de mettre au jour leurs fragilités et les lignes de polarisation qui traversent le débat public, de saturer l'espace informationnel et, par ce biais, de fracturer le tissu social afin d'y faire prospérer des narratifs favorables à l'émetteur.

II. La rupture du numérique et l'émergence de vulnérabilités nouvelles

La démocratisation et l'expansion du numérique ont engendré une massification de la propagande et de la manipulation computationnelle, par un changement d'échelle et de vitesse. Le coût marginal de la production et diffusion des contenus, couplé à la viralité et la vastitude des publics touchés par les contenus en font un outil de choix dans la diffusion de certains narratifs. Cet effet est accentué par **l'effacement progressif des gardes-fous traditionnels**, tels que les rédactions ou modérateurs, au profit d'une architecture algorithmique qui traite l'information comme un flux indifférencié à optimiser pour l'engagement et non pour la véracité des propos tenus. Par exemple, suite à l'acquisition en octobre 2022 de Twitter, rebaptisé X, par Elon Musk, une refonte des algorithmes a été entreprise. Cela s'est particulièrement manifesté lors de l'élection présidentielle américaine de 2024, [1] où l'on a pu recenser une mise en avant des personnalités et comptes utilisateurs relayant des positions conservatrices y compris lorsque l'utilisateur a un compte sans affinité politique apparente. [2] En réduisant drastiquement les effectifs chargés de la modération, les contenus à caractère haineux ou scandaleux, sans preuves de véracité, pullulent et ne sont plus régulés par la plateforme. Près de 86 % d'entre eux demeurent en ligne après leur signalement. [3] Une étude de 2018 a par ailleurs démontré que **les fausses informations tendaient à se diffuser plus rapidement et plus largement sur les réseaux sociaux que les vraies**. [4] Concomitamment, **le développement de l'IA générative constitue un nouveau facteur de risque identifié** par VIGINUM dans son rapport de février 2025, [5] notamment du fait du gain de réactivité et de volume qu'elle permet pour les acteurs malveillants, sans emporter un gain qualitatif en matière de sophistication. Si le risque est réel, la jeunesse de ces dispositifs rend leur impact réel encore mesuré et difficile à quantifier. Cependant, des exemples permettent déjà d'en illustrer les effets concrets. À l'approche des élections municipales françaises de 2026, le réseau de désinformation pro-russe Storm-1516 a mené des opérations d'ingérence numérique en utilisant l'intelligence artificielle générative, notamment à travers la création de plus de 140 faux sites d'actualité, notamment typosquattés, imitant la presse régionale pour diffuser des contenus trompeurs en exploitant la confiance des citoyens envers les médias de proximité, et en menant des attaques ciblant des candidats, par la diffusion de fausses informations et rumeurs à leur égard, comme ce fût le cas pour Pierre-Yves Bournazel à Paris. Parallèlement, une campagne de désinformation est lancée dès le mois de mars 2026 par Blackcore, une société privée basée en Israël, spécialisée dans la vente de prestations et d'opérations de déstabilisations. Blackcore met en place un réseau de plusieurs noms de domaines et de *Sock Puppets*, de fausses identités numériques individuelles se faisant passer pour des utilisateurs authentiques, notamment alimentés par l'IA générative, visant en particulier le parti LFI, ainsi que plusieurs de ses candidats, révélée par les services de

VIGINUM.

> Les plateformes deviennent des actrices géopolitiques de plein droit, brouillant la distinction entre ingérence étatique et pouvoir structurel privé.

Antoine Marie, du Cevipof, a mis en lumière l'utilisation inédite et massive de l'IA générative dans les stratégies de manipulation et de communication lors de ces élections locales, qui pourrait laisser à présager un scénario similaire et délétère pour d'autres scrutins. [6] Outre la modification de la perception d'un candidat ou parti auprès de l'opinion publique et la polarisation du débat public, ces stratégies de manipulations et d'ingérences visent également à délégitimer les médias nationaux en alimentant la défiance à leur égard, ainsi qu'à décrédibiliser le processus électoral et les institutions garantes de son fonctionnement. Les plateformes numériques, très majoritairement américaines, bénéficient d'un cadre juridique plus favorable par leur nationalité, et ce malgré l'implantation d'outils légaux comme le *Digital Services Act* (DSA, 2024) dont l'application, par manque de coopération des plateformes, diffère effectivement de la lettre. Ces plateformes deviennent des actrices géopolitiques de plein droit, brouillant la distinction entre ingérence étatique et pouvoir structurel privé.

