

**Désinformation et résilience informationnelle en Algérie : diagnostic des
vulnérabilités et cadre stratégique à la lumière du Global Risks Report 2026**

Pr. Noufeyle HADID - Université d'Alger 3

المخلص :

يصنّف تقرير المخاطر العالمية 2026 الصادر عن المنتدى الاقتصادي العالمي التضليل المعلوماتي في المرتبة الثانية ضمن المخاطر العالمية على المدى القصير، وفي المرتبة الرابعة على المدى الطويل. وبفعل تفاعله مع الاستقطاب المجتمعي وانعدام الأمن السيبراني والآثار السلبية للذكاء الاصطناعي، فإنه يشكّل خطرًا نظاميًا يهدد التماسك الاجتماعي والاستقرار المؤسسي. وانطلاقًا من تحليل نوعي يزاوج بين بيانات تقرير المخاطر العالمية 2026 واستطلاع إدراك المخاطر العالمية 2025-2026 واستطلاع آراء المديرين التنفيذيين 2025 وبين مصادر ثانوية حول الجزائر، تبين هذه الدراسة أن البلد، المنخرط في رقمنة متسارعة، يواجه أربعة تحديات: تثقيف إعلامي يحتاج إلى تعزيز، ومنظومة إعلامية معرضة للتضليل، وإطار تشريعي في طور التكييف، وقدرات كشف المحتويات التركيبية تستدعي التطوير. واستجابةً لذلك، تقترح الدراسة إطارًا استراتيجيًا للمرونة المعلوماتية يركز على خمسة دعائم: التعليم، والإعلام، والتكيف القانوني والمؤسسي، والقدرات التكنولوجية، والتعاون الدولي. وتُختلص إلى أنه، في السياق الجزائري، ينبغي النظر إلى المرونة المعلوماتية بوصفها أولوية استراتيجية للأمن الوطني.

الكلمات المفتاحية: التضليل المعلوماتي، المرونة المعلوماتية، التربية الإعلامية، الذكاء الاصطناعي، الأمن السيبراني، الجزائر

Résumé :

Le Global Risks Report 2026 du World Economic Forum classe la désinformation au 2e rang des risques mondiaux à court terme et au 4e rang à long terme. En interaction avec la polarisation sociétale, la cyber-insécurité et les effets négatifs de l'intelligence artificielle, elle constitue un risque systémique pour la cohésion sociale et la stabilité institutionnelle. À partir d'une analyse qualitative croisant les données du Global Risks Report 2026, de la Global Risks Perception Survey 2025-2026 et de l'Executive Opinion Survey 2025 avec des sources secondaires sur l'Algérie, cet article montre que le pays, engagé dans une numérisation rapide, fait face à quatre défis : une littératie médiatique à consolider, un écosystème médiatique exposé à la désinformation, un cadre normatif en adaptation, et des capacités de détection des contenus synthétiques à renforcer. En réponse, l'article propose un cadre stratégique de résilience informationnelle articulé autour de cinq piliers : éducation, médias, adaptation juridique et institutionnelle, capacités technologiques et coopération internationale. Il conclut que, dans le contexte algérien, la résilience informationnelle doit être pensée comme une priorité stratégique de sécurité nationale.

Mots-clés : désinformation, résilience informationnelle, littératie médiatique, intelligence artificielle, cybersécurité, Algérie.

Auteur expéditeur : Noufeyle HADID

1. Introduction:

1.1. Contexte général : un monde submergé par la désinformation:

L'édition 2026 du rapport du World Economic Forum (WEF) confirme la persistance de la désinformation au sommet des périls mondiaux. L'analyse de la figure 1 montre que ce risque occupe désormais la 2e position à court terme (horizon 2 ans) et la 4e à long terme (horizon 10 ans). Cette trajectoire témoigne d'une volatilité extrême de la menace : après être classée au 16e rang à court terme en 2023 (WEF, 2023), la désinformation a bondi au 1er rang mondial en 2024 (WEF, 2024) et 2025 (WEF, 2025), avant de se stabiliser au 2e rang pour cette année 2026 (WEF, 2026). Pour la troisième année consécutive, ce phénomène demeure ainsi ancré dans le trio de tête des menaces les plus sévères de notre époque.

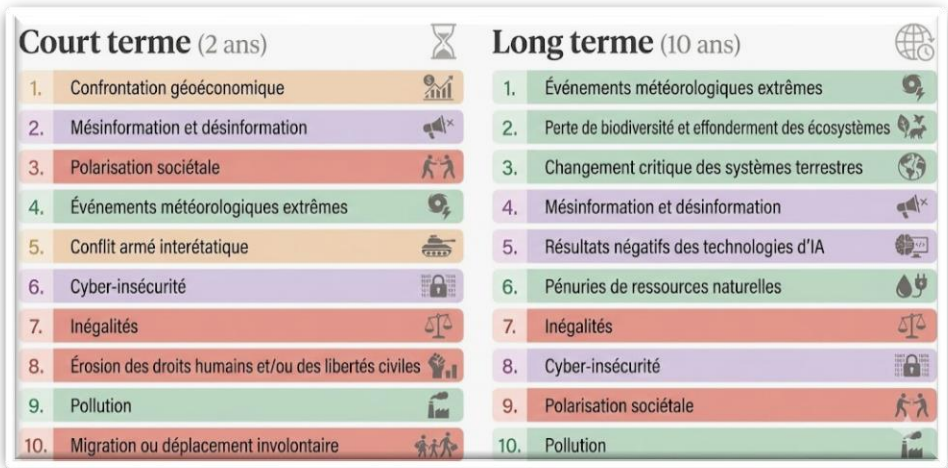


Figure 1 : Risques mondiaux : classement par sévérité à court terme et à long terme

Source : (WEF, 2026, p. 14)

Ce constat s'inscrit dans un contexte mondial caractérisé par une convergence inédite de facteurs amplificateurs. L'enquête annuelle "Global Risks Perception Survey 2025-2026 (GRPS)" constitue à cet égard l'outil annuel central du WEF, mobilisant plus de 1300 experts pour évaluer les menaces sur divers horizons temporels.

L'enquête de 2025-2026 révèle une dégradation du sentiment de sécurité : 50% des répondants anticipent des perspectives "turbulentes" ou "orageuses" à court terme, soit une hausse de 14 points par rapport à l'édition précédente. Cette vision s'assombrit à long terme avec 57% d'opinions pessimistes, contre seulement 1% de prévisions "calmes" (WEF, 2026, p. 7). La désinformation est identifiée comme à la fois un symptôme et un catalyseur de cette turbulence mondiale.

Cette turbulence s'inscrit dans le cadre plus large de ce que les stratégies militaires qualifient de guerre de quatrième génération (Fourth Generation Warfare : 4GW), définie comme "la guerre de l'information, impliquant des populations entières dans

tous les domaines : politique, économique, social et culturel" (Hadid, 2021a, p. 2). Une forme de guerre hybride qui mobilise les technologies numériques et les médias pour déstabiliser les États de l'intérieur, en substituant aux armes classiques la désinformation et des opérations psychologiques ciblant l'esprit et l'organisation de l'adversaire. Ce constat rejoint les analyses de Lind et al. (1989), pionniers du concept de 4GW, qui anticipaient dès la fin de la Guerre froide l'émergence de conflits asymétriques où l'information deviendrait l'arme principale.