Cette autonomisation des plateformes numériques comme acteurs géopolitiques ne doit cependant pas occulter le rôle central que continuent de jouer les États dans l'orchestration des ingérences informationnelles.

III. Moscou, Pékin, Washington : trois visages de l'ingérence

Trois acteurs se distinguent aujourd'hui par l'ampleur et la spécificité de leurs stratégies à l'égard de la France : la Russie, la Chine et les États-Unis, dont les logiques d'ingérence, bien que convergentes dans leurs effets déstabilisateurs, obéissent à des rationalités et des méthodes profondément différentes.

A. La Russie, ou la maturité d'un dispositif d'ingérence

La stratégie informationnelle déployée par la Russie à l'égard de la France s'inscrit moins dans une logique de persuasion que dans une logique d'attrition, dont la finalité n'est pas tant de convertir l'opinion française à un récit pro-russe structuré que d'**exploiter et d'approfondir les lignes de fracture déjà présentes au sein du débat public**. À la différence d'acteurs plus récents ou plus rudimentaires, la Russie se distingue par le statut d'acteur mature qu'elle occupe dans l'écosystème des ingérences informationnelles visant la France. Héritière directe des « mesures actives » soviétiques, elle dispose d'un savoir-faire éprouvé sur plusieurs décennies, qui se traduit par la diversité et l'évolution constante de ses modes opératoires informationnels (MOI). Cette plasticité, qui va de la saturation numérique à l'action physique hors ligne, en passant par le piratage ciblé, constitue en elle-même une signature distinctive de la maturité du dispositif russe. Le mode opératoire Storm-1516, directement rattaché au renseignement militaire russe (GRU) et documenté par VIGINUM à travers l'analyse de soixante-dix-sept opérations conduites entre la fin de l'année 2023 et mars 2025, en constitue l'expression la plus aboutie. Son architecture repose sur la combinaison de plusieurs MOI : la diffusion de *deepfakes*, l'usurpation systématique de la presse locale par l'enregistrement de plus d'une centaine de noms de domaine imitant des titres régionaux français (*media cloning* et *typosquatting*), et un ciblage résolument calé sur le calendrier électoral national, des élections européennes de juin 2024 aux municipales de mars 2026, en passant par les