1.2. Spécificités et vulnérabilités de l'Algérie face à la désinformation:

L'Algérie présente un profil de vulnérabilité particulier face au risque de désinformation. Avec une population de plus de 47 millions d'habitants, un taux de pénétration d'Internet avoisinant 77% et plus de 25 millions d'utilisateurs actifs des réseaux sociaux (Kemp, 2025), le pays se trouve au carrefour d'une transformation numérique accélérée et de dynamiques sociopolitiques complexes. Cette importante base d'utilisateurs, issue d'une population dont environ 54% a moins de 30 ans (ONS, 2019 ; UNFPA, 2022), constitue une surface d'exposition considérable aux campagnes de manipulation informationnelle, d'autant que les fausses informations se propagent sur Twitter/X, par exemple, six fois plus vite que les informations vraies (Vosoughi et al., 2018).

La transformation numérique, bien qu'essentielle pour la modernisation de l'État et de l'économie, génère simultanément de nouvelles vulnérabilités exploitables par des acteurs malveillants. Cette fragilité découle directement de l'ouverture sans précédent des systèmes d'information. En effet, "l'évolution des besoins et des technologies numériques, notamment celles du Cloud, des objets connectés et de l'intelligence artificielle (IA), et l'accroissement du nombre d'utilisateurs d'appareils mobiles, ont rendu les systèmes informatiques des entreprises et des institutions étatiques plus ouverts que jamais, donc plus fragiles et plus vulnérables" (Hadid, 2022, p. 2).

Cette vulnérabilité ne se limite pas à la cybersécurité au sens technique, mais s'étend à l'intégrité de l'espace informationnel dans son ensemble (Conti et al., 2018). En effet, "les approches traditionnelles de cybersécurité, lorsqu'elles sont utilisées de manière isolée (technologiques, organisationnelles, législatives, etc.), sont insuffisantes pour faire face à la complexité et à la sophistication croissantes des menaces" (Hadid, 2024a, p. 158).

Par ailleurs, l'Algérie se situe dans une région — le Moyen-Orient et l'Afrique du Nord (MENA) — particulièrement exposée à la désinformation. Selon le Digital News Report 2025, publié en juin 2025 par le Reuters Institute for the Study of Journalism de l'Université d'Oxford, 73% des répondants africains se disent préoccupés par la difficulté de distinguer le vrai du faux dans l'information en ligne, un chiffre nettement supérieur à la moyenne mondiale de 58% (Newman et al., 2025, cité dans WEF, 2026, p. 34). Cette préoccupation régionale est amplifiée par la faible modération des

contenus en langue arabe et en dialectes locaux sur les principales plateformes numériques (Shahid et al., 2025), ainsi que par l'accessibilité croissante des outils de création de deepfakes qui rendent la production de contenus synthétiques en langue arabe de plus en plus aisée (Paris et Donovan, 2019). L'ensemble de ces facteurs place l'Algérie dans une position où le risque de désinformation, tel que caractérisé par le WEF comme le deuxième risque mondial le plus sévère à court terme, revêt une pertinence stratégique de premier ordre.

1.3. Question de recherche:

Dans quelle mesure le risque de désinformation, tel qu'identifié par le WEF, se manifeste-t-il dans le contexte algérien, et quelles stratégies l'Algérie devrait-elle déployer pour construire une résilience informationnelle durable ?

1.4. Objectifs:

Cet article poursuit quatre objectifs : (a) analyser en profondeur le risque de désinformation tel que caractérisé par le WEF et ses interconnexions avec les autres risques mondiaux ; (b) évaluer la position spécifique de l'Algérie face à ce risque ; (c) identifier les vulnérabilités structurelles de l'écosystème informationnel algérien ; (d) proposer un cadre stratégique de résilience informationnelle adapté au contexte national.

2. Cadre théorique et méthodologique:

2.1. Définitions:

La désinformation, selon la définition de référence dans la littérature académique, désigne "une information fausse, délibérément créée et diffusée dans l'intention de nuire à une personne, un groupe social, une organisation ou un pays" (Wardle et Derakhshan, 2017, p. 20). Wardle et Derakhshan ont proposé un cadre conceptuel influent, illustré par la figure 2 ci-dessous, distinguant trois formes de désordre informationnel selon les axes du Faux et du Nuisible. La première, la mésinformation, située dans la sphère du "Faux", regroupe les contenus erronés comme les connexions fausses, mais diffusés sans intention de nuire. La deuxième, la désinformation, représentée à l'intersection centrale, concerne les informations fausses créées délibérément pour nuire, tels que les contenus fabriqués ou manipulés. La troisième, la malinformation, située dans la sphère du "Nuisible", désigne une information vraie utilisée pour causer du tort, à l'image des fuites ou du harcèlement. Ce cadre, adopté par l'UNESCO (Ireton et Posetti, 2018 ; Posetti et Bontcheva, 2020) et le Conseil de l'Europe (Wardle et Derakhshan, 2017), reste la référence analytique dans le domaine pour cartographier les menaces informationnelles contemporaines.

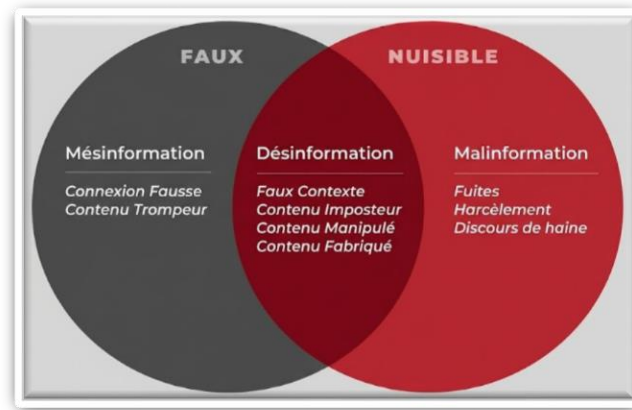


Figure 2 : Trouble de l'information

Source : (Wardle et Derakhshan, 2017, p. 20)

Quant au WEF, il définit la désinformation comme la diffusion massive et persistante d'informations délibérément fausses par les réseaux médiatiques, "orientant de manière significative l'opinion publique vers une méfiance à l'égard des faits et de l'autorité. Cela inclut, sans s'y limiter, les contenus faux, usurpés, manipulés et fabriqués" (WEF, 2026, Appendice A, p. 76).