législatives de juillet 2024. Cette entreprise ne se limite d'ailleurs pas au scrutin lui-même mais cible également des personnalités politiques ou institutions nationales, comme précédemment évoqué. Déjà durant la campagne présidentielle de 2017, les e-mails de l'équipe d'Emmanuel Macron avaient été piratés, avec l'objectif d'influencer l'opinion publique. Des milliers de documents internes de l'entourage du futur président avaient été diffusés, avec l'ajout de documents frauduleux parmi des documents authentifiés, destinés à semer le doute à la veille d'un scrutin crucial. Aujourd'hui, alors que l'élection présidentielle de 2027 se profile, des tentatives d'ingérences ont déjà été recensées à l'encontre de plusieurs candidats, tels que Édouard Philippe et Raphaël Glucksmann. Même si ces opérations sont, à ce stade, peu visibles, elles n'en demeurent pas moins nombreuses, comme s'en inquiétait le premier ministre, Sébastien Lecornu, qualifiant le risque « d'une menace lourde » sur l'élection présidentielle. [7] Ce dispositif se prolonge enfin hors ligne, par des actions s'appuyant sur l'actualité et les tensions traversant le débat public, dans le seul but d'accentuer la polarisation et de fragiliser la cohésion sociale. Ces dernières années, nombre d'affaires illustrent particulièrement ces modes d'action. En 2023, à l'aube de la Coupe du monde de rugby, des faux articles circulent attestant d'une infestation de punaises de lit dans les transports parisiens. Ces articles apparaissent dans un contexte de sanctions occidentales imposées à l'encontre de Moscou, et impliquent, notamment dans des faux articles usurpant l'identité de *La Montagne* ou de *Libération*, le lien entre cette « épidémie » parisienne et l'afflux de réfugiés ukrainiens. VIGINUM avait dénoncé dès juin 2023 cette opération d'ingérence numérique baptisée « Doppelgänger », consistant à publier de faux contenus hostiles à l'Ukraine sur des sites imitant les grands quotidiens français. Fin octobre 2023, plusieurs centaines d'étoiles de David bleues réalisées au pochoir ont été découvertes sur des façades d'immeubles à Paris et en banlieue parisienne, peu de temps après l'attaque du 7 octobre. Les tags sont l'œuvre d'un couple moldave, commandités par Anatoli Prizenko, un homme d'affaires proche de Moscou. Ce dernier a reconnu avoir ordonné l'opération, invoquant un « acte de soutien envers les juifs ». Le 9 novembre 2023, la France a dénoncé l'implication du réseau russe RRN/Doppelgänger dans la diffusion artificielle et la mise en ligne initiale des photos de ces tags. VIGINUM avait en effet repéré un botnet de 1 095 comptes sur X ayant diffusé plus de 2 500 messages en quelques jours, une part significative recourant à la technique du *Copy-Pasta*, consistant à dupliquer un même contenu sur un grand nombre de comptes pour en simuler l'ampleur organique et à l'*AstroTurfing*. Cette méthode donne l'illusion d'une adhésion spontanée et désintéressée à un narratif en réalité orchestré. Cette opération hybride sera suivie par plusieurs autres qui reprendront le même MOI. Ces opérations se multiplient dans les mois suivants : mains rouges taguées sur le Mur des Justes du Mémorial de la Shoah en mai 2024, peinture verte sur des synagogues parisiennes en mai 2025, têtes de cochon devant des mosquées d'Île-de-France en septembre 2025. Une fuite de documents internes attribués à la *Social Design Agency*, structure proche du Kremlin et spécialisée dans les opérations d'ingérences informationnelles, confirment l'implication de Moscou. Des rapports détaillent la préparation de ces évènements, la liste des lieux ciblés, le timing, les itinéraires, ainsi que des photographies des repérages et actes préparatoires. Cette fuite dévoile également la préparation d'actions avortées, telles que la dégradation d'une statue du général de Gaulle à Paris, par un slogan pro-ukrainien ; le lâcher des poupées gonflables portant des slogans anti-migrants dans la Seine, ou le collage des stickers commémorant le génocide arménien devant les ambassades turque et azérie dans la capitale. Fruits de l'intensification de la guerre hybride menée par la Russie, misant sur l'affaiblissement du soutien européen à l'Ukraine par la division et la fracturation sociétale, ces opérations répondent à une logique commune. Par des actions chocs, **polariser brutalement le débat public et accentuer les disparités existantes**, tout en accentuant leur diffusion et les narratifs qui les entourent par l'intermédiaire des réseaux sociaux et d'usurpations de médias occidentaux. Ce qui frappe dans cette grammaire russe, c'est moins la sophistication de chaque contenu pris isolément, nombre des sites générés par IA, par exemple, restent d'ailleurs peu consultés, que la structuration et la persistance du dispositif dans son ensemble : la surinformation et la saturation y fonctionnent comme des armes à part entière, couplées au mensonge et à l'exploitation des sensibilités publiques.