Dans ce contexte, l'utilisation intensive des technologies de l'information, malgré ses apports en matière de gouvernement électronique et d'économie numérique, porte en elle de nombreux risques pouvant engendrer des atteintes très graves "touchant la crédibilité des informations circulant dans l'espace numérique, la vie privée des individus et le bon fonctionnement des institutions de l'État" (Hadid, 2021b, p. 7). Ce constat est corroboré par Benkler et al. (2018), qui documentent comment les écosystèmes médiatiques en réseau créent de nouvelles vulnérabilités informationnelles dans les sociétés en transition.

2.2. Le cadre d'analyse des risques mondiaux du WEF:

Le GRPS évalue 33 risques mondiaux, classés en cinq catégories (économique, environnemental, géopolitique, sociétal, technologique) selon leur sévérité probable sur une échelle de Likert à 7 points, sur trois horizons temporels : immédiat (2026), court-moyen terme (2028) et long terme (2036). Ce GRPS repose sur les réponses de plus de 1300 experts issus du monde académique, du business, des gouvernements, des organisations internationales et de la société civile. Le WEF intègre également l'Executive Opinion Survey (EOS), qui recueille les perceptions de plus de 11000 dirigeants d'entreprise (business leaders) dans 116 économies. Cette enquête cible spécifiquement les risques les plus sévères par pays sur deux ans, révélant des "points chauds" régionaux (WEF, 2026, pp. 6-7).

Le GRPS offre une vue globale experte, tandis que l'EOS apporte une perspective locale et orientée business, enrichissant ainsi l'analyse des risques.

2.3. Le cadre de la convergence cybercriminalité-désinformation:

La désinformation, classée n°2 au GRPS et étroitement corrélée à la cyber-insécurité classée n°6, illustre la convergence des menaces hybrides. Les interconnexions analysées montrent que la polarisation sociétale amplifie la désinformation, créant un cercle vicieux (WEF, 2026). Les deepfakes et contenus IA-synthétiques brouillent la frontière réel/fiction et menacent directement la confiance démocratique (WEF, 2026).

Les solutions traditionnelles appliquées de manière isolée ne parviennent plus à répondre aux menaces sophistiquées et interconnectées, nécessitant des approches holistiques intégrant cybersécurité avancée et résilience informationnelle.

2.4. Approche méthodologique:

Notre analyse repose sur une approche qualitative fondée sur le croisement de trois catégories de sources complémentaires, articulées selon une logique multi-scalaire.

La première catégorie, qui constitue le socle empirique principal de cet article, est constituée des données primaires du WEF, à savoir le GRPS 2025-2026 et l'EOS 2025, dont les caractéristiques méthodologiques ont été présentées en section 2.2. Ces deux instruments permettent d'analyser le risque de désinformation à la fois dans sa dimension mondiale et dans sa manifestation spécifiquement algérienne.

La deuxième catégorie regroupe les rapports internationaux spécialisés dans l'intégrité informationnelle et l'écosystème numérique, notamment le Digital News Report 2025 du Reuters Institute (Newman et al., 2025), le World Justice Project Rule of Law Index 2025 et les données de DataReportal (2025) sur le profil numérique de l'Algérie.

La troisième catégorie est constituée de la littérature académique, mobilisée à trois niveaux : le niveau théorique général sur le désordre informationnel et la perception des risques (Wardle et Derakhshan, 2017 ; Slovic, 2000 ; Vosoughi et al., 2018) ; le niveau de la cybersécurité et de la cyberrésilience, dont les cadres ont été exposés en sections 2.1 et 2.3 ; et le niveau régional nord-africain (Bradshaw et Howard, 2019 ; Shahid et al., 2025).

Cette triangulation permet de croiser les perspectives macro (risques mondiaux), méso (dynamiques régionales) et micro (écosystème informationnel algérien). Il convient toutefois de souligner une limite : l'absence de données primaires collectées directement auprès de la population ou des institutions algériennes, notre analyse du contexte national reposant principalement sur des données secondaires, ce qui constitue une piste pour des recherches futures mobilisant des enquêtes de terrain.

3. La désinformation dans le Global Risks Report 2026 : une analyse approfondie:

3.1. Perception par groupe de parties prenantes:

Le WEF offre une granularité inédite dans l'analyse des perceptions par groupe de parties prenantes et par tranche d'âge. Le tableau 1 présente le classement de la désinformation selon les différents groupes de parties prenantes interrogés dans le cadre du GRPS sur l'horizon court terme.

Tableau 1 : Classement de la désinformation par groupe de parties prenantes (court terme)

Groupe de parties prenantes	Rang de la désinformation	Observation
Organisations internationales	Top 3	Préoccupation forte
Société civile	Top 3	Préoccupation forte
Monde académique	Top 3	Préoccupation forte
Gouvernements	Top 5	Préoccupation significative
Secteur privé	Top 5	Préoccupation significative

Source : Élaboration de l'auteur à partir de WEF (2026), pp. 17-18

L'analyse révèle un consensus remarquable entre les différentes catégories de parties prenantes. Les organisations internationales, la société civile et le monde académique placent unanimement la désinformation dans le trio de tête des risques les plus sévères, tandis que les gouvernements et le secteur privé la maintiennent dans le Top 5. Cette convergence transversale souligne le caractère systémique de la menace : la désinformation n'est plus perçue comme un enjeu sectoriel, mais comme un risque structurel affectant l'ensemble des sphères de gouvernance, de production et de mobilisation sociale.

Le tableau 2 complète cette analyse en détaillant la perception de la désinformation selon les tranches d'âge des répondants au GRPS.

Tableau 2 : Classement de la désinformation par tranche d'âge (court terme)

Tranche d'âge	Rang relatif de la désinformation	Observation clé
Moins de 30 ans	1er devant la confrontation géoéconomique	La désinformation prime sur les risques géoéconomiques
30-39 ans	Top 3	Préoccupation forte
40-49 ans	Top 3	Préoccupation forte
50-59 ans	Top 3	Préoccupation forte
60-69 ans	Top 5	Relativement moins prioritaire
70 ans et plus	Top 5	Relativement moins prioritaire

Source : Élaboration de l'auteur à partir de WEF (2026), p. 18

Ce tableau fait apparaître un clivage générationnel significatif. Le fait que les répondants de moins de 30 ans classent la désinformation comme le premier risque mondial est particulièrement révélateur pour un pays comme l'Algérie, dont la population est majoritairement jeune. Cette jeunesse constitue la population la plus active sur les réseaux sociaux, ce qui en fait la cible privilégiée des campagnes de manipulation informationnelle. En effet, selon l'enquête Eurobarometer Youth Survey

2024 du Parlement européen, publiée en février 2025, 42% des jeunes européens de 16 à 30 ans s'informent principalement via les réseaux sociaux, et 76% d'entre eux déclaraient avoir été exposés à de fausses informations au cours de la semaine précédant l'enquête (European Parliament, 2025 ; Batista Cabanas, 2025). Ce phénomène de surexposition est amplifié par la vitesse de propagation des contenus trompeurs en ligne : Vosoughi et al. (2018) ont démontré que les fausses informations se propagent sur Twitter/X six fois plus vite que les informations vraies.

3.2. Interconnexions systémiques:

Le WEF modélise les interconnexions entre les 33 risques mondiaux à partir des réponses du GRPS. L'analyse de ces interconnexions révèle que la désinformation fonctionne comme un risque amplificateur qui exacerbe la sévérité de multiples autres risques, comme le met en évidence la figure 3 ci-dessous.

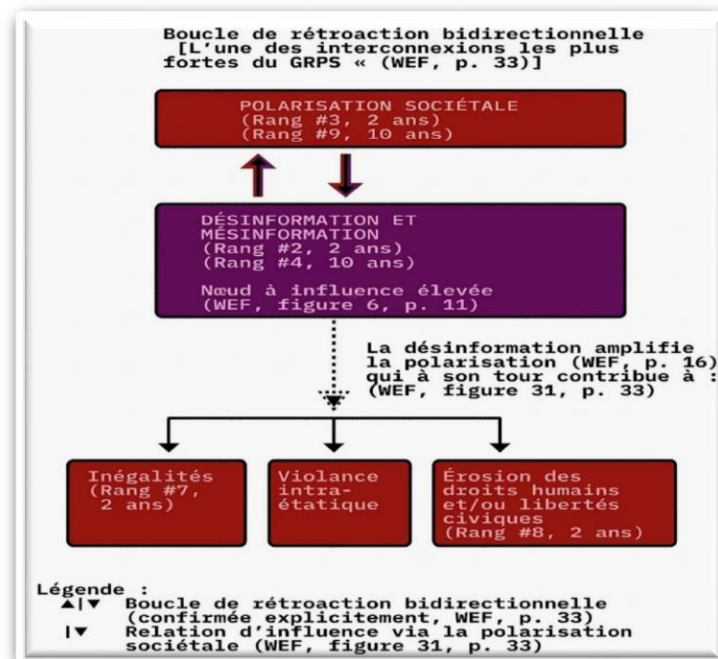


Figure 3 : Boucle désinformation–polarisation et ses effets sur les risques mondiaux

Source : Élaboration de l'auteur à partir de WEF (2026), Figures 6 (p. 11) et 31 (p. 33)

Le rapport identifie explicitement l'une des interconnexions les plus fortes du GRPS comme étant celle entre la polarisation sociale et la désinformation (WEF, 2026, p. 33). Ces deux risques se renforcent mutuellement dans une boucle de rétroaction. Cette dynamique rejoint les analyses de Sunstein (2017) sur les "chambres d'écho", où les algorithmes des plateformes numériques enferment les utilisateurs dans des bulles informationnelles qui renforcent leurs convictions préexistantes et amplifient la polarisation (Sunstein, 2017). Par ailleurs, dans le contexte géopolitique de l'Algérie, les cyber-opérations entre États rivaux s'inscrivent dans des dynamiques de rivalité stratégique de long terme, dépassant le cadre d'intrusions techniques isolées (Mauslein et Pickering, 2021), ce qui renforce la vulnérabilité de l'espace informationnel national aux ingérences extérieures.

Le point essentiel de la figure 3 est que les trois conséquences de cette polarisation — inégalités, violence intra-étatique et érosion des droits humains et/ou libertés civiques — ne sont pas linéaires mais systémiques. Le rapport le dit explicitement : "Cet ensemble de risques est profondément imbriqué, avec des impacts dans toutes les directions" (WEF, 2026, p. 33). Concrètement, les inégalités alimentent le ressentiment qui nourrit la violence intra-étatique ; la violence intra-étatique crée des situations d'urgence qui justifient la restriction des droits humains et/ou libertés civiques ; l'érosion des droits empêche les citoyens de contester les politiques qui creusent les inégalités, et ainsi de suite. La désinformation, via la polarisation, est le détonateur qui met en mouvement ce cercle vicieux. C'est précisément pour cette raison que le WEF l'identifie comme un "nœud à influence élevée" (WEF, 2026, p. 11) : elle n'est pas seulement un risque parmi d'autres, mais un multiplicateur systémique qui aggrave l'ensemble du paysage des risques mondiaux.

3.3. Données empiriques mondiales sur l'écosystème informationnel:

Le WEF s'appuie sur des données empiriques récentes du Reuters Institute Digital News Report 2025 pour documenter la dégradation de l'écosystème informationnel mondial. Le tableau 3 ci-dessous synthétise les principaux indicateurs de cette dégradation.

Tableau 3 : Évolution récente de l'écosystème informationnel mondial

Indicateur	2018	2025	Évolution
Confiance dans les médias d'information	44%	40%	-4 points
Évitement actif de l'information (news avoidance)	32%	40%	+8 points
Préoccupation face à la désinformation	54%	58%	+4 points
Part des personnes utilisant les réseaux sociaux comme source principale d'information (États-Unis)	4% (2015)	34% (2025)	+30 points
Part des personnes utilisant des outils d'IA pour s'informer	11% (2024)	24% (2025)	+13 points

Source : Élaboration de l'auteur à partir de Newman et al. (2025) et Simon et al. (2025), cités dans le rapport du WEF (2026), Figure 33, p. 35, et pp. 35-36

Ce tableau met en évidence une triple dégradation de l'écosystème informationnel mondial : une confiance en baisse, un évitement en hausse et une préoccupation croissante face à la désinformation. Le basculement le plus frappant concerne les États-Unis, où la part des personnes citant les réseaux sociaux comme source principale d'information est passée de 4% à 34% en une décennie, signalant un transfert massif vers des environnements moins régulés et plus propices à la désinformation (WEF, 2026, pp. 35-36).

3.4. Perception nationale : l'Exécutive Opinion Survey (EOS):

Les données de l'EOS 2025 confirment la dimension mondiale de ce risque. La désinformation est classée parmi les 10 premiers risques nationaux dans 67 pays et

constitue le risque le plus important dans 4 économies (WEF, 2026, p. 34). Le tableau 4 présente le classement régional de ce risque.

Tableau 4 : Classement de la désinformation dans l'EOS par région (2025)

Région	Rang de la désinformation dans le classement régional	Position relative
Amérique du Nord	2e	Très élevé
Europe	Top 3	Très élevé
Asie de l'Est	Top 3	Très élevé
Moyen-Orient et Afrique du Nord (MENA)	Top 10	Élevé
Afrique subsaharienne	Top 10	Élevé
Amérique latine	Top 10	Élevé

Source : Élaboration de l'auteur à partir de WEF (2026), Figure 34, p. 35 ; EOS (2025)

Ce tableau confirme que la désinformation est perçue comme une menace de premier plan dans toutes les régions du monde, avec une intensité particulièrement marquée dans les économies avancées d'Amérique du Nord, d'Europe et d'Asie de l'Est, où l'hyperconnectivité numérique amplifie la vulnérabilité des écosystèmes informationnels.

Pour l'Algérie, plus spécifiquement, l'examen des données de l'EOS dans l'Appendice C du rapport du WEF 2026 (WEF, 2026, pp. 82-90) révèle que la désinformation ne figure pas parmi les cinq premiers risques identifiés par les dirigeants d'entreprise algériens, ceux-ci étant dominés par des préoccupations macroéconomiques (WEF, 2026, p. 82), comme le détaille le tableau 5 ci-dessous.