B. La Chine ou l'influence par le récit

Loin de reprendre le schéma russe d'ingérence déstabilisatrice et agressive, la Chine exerce davantage une stratégie de construction narrative et politique. Là où la Russie cherche à discréditer et à polariser, **la Chine cherche avant tout à sécuriser, dans la durée, une image favorable au Parti communiste chinois et à neutraliser les récits qui lui sont défavorables sur des dossiers sensibles pour sa réputation internationale**. Outre-Atlantique, la Chine a été accusée à plusieurs reprises de tentatives d'ingérences dans les scrutins nationaux, se manifestant notamment, mais pas seulement, par des activités d'espionnage ou des tentatives d'influences des responsables politiques et des fonctionnaires, visant à impacter les résultats des votes pour placer au pouvoir des leaders plus favorables à Pékin. Systématiquement, le régime chinois dément formellement ces ingérences. Cependant, nombre de ces cas sont documentés. L'un des principaux vecteurs de cette stratégie est l'opération Spamouflage (aussi connue sous le nom de Dragonbridge), constituée par un réseau de *Sock Puppets*, diffusant, sur de multiples plateformes, des narratifs favorables aux intérêts du régime et visant à discréditer des personnalités publiques ou régimes occidentaux. Rapportée en 2019 par Graphika, l'opération procède par l'usage de *deepfakes*, de messages ciblés et de spams afin de discréditer et dénigrer des individus, mais également afin d'empêcher l'usage les comptes de réseaux sociaux des personnes visées en empêchant toute interaction authentique avec les autres utilisateurs, mais également à instiguer la crainte par des opérations allant jusqu'au faux signalement (*swatting*). VIGINUM a documenté son activation directe en France à l'occasion des Jeux olympiques et paralympiques de Paris 2024, où entre le 1er et le 6 août 2024, des comptes affiliés à ce dispositif ont cherché à polariser le débat numérique autour de la cérémonie d'ouverture, tout en valorisant en parallèle le rôle de l'industrie chinoise dans la réussite de l'événement. Plus révélateur encore des limites de cette stratégie, VIGINUM a identifié un réseau d'une douzaine de sites de désinformation directement rattachés à la chaîne de télévision publique chinoise CGTN. L'opération a d'ailleurs été qualifiée d'échec relatif par le service français lui-même, signe que **la vigilance institutionnelle, quand elle est suffisamment outillée, peut désamorcer une partie de ce type de dispositif**. La différence de finalité avec la Russie est ici essentielle à la démonstration : il ne s'agit pas tant, pour Pékin, de délégitimer la démocratie française en tant que telle ou de fracturer le corps social, mais de **décrédibiliser les politiques hostiles ou opposés au régime chinois**, et de gagner, patiemment et sur la durée, la bataille de l'image dans un espace tiers où se joue une partie de la crédibilité internationale du régime.

C. Les États-Unis ou l'influence par l'infrastructure

Les ingérences américaines prennent une forme davantage marquée par **l'hybridité des méthodes**. L'intégration au sein du de la seconde gouvernance Trump d'acteurs privés de premier plan, tels qu'Elon Musk ou OpenAI, a modifié les rapports d'influences politiques et étatiques. Il ne s'agit plus ici seulement d'un service de renseignement étranger agissant clandestinement contre une démocratie considérée comme adverse, mais d'un ressortissant d'un État considéré comme allié, propriétaire d'une infrastructure numérique structurante pour le débat public français, qui prend position dans une élection nationale à visage découvert et s'exprime publiquement en soutien à des formations politiques proches du gouvernement américain, comme nous l'avons explicité ci-avant. Après avoir dénoncé, dès avril 2025, la condamnation en première instance de Marine Le Pen comme une « persécution » judiciaire et l'avoir encouragée à se présenter en 2027, le patron de X a réitéré son soutien le 15 juillet 2026 en la qualifiant, sur son propre réseau, de « dernier espoir de la France », relayant un compte affilié à une formation britannique d'extrême droite, vu par près de deux millions de personnes en quelques heures.