Tableau 5 : Les cinq premiers risques identifiés pour l'Algérie dans l'EOS 2025

Rang	Risque identifié	Catégorie
1er	Inflation	Économique
2e	Manque d'opportunités économiques ou chômage	Sociétal
3e	Perturbations d'une chaîne d'approvisionnement d'importance systémique	Économique
4e	Perturbations des infrastructures critiques	Économique
5e	Éclatement de bulles d'actifs	Économique

Source : Élaboration de l'auteur à partir de WEF (2026), Appendice C, Tableau C.2, p. 82

L'absence de la désinformation dans le top 5 algérien traduit vraisemblablement une sous-estimation du risque informationnel par les décideurs économiques. Ce biais perceptuel a été documenté dans la littérature sur la cybersécurité : Schneier (2008) note que les individus et les organisations tendent systématiquement à sous-estimer les risques numériques tant qu'ils n'ont pas été directement affectés, un phénomène lié au "biais d'optimisme". Dans les pays en développement, ce biais est amplifié par les barrières économiques et institutionnelles qui relèguent les risques numériques au second plan (Kshetri, 2019).

3.5. Le facteur amplificateur de l'IA et des deepfakes:

Le WEF établit un lien explicite entre les progrès de l'IA générative et l'amplification du risque de désinformation. La section 2.3 ("Values at war") souligne

que "l'intégrité de l'information en ligne est de plus en plus menacée, car distinguer entre contenu authentique et contenu synthétique — qu'il s'agisse de vidéo, d'audio ou de texte — devient progressivement plus difficile" (WEF, 2026, p. 34). Le tableau 6 ci-dessous synthétise les indicateurs clés présentés dans le rapport à cet égard.

Tableau 6 : Désinformation à l'ère de l'IA : données clés de contexte citées par le WEF

Indicateur	Valeur	Source dans le rapport
Part des répondants préoccupés par les deepfakes affectant les résultats électoraux (Royaume-Uni)	87%	Dennehy (2024), cité dans WEF (2026, p. 36)
Nombre de conflits actifs dans le monde en 2024	61 conflits dans 36 pays	PRIO (2025), cité dans WEF (2026, p. 36)
Part des utilisateurs américains citant les réseaux sociaux comme source principale d'information	34% (contre 4% en 2015)	Simon et al. (2025), cité dans WEF (2026, p. 36)
Part des utilisateurs recourant à des outils d'IA pour s'informer	24% (contre 11% en 2024)	Simon et al. (2025), cité dans WEF (2026, p. 36)

Source : Élaboration de l'auteur à partir de WEF (2026), chapitre 2.3, pp. 34-36

L'IA est devenue "une arme à double tranchant" dans sa relation avec la désinformation et la démocratie : elle peut être utilisée pour renforcer la démocratie, mais elle peut également être mobilisée pour saper les fondements démocratiques par la diffusion de fausses nouvelles et la désinformation médiatique (Hadid, 2024b). Cette ambivalence de l'IA est confirmée par Chesney et Citron (2019), qui qualifient les deepfakes de "dividendes du mensonge", dans la mesure où leur simple existence permet à quiconque de nier l'authenticité de contenus réels en prétendant qu'ils ont été fabriqués par l'IA (Chesney et Citron, 2019).

4. L'Algérie face à la désinformation : diagnostic multidimensionnel:

4.1. L'écosystème numérique algérien : une surface d'exposition croissante:

L'Algérie connaît une transformation numérique qui élargit considérablement son espace d'exposition à la désinformation. Bien qu'indispensable à la modernisation de l'économie et de l'administration, cette transformation génère simultanément de nouvelles vulnérabilités informationnelles et cybernétiques. Cette dynamique s'inscrit dans une orientation nationale explicite, qui considère la numérisation comme un levier central du développement socio-économique du pays tout en soulignant que sa réussite dépend de la sécurisation du cyberspace national et de la protection du patrimoine informationnel de l'État (ASSI, 2026).

Dans la même perspective, Schwab (2016) inscrit cette dynamique dans le cadre de la quatrième révolution industrielle, où la vitesse d'adoption technologique dépasse souvent la capacité des sociétés à en maîtriser les risques. Le tableau 7 ci-dessous dresse le profil numérique de l'Algérie et met en évidence l'ampleur de cette surface d'exposition.

Tableau 7 : Profil numérique de l'Algérie : données les plus récentes disponibles

Indicateur	Valeur	Implications pour la désinformation
Population totale	~47 millions	Large base démographique exposée
Âge médian	28,6 ans	Population jeune, forte consommation numérique
Population de moins de 30 ans	~54%	Population jeune, forte consommation numérique
Taux de pénétration d'Internet	~77% (36,2 millions d'internautes)	Exposition massive à l'information en ligne
Nombre d'abonnés mobiles	~55 millions (116% de la population)	Accès quasi-universel aux plateformes numériques
Utilisateurs actifs des réseaux sociaux	~26 millions (~54% de la population)	Vecteur principal de circulation de la désinformation
Plateforme dominante	Facebook (~26 millions d'utilisateurs)	Faible modération en langues arabe, amazighe et en darija
Deuxième plateforme	TikTok (~21 millions d'utilisateurs)	Croissance rapide (+21% en un an), contenu viral peu vérifié
Temps moyen quotidien sur les réseaux sociaux	~3 heures (estimation)	Exposition prolongée aux contenus non vérifiés
Taux d'alphabétisation	~81%	Défis persistants en littératie médiatique et numérique

Sources : Élaboration de l'auteur à partir de Kemp (2025) ; ONS (2019) ; UNFPA (2022) ; Banque mondiale (2018).

La lecture croisée de ces indicateurs révèle un écosystème numérique à la fois dynamique et fragile. Le taux de pénétration d'Internet a progressé de 73% à 77% en seulement un an (Kemp, 2024 ; Kemp, 2025), tandis que TikTok a enregistré une croissance de 21% sur la même période, dépassant les 21 millions d'utilisateurs adultes. Cette expansion rapide, combinée à un âge médian de 28,6 ans et à un taux d'alphabétisation qui, bien qu'en progression, reste insuffisant pour garantir une littératie médiatique efficace, fait de l'Algérie un terrain particulièrement réceptif aux campagnes de manipulation informationnelle.

4.2. Matrice des vulnérabilités informationnelles algériennes:

L'analyse du profil numérique algérien présenté dans la section précédente met en lumière une surface d'exposition croissante, mais elle ne suffit pas à elle seule à caractériser la nature des vulnérabilités auxquelles le pays fait face. Pour affiner ce diagnostic, il convient d'identifier les fragilités structurelles qui amplifient l'impact potentiel de la désinformation sur la société algérienne. La matrice ci-dessous (tableau 8) propose une cartographie de ces vulnérabilités, organisées en quatre catégories, en évaluant leur niveau de risque et en les articulant avec les constats du WEF.

Tableau 8 : Matrice des vulnérabilités informationnelles de l'Algérie

Catégorie de vulnérabilité	Description détaillée	Niveau de risque	Lien avec le rapport
1. faible littératie médiatique	Absence d'éducation aux médias dans les curricula scolaires et universitaires ; faible capacité de la population à identifier les contenus manipulés ; confusion entre opinion, information et désinformation	Critique	Le WEF identifie la sensibilisation et l'éducation du public comme l'approche n°1 pour réduire la polarisation sociétale, avec 29% des répondants (WEF, 2026, section 2.3). L'UNESCO qualifie la littératie médiatique et informationnelle de "première ligne de défense" contre la désinformation (UNESCO, 2020, citant R. Tuazon ; réitéré dans UNESCO, 2023)
2. vulnérabilité de l'écosystème médiatique	Presse écrite en crise économique; concentration de l'audience sur les réseaux sociaux au détriment des médias professionnels ; recul de la confiance dans les médias institutionnels	Élevé	La confiance mondiale dans les médias est passée de 44% en 2018 à 40% en 2025, niveau stable depuis trois ans, avec une remontée temporaire à 44% durant le pic COVID en 2021 (Reuters Institute, Digital News Report 2018 et 2025). Le WEF confirme que "la confiance dans l'information recule et l'évitement de l'actualité progresse" (WEF, 2026, section 2.3, Figure 33).
3. limites du cadre normatif	Loi n° 20-06 du 28 avril 2020 modifiant le code pénal, dont l'article 196 bis incrimine la diffusion volontaire de fausses informations portant atteinte à l'ordre ou à la sécurité publics (JORADP, n° 25) ; cadre renforcé par l'ordonnance n° 21-08 du 8 juin 2021. Toutefois, absence de loi autonome et globale sur la désinformation en ligne ; à notre connaissance, il n'existe pas d'obligation de transparence algorithmique pour les plateformes en Algérie.	Élevé	Le WEF souligne que l'adoption à grande échelle de solutions d'authentification des contenus nécessite des cadres politiques alignés sur des principes partagés, des règles communes et des normes technologiques (WEF, 2026, section 2.3).
4. faibles capacités de détection des contenus synthétiques	Production croissante de contenus synthétiques en langue arabe ; faible capacité de détection ; Absence d'outils de vérification adaptés à l'amazighe et au darija.	Élevé	Le WEF note que la création de deepfakes est devenue "plus facile, moins coûteuse et plus convaincante" au cours des cinq dernières années (WEF, 2026, section 2.3). Paris et Donovan (2019) distinguent les deepfakes, techniquement exigeants mais de plus en plus accessibles grâce à des outils open source (FakeApp, FaceSwap, DeepFaceLab), des cheap fakes, réalisables sans compétences techniques via de simples applications mobiles gratuites (Paris et Donovan, 2019).

Source : Élaboration de l'auteur à partir de WEF (2026) ; Newman et al. (2018 ; 2025) ; UNESCO (2020) ; Paris et Donovan (2019) ; JORADP (2020).

Cette matrice fait ressortir un constat majeur : la seule vulnérabilité évaluée au niveau "critique" est celle de la littératie médiatique et numérique. Ce résultat converge avec les conclusions du WEF, qui place l'éducation et la sensibilisation publiques au premier rang des mesures d'atténuation (WEF, 2026, p. 39). En d'autres termes, les trois autres vulnérabilités — écosystème médiatique, cadre normatif et faibles capacités de détection des contenus synthétiques — voient leur impact démultiplié par l'absence d'un socle solide de compétences informationnelles au sein de la population. Cette interdépendance suggère que toute stratégie de résilience informationnelle en Algérie devrait accorder une priorité structurelle au développement de la littératie médiatique, en amont des réponses technologiques ou réglementaires.

4.3. Cartographie des types de désinformation affectant l'Algérie:

L'écosystème informationnel algérien est particulièrement exposé aux opérations de manipulation. Selon BBC Media Action (2021), 93% des utilisateurs algériens de réseaux sociaux ont été confrontés à de fausses informations, dont 31% quotidiennement. Ce constat s'inscrit dans une dynamique mondiale où Bradshaw et Howard (2019) recensent des campagnes organisées de manipulation dans 70 pays. Le tableau 9 synthétise les six catégories de désinformation identifiées.

Tableau 9 : Typologie de la désinformation en Algérie

Type	Description	Exemples observés	Vecteur principal	Impact
Désinformation politique interne	Manipulation de l'information pour influencer le débat politique national	Faux comptes sur les réseaux sociaux; campagnes de dénigrement ; fausses déclarations attribuées à des personnalités	Facebook, YouTube	Érosion de la confiance institutionnelle
Désinformation géopolitique	Campagnes liées à la question du Sahara occidental	Faux reportages, manipulation d'images satellite, décontextualisation d'événements	Twitter/X, sites web, Telegram	Exacerbation des tensions régionales
Désinformation sanitaire	Diffusion de fausses informations sur les traitements, vaccins, épidémies	Remèdes miracles, théories du complot anti-vaccins (amplifiées pendant la COVID-19)	WhatsApp, Facebook	Risques pour la santé publique
Désinformation économique	Rumeurs sur les pénuries, manipulations de prix, fausses annonces économiques	Fausses alertes sur les pénuries alimentaires ; rumeurs sur les taux de change	Facebook, WhatsApp	Paniques d'achat, instabilité des marchés informels
Contenus synthétiques, dont les	vidéos, enregistrements audio et images générées par IA	Faux discours de responsables, vidéos manipulées	YouTube, TikTok, Telegram	Destruction de la confiance dans l'information

deepfakes		de personnalités publiques		visuelle
Désinformation diasporique	Contenus produits par certains segments de la diaspora algérienne établis à l'étranger, issus de cercles se revendiquant de l'opposition	Chaînes YouTube à forte audience, comptes militants actifs de la diaspora dite "opposante"	YouTube, Facebook, TikTok	Amplification des clivages identitaires et politiques au sein de la société algérienne

Source : Élaboration de l'auteur à partir de Bradshaw et Howard (2019) ; Gursky et al. (2021) ; Dou (2023) ; BBC Media Action (2021)

Le tableau met en évidence la diversité des vecteurs et des finalités de la désinformation en Algérie. Bradshaw et Howard (2019) ont démontré que les "troupes cybernétiques" opèrent dans 70 pays via faux comptes et manipulation algorithmique. Dou (2023) confirme Facebook comme vecteur principal de l'infodémie dans le pays. Gursky, Riedl et Woolley (2021) montrent par ailleurs que les diasporas sont à la fois cibles et relais de désinformation via les messageries chiffrées, un phénomène potentiellement transposable au contexte algérien.