Ce geste d'Elon Musk s'inscrit dans un précédent déjà établi : le même soutien avait été apporté à

l'*AfD* lors des élections fédérales allemandes de février 2025. Mais le cas français a pris une tournure judiciaire inédite : le parquet de Paris avait ouvert dès janvier 2025 une enquête sur un possible usage de l'algorithme de X à des fins d'ingérence dans le débat politique français, enquête qui a débouché en avril 2026 sur une perquisition des locaux parisiens de la plateforme et sur des convocations à audition libre adressées à Elon Musk et à l'ancienne directrice générale de X, Linda Yaccarino. Quelques mois plus tôt, en décembre 2025, la Commission européenne avait déjà infligé à X une amende de 120 millions d'euros au titre du DSA pour manquements à la transparence de son registre publicitaire et à l'accès des chercheurs aux données de la plateforme. Il s'agissait de la toute première sanction financière prononcée dans le cadre de ce règlement, une décision aujourd'hui contestée par X devant le Tribunal de l'Union européenne.

La proximité de X avec le gouvernement américain a été établie à de nombreuses reprises, non seulement par l'utilisation systématique de la plateforme comme outil de communication par les membres de l'administration Trump, en sus de *Truth Social*, mais également par la brève nomination d'Elon Musk à la tête du département américain de l'efficacité gouvernementale (DOGE). Si des tensions ont pu émerger après l'officialisation du départ de Musk du gouvernement, les liens entre les deux hommes restent marqués.

Parallèlement, *Der Spiegel* révélait le 30 décembre 2025 que Donald Trump aurait envisagé plusieurs actions d'ingérence en sanctionnant des fonctionnaires allemands ayant classé l'*Afd* comme parti d'extrême-droite mais également en envisageant l'imposition de sanctions envers les magistrats prenant part au procès dans affaire des assistants parlementaires européens du Front national. Ces sanctions s'inscrivent dans une politique des sanctions menées par l'administration Trump, ayant par exemple visé Nicolas Guillou, juge français à la Cour pénale internationale suite à l'émission de mandats d'arrêts à l'encontre de hauts responsables israéliens, ou contre Thierry Breton, ancien commissaire européen chargé des règlements européens sur les marchés numériques (DMA) et sur les services numériques (DSA), interdit de visa pour les États-Unis, après l'adoption de textes plus régulateurs et de sanctions à l'encontre des plateformes.

> La question n'est plus seulement de savoir qui manipule le débat public, mais qui en possède l'infrastructure.

Ce cas illustre un déplacement conceptuel que ni la grammaire russe ni la grammaire chinoise ne permettent, à elles seules, de saisir : la question n'est plus seulement de savoir qui manipule le débat public, mais qui en possède l'infrastructure. La frontière classique entre la liberté d'expression d'un acteur privé étranger et l'ingérence dans un processus électoral s'effondre dès lors que cet acteur contrôle également l'algorithme de recommandation qui façonne la visibilité de chaque prise de position ou est en lien avec une puissance étrangère. Ce cas peut être qualifié de paradoxal : l'allié le plus proche de la France sur le plan technologique et sécuritaire est aussi celui dont un ressortissant privé peut influer sur le débat électoral national, dans un cadre juridique encore peu adapté à ce type de situation. La relation bilatérale franco-américaine introduit des considérations diplomatiques qui ne se posent pas dans les mêmes termes vis-à-vis de la Russie ou de la Chine. Ce paradoxe a d'ailleurs connu un net rebondissement rhétorique : **un rapport américain a récemment retourné l'accusation**, qualifiant le DSA lui-même, et la pression qu'il exercerait sur les plateformes, d'ingérence électorale massive imputable aux dirigeants européens. Ce retournement signale, mieux que tout autre exemple, la crise de la notion même d'ingérence, devenue un objet de contestation politique réciproque entre alliés, ce qui pourrait, à terme, complexifier la qualification juridique et politique de telles opérations

Par ailleurs, ces ingérences ne sont pas l'apanage des seules grandes puissances : des acteurs plus discrets, dotés de moyens plus modestes mais d'objectifs tout aussi ciblés, s'en emparent également. VIGINUM a ainsi documenté, dans son rapport « UN-notorious BIG » d'octobre 2024, l'activité numérique du *Baku Initiative Group* (BIG), officine de propagande d'État basée en Azerbaïdjan, se présentant faussement comme une ONG anticolonialiste. Entre juillet 2023 et octobre 2024, ce dispositif a mené, sur X, plusieurs campagnes coordonnées visant à instrumentaliser la situation politique et économique des départements, régions et collectivités d'Outre-mer ainsi que de la Corse, en y relayant des narratifs accusant la France de colonialisme et de néocolonialisme. Cette ligne d'action était directement liée au soutien français à l'Arménie dans le conflit du Haut-Karabakh. L'opération, marquée par un recours massif aux *Copy-Pasta*, n'est cependant pas parvenue à s'ancrer durablement dans le débat public francophone.