5. Cadre stratégique pour la résilience informationnelle de l'Algérie:

5.1. De la cybersécurité à la cyberrésilience informationnelle:

La construction d'une résilience informationnelle pour l'Algérie ne peut se concevoir dans le seul cadre de la cybersécurité classique. Le NIST Cybersecurity Framework (NIST, 2024) propose une approche en cinq fonctions — Identifier, Protéger, Détecter, Répondre et Récupérer — qui, transposée au domaine informationnel, implique non seulement de prévenir la désinformation, mais aussi de doter la société des capacités de résistance et de récupération face aux campagnes informationnelles. Sa mise en œuvre requiert le passage d'une logique de protection statique à une logique de cyberrésilience, capable d'anticiper, de résister et de se rétablir face aux campagnes de désinformation. En effet, la théorie des systèmes complexes appliquée à la cybersécurité montre que "les organisations doivent être conceptualisées comme des systèmes dynamiques composés de multiples éléments interagissant de manière non linéaire", et que la sécurité nécessite "une compréhension multidimensionnelle incluant les aspects technologiques ainsi que les dynamiques comportementales et culturelles des utilisateurs" (Hadid, 2024a, pp. 148-150). Cette approche sociotechnique est directement transposable à la lutte contre la désinformation.

Ce changement de paradigme — de la cybersécurité statique à la cyberrésilience dynamique — est d'autant plus nécessaire que le WEF (2026, p. 9) souligne que les risques technologiques "se développent en grande partie sans contrôle", dépassant la capacité des cadres réglementaires et institutionnels existants à y répondre. Dans le contexte algérien, où les urgences macroéconomiques tendent à reléguer les risques informationnels au second plan (WEF, 2026, p. 82), cette transition suppose un effort de sensibilisation stratégique auprès des décideurs publics et privés quant à la nature

systémique de la menace de désinformation. Comme le souligne Schneier (2008), les organisations tendent systématiquement à sous-estimer les menaces numériques tant qu'elles n'ont pas été directement affectées.

5.2. Modèle proposé : les cinq piliers de la résilience informationnelle:

En nous appuyant sur les recommandations du WEF et sur la littérature spécialisée, nous proposons un cadre stratégique intégrateur articulé autour de cinq piliers complémentaires : (1) l'éducation et la littératie médiatique ; (2) un écosystème médiatique pluraliste et résilient; (3) un cadre juridique et institutionnel adapté ; (4) des capacités technologiques de détection et de réponse ; et (5) la coopération internationale et régionale.

Ce modèle ne repose pas sur une logique défensive étroite, mais sur une conception évolutive de la résilience informationnelle. Il s'agit non seulement de prévenir la désinformation, mais également de détecter rapidement les campagnes informationnelles hostiles, d'y répondre de manière coordonnée, puis de restaurer la confiance dans l'espace informationnel national. Cette approche est cohérente avec l'esprit de la doctrine nationale en matière de sécurité des systèmes d'information, laquelle rappelle explicitement que "la stratégie nationale de la sécurité des systèmes d'information ne constitue nullement une fin en soi et elle n'a de valeur que si elle est évaluée, autant que faire se peut, pour la maintenir en adéquation avec les évolutions technologiques et les objectifs escomptés" (ASSI, 2026, préface). La boucle de rétroaction intégrée à notre modèle — évaluation, adaptation, amélioration continue — trouve ainsi un fondement direct dans cette vision stratégique nationale.

Le premier pilier, consacré à l'éducation et à la littératie médiatique, constitue le socle de l'ensemble. Le WEF (2026, p. 39) identifie en effet la sensibilisation et l'éducation publiques comme l'approche de gouvernance la plus pertinente pour atténuer les effets de la polarisation sociétale et de la désinformation. Le deuxième pilier vise à renforcer l'écosystème médiatique en soutenant le journalisme professionnel, le fact-checking et les mécanismes de qualité informationnelle. Le troisième pilier porte sur l'adaptation du cadre juridique et institutionnel, dans une logique d'équilibre entre lutte contre la désinformation et protection de la liberté d'expression. Le quatrième pilier concerne le développement de capacités technologiques nationales, notamment pour la veille automatisée, la détection des deepfakes et la vérification multilingue. Enfin, le cinquième pilier souligne la nécessité d'une coopération internationale et régionale, indispensable dans un environnement informationnel transfrontalier.

Ce cadre vise ainsi à faire passer l'Algérie d'une posture de réaction fragmentée à une posture de résilience informationnelle structurée, capable d'anticiper les menaces, de limiter leurs effets et de préserver durablement la confiance sociale et institutionnelle.

6. Discussion:

6.1. Un risque systémique sous-estimé en Algérie:

L'analyse présentée dans cet article révèle un paradoxe préoccupant. Alors que le WEF classe la désinformation comme le 2e risque mondial le plus sévère à court terme, les dirigeants d'entreprise algériens interrogés dans l'EOS ne l'identifient pas parmi leurs cinq premières préoccupations nationales (WEF, 2026, p. 82). Ce décalage perceptuel a été théorisé par Slovic (2000) dans sa recherche sur la perception des risques : les individus et les organisations tendent à sous-estimer les menaces intangibles (comme la désinformation) au profit de risques perçus comme plus concrets et immédiats (comme l'inflation ou le chômage).

Or, la protection de l'information constitue un axe majeur de la sécurité économique, ce qui signifie que la désinformation devrait être appréhendée comme un risque économique et sécuritaire de premier ordre, et non comme un phénomène secondaire.

6.2. L'effet multiplicateur de l'IA:

Le WEF souligne que l'IA générative amplifie considérablement le risque de désinformation. Les effets négatifs de l'IA enregistrent la progression la plus forte parmi l'ensemble des 33 risques évalués, passant du 30e rang à court terme au 5e rang à long terme (WEF, 2026, p. 9). Chio et Freeman (2018) ont documenté comment le machine learning est de plus en plus utilisé pour automatiser les cyberattaques, une dynamique transposable aux campagnes de désinformation. Goldstein et al. (2023) confirment que les grands modèles de langage (LLMs — Large Language Models) réduisent considérablement le coût et le temps nécessaires pour produire de la propagande ciblée, permettant à des acteurs disposant de faibles ressources de mener des campagnes de désinformation à grande échelle.

Pour l'Algérie, cette convergence IA-désinformation est particulièrement préoccupante. La production de deepfakes en langue arabe devient de plus en plus accessible, alors que les capacités de détection et de vérification demeurent limitées en arabe et totalement absentes en amazighe et en darija. L'Algérie pourrait devenir un "importateur net" de désinformation générée par l'IA sans disposer des outils technologiques et humains pour y répondre.

6.3. L'interconnexion désinformation-polarisation : un avertissement pour l'Algérie:

Le WEF identifie l'interconnexion entre désinformation et polarisation sociétale comme l'une des plus fortes de l'ensemble du GRPS (WEF, 2026, p. 33). Le rapport note que "la dépendance croissante à la fois aux réseaux sociaux et aux outils d'IA renforce l'impact des biais algorithmiques, qui façonnent l'information que les utilisateurs voient en ligne et renforcent l'exposition des individus à des informations alignées sur leurs opinions" (WEF, 2026, p. 36).