IV. Des risques systémiques pour la démocratie française

Au-delà des méthodes et des opérations, c'est la nature cumulative et systémique de ces ingérences qui appelle l'attention. Leur premier effet, le plus diffus mais sans doute le plus profond, relève moins de la conviction directe que de la saturation cognitive : comme le montre le MOI Storm-1516, l'objectif n'est pas tant de faire adhérer l'opinion française à un récit déterminé que d'**épuiser sa capacité collective à distinguer le vrai du faux**. Ce mécanisme produit un effet plus insidieux et plus durable qu'une simple fausse information ponctuelle, en ce qu'il érode la confiance générique envers l'information elle-même, y compris lorsqu'elle est vérifiée et sourcée, fragilisant ainsi le socle même sur lequel repose le débat démocratique. Les campagnes informationnelles tablent également sur les fragilités du tissu social français. En instrumentalisant des tensions vives et des sujets hautement polarisants, les acteurs se positionnent délibérément sur les terrains les plus difficiles à neutraliser, ceux-là mêmes qui mobilisent l'affect davantage que des éléments susceptibles d'être factuellement réfutés. Cet effet de sape se trouve d'autant plus décuplé que la France entre dans un cycle électoral particulièrement dense : l'enchaînement des scrutins européens de 2024, législatifs la même année, municipaux en 2026 et, à terme, présidentiel en 2027, constitue une fenêtre de vulnérabilité prolongée où chaque opération d'ingérence alimente la suivante dans la mémoire collective, entretenant un climat de défiance cumulative envers le processus électoral plutôt qu'un effet circonscrit à un seul rendez-vous.

La France a néanmoins pris conscience de cette menace, exacerbée par l'essor du numérique, comme en témoignent diverses évolutions législatives récentes. La réponse institutionnelle française s'est d'abord structurée autour de VIGINUM, chargé d'identifier et de documenter ce phénomène. Cette architecture institutionnelle s'est ensuite consolidée par voie législative : en 2024, l'adoption de la loi visant à prévenir les ingérences étrangères a marqué une étape décisive vers une répression accrue de ces pratiques, notamment par la création d'un registre numérique public des activités d'influence étrangère, placé sous la gestion de la Haute Autorité pour la transparence de la vie publique. Ce texte renforce en outre les capacités du renseignement, par le recours à des algorithmes de détection, et durcit la réponse pénale. D'autres instruments existent par ailleurs à l'échelle européenne, à l'instar du DSA, dont l'application demeure toutefois partielle. Les mécanismes d'urgence qu'il institue, destinés à responsabiliser les plateformes numériques, se révèlent en effet difficiles à mobiliser lorsque ces dernières se montrent peu enclines à coopérer. À l'approche des élections présidentielles, le Premier ministre, Sébastien Lecornu, a manifesté sa volonté de renforcer la lutte contre les ingérences étrangères, en déposant en juillet 2026 un projet de loi visant à préserver la qualité du débat démocratique.

> La dépendance de la France, et plus largement de l'Union européenne, à des dispositifs non souverains engendre une fragilité supplémentaire.

Parallèlement, la dépendance de la France, et plus largement de l'Union européenne, à des dispositifs non souverains engendre une fragilité supplémentaire, qui se manifeste sur trois plans principaux. D'un point de vue matériel, en ce qui concerne l'hébergement des données et les plateformes utilisées ; d'un point de vue algorithmique, la visibilité même du débat public dépendant de choix de conception opérés par des plateformes et modifiables unilatéralement ; et juridictionnelle enfin, le *Cloud Act* américain autorisant l'accès à des données européennes y compris hébergées sur le territoire européen, sans que le droit de l'Union n'ait encore trouvé de parade pleinement opérante. Indépendamment de toute intention malveillante éventuelle, cette configuration produit ce que l'on pourrait qualifier de **souveraineté par procuration : la France conserve la capacité formelle de légiférer sur son espace numérique, mais l'effectivité de cette législation dépend in fine de la coopération d'acteurs privés étrangers** soumis à un droit et à des intérêts qui ne coïncident pas nécessairement avec les siens. Cette situation pose donc la question, plus large, d'une souveraineté numérique européenne encore embryonnaire.

*****

L'examen comparé des dynamiques d'ingérences prégnantes en France, révèle moins une convergence des méthodes qu'une diversité des finalités poursuivies à travers un même terrain d'affrontement : celui de l'information. Les évolutions contemporaines invitent à dépasser une lecture strictement étatique de l'ingérence pour intégrer pleinement le rôle des acteurs privés transnationaux, dont l'influence peut désormais rivaliser avec celle des services de renseignement traditionnels, sans pour autant relever des mêmes outils de qualification ou de sanction. Ces stratégies informationnelles ne constituent par ailleurs pas nécessairement une fin en soi, mais un instrument au service d'une conflictualité hybride plus vaste, où l'ambiguïté délibérée du seuil permet à leurs commanditaires de peser sur les équilibres démocratiques tout en s'exonérant des cadres juridiques classiques de la sanction interétatique.

Pour la France, ces évolutions appellent une réponse à la mesure de leur caractère systémique : le renforcement des capacités de détection et de caractérisation, à l'image du travail conduit par VIGINUM, ne saurait suffire s'il n'est pas articulé à une réflexion plus large sur la souveraineté numérique européenne, sur l'adaptation du cadre juridique aux ingérences émanant d'acteurs privés alliés, et sur la préservation d'une définition opérationnelle claire de la notion même d'ingérence. À défaut, le risque n'est pas seulement celui d'une manipulation ponctuelle de l'opinion, mais celui, plus profond, d'un effritement progressif de la capacité collective à distinguer le vrai du faux, condition pourtant élémentaire de tout débat démocratique.

Copyright Septembre 2026-Ciftcisoy/Diploweb.com

P.-S.

L'auteure s'exprime ici en son nom propre. Alizéa-Maïwenn Ciftcisoy est docteure en droit et cheffe analyste-documentaliste à l'Office central de lutte contre les crimes contre l'humanité et les crimes de haine (OCLCH, Gendarmerie nationale). Chercheuse associée au CUREJ (Université de Rouen Normandie), ses travaux portent notamment sur la répression des crimes internationaux les plus graves, en particulier des violences sexuelles et fondées sur le genre.

Notes

[1] GRAHAM Timothy & ANDREJEVIC Mark, *A computational analysis of potential algorithmic bias on platform X during the 2024 US election,* Queensland University of Technology, 2024.

[2] GILLUM Jack, CORSE Alexa & TONG Adrienne, « X Algorithm Feeds Users Political Content – Whether They Want It or Not », The Wall Street Journal, 29 octobre 2024.

[3] Center for Countering Digital Hate, *Report : X Content Moderation Failure*, 2023.

[4] VOSOUGHI Soroush, ROY Deb et ARAL Sinan, « The Spread of true and false news online », Science, 9 mars 2018.

[5] VIGINUM, « Défis et opportunités de l'intelligence artificielle dans la lutte contre les manipulations de l'information », février 2025.

[6] MARIE Antoine, « L'IA dans les élections municipales 2026 : Des usages qui appellent un regard nuancé », Note de recherche du Cevipof, Collection Municipales 2026, n°9, avril 2026

[7] « Sébastien Lecornu alerte sur des « menaces lourdes » en matière d'ingérence étrangère pour la présidentielle et promet un projet de loi pour durcir les peines. » Le Monde. 11 juin 2026.