Pour l'Algérie, où des lignes de fracture existent déjà entre générations et entre visions de la société, la désinformation risque de transformer des tensions latentes en conflits ouverts. Tucker et al. (2018), dans leur revue de littérature commandée par la Hewlett Foundation, identifient plusieurs mécanismes par lesquels les réseaux sociaux peuvent contribuer à la polarisation politique, notamment l'exposition à des contenus hyperpartisans, la formation de chambres d'écho et l'amplification de la polarisation affective. Les auteurs soulignent toutefois que la relation causale reste débattue dans la littérature scientifique.

Le rapport note également que "l'exposition à des niveaux élevés de contenu violent est liée à une désensibilisation émotionnelle" (WEF, 2026, p. 36). Dans le contexte algérien, où 77% de la population est connectée à Internet et où les réseaux sociaux constituent une source d'information majeure, cette dynamique pourrait à terme éroder la capacité de la société à répondre collectivement aux crises.

6.4. La nécessité d'une approche intégrée:

Le défi de la désinformation ne peut être relevé par une approche sectorielle ou uniquement technologique. L'approche sociotechnique, telle que définie par Bostrom et Heinen (1977) et appliquée à la cybersécurité par Sadok et al. (2020), souligne l'interdépendance complexe entre les systèmes techniques et les dimensions humaines et organisationnelles. Appliquée au domaine de la désinformation, cette perspective montre que la résistance aux campagnes de manipulation informationnelle nécessite une action simultanée sur les technologies de détection, les comportements des utilisateurs, les structures organisationnelles des médias et les cadres institutionnels de régulation.

6.5. Le défi de l'état de droit:

Le WEF documente ce qu'il qualifie d'accélération d'une "récession mondiale de l'état de droit", dans laquelle 68% des 143 pays et juridictions évalués ont vu leur état de droit se détériorer en 2025 (WEF, 2026, p. 30). La construction d'un cadre juridique et institutionnel efficace contre la désinformation, qui protège simultanément la liberté d'expression, représente un défi d'équilibre particulièrement délicat. Comme le soulignent Clough (2014) et Wang (2016), l'harmonisation des législations nationales avec les standards internationaux en matière de cybercriminalité reste un défi majeur, amplifié par les différences culturelles et juridiques entre les systèmes.

7. Recommandations et feuille de route stratégique:

Le diagnostic conduit dans les sections précédentes — analyse du WEF (section 3), cartographie des vulnérabilités algériennes (section 4) et cadre conceptuel des cinq piliers (section 5) — permet de formuler sept recommandations opérationnelles, hiérarchisées selon trois niveaux de priorité : urgente, haute et moyenne.

Recommandation 1 (urgente) — Pilier 1 (Éducation) : Lancer une campagne nationale de littératie médiatique à double volet. Cette urgence se justifie par la convergence de plusieurs constats issus du diagnostic. D'une part, les moins de 30 ans — qui représentent 54% de la population algérienne (tableau 7) — constituent la population la plus massivement exposée à la désinformation en raison de leur consommation intensive des réseaux sociaux : bien qu'ils soient les plus conscients du risque, le classant au 1er rang mondial (tableau 2), cette conscience ne se traduit pas en capacité effective de résistance, comme le confirme l'Eurobarometer Youth Survey 2024 selon lequel 76% des jeunes européens de 16 à 30 ans estiment avoir été exposés à de fausses informations au cours de la semaine précédant l'enquête (European Parliament, 2025). Ce volet devrait donc être axé sur les compétences pratiques de vérification et d'analyse critique des contenus. D'autre part, les tranches d'âge supérieures, qui classent la désinformation relativement plus bas dans leur hiérarchie des risques (tableau 2), présentent un déficit de conscience de la menace qui les rend vulnérables lorsqu'elles y sont confrontées, ce qui appelle un volet spécifique de sensibilisation. Ce double ciblage s'impose d'autant plus que la littératie médiatique constitue la seule vulnérabilité de niveau "critique" dans notre matrice (tableau 8) — un diagnostic qui converge avec la position du WEF, identifiant l'éducation publique comme l'approche n°1 d'atténuation (WEF, 2026, p. 39).

Recommandation 2 (urgente) — Pilier 4 (Technologie) : Créer une cellule de veille et de réponse à la désinformation rattachée à l'ASSI. L'absence de la désinformation dans le top 5 algérien de l'EOS (tableau 5) traduit un biais perceptuel documenté par Schneier (2008) et Slovic (2000), que seul un dispositif institutionnel dédié peut contribuer à corriger. Cette cellule s'inscrirait dans le prolongement de la stratégie nationale de sécurité des systèmes d'information 2025-2029 (ASSI, 2026).

Recommandation 3 (haute) — Pilier 2 (Médias) : Développer un écosystème de fact-checking multilingue. Cette recommandation répond au constat que 93% des utilisateurs algériens de réseaux sociaux ont été exposés à de fausses informations (BBC Media Action, 2021), dans un contexte de faible modération en langues arabe et amazighe et en dialectes locaux (Shahid et al., 2025). Elle revêt une dimension de souveraineté linguistique informationnelle : la langue amazighe et la darija constituent aujourd'hui des angles morts quasi totaux des dispositifs de modération et de vérification des grandes plateformes numériques. La désinformation qui circule dans ces langues échappe donc à tout mécanisme de détection automatisée, ce qui en fait un vecteur privilégié de manipulation ciblant précisément les populations les moins outillées pour s'en défendre. Le développement de corpus linguistiques, d'outils de traitement du langage naturel (NLP — Natural Language Processing) et de plateformes de fact-checking en arabe, en amazighe et en darija constitue par conséquent une condition préalable à toute stratégie crédible de résilience informationnelle en Algérie.

Recommandation 4 (haute) — Pilier 3 (Cadre juridique et institutionnel) : Élaborer un cadre réglementaire équilibré incluant une obligation de transparence algorithmique. L'absence de loi autonome sur la désinformation en ligne constitue une vulnérabilité de niveau "élevé" (tableau 8). Le WEF souligne que l'adoption de solutions d'authentification des contenus nécessite des cadres politiques alignés sur des normes technologiques partagées (WEF, 2026, section 2.3).

Recommandation 5 (haute) — Pilier 4 (Technologie) : Investir dans la détection des deepfakes et adopter les standards C2PA/watermarking. Cette recommandation s'impose face à la réduction considérable du coût de production de la propagande ciblée permise par les LLMs (Goldstein et al., 2023). Cet investissement doit impérativement couvrir, au-delà de l'arabe, la langue amazighe et le darija, pour lesquelles les capacités de détection des contenus synthétiques sont actuellement inexistantes, créant une asymétrie exploitable par les acteurs malveillants.

Recommandation 6 (haute) — Transversal : Adopter une approche de cyberrésilience informationnelle intégrée. Cette recommandation traduit le constat central de cet article : la désinformation fonctionne comme un "nœud à influence élevée" (WEF, 2026, p. 11) qui exige une réponse systémique articulant l'ensemble des cinq piliers du modèle proposé (section 5.2).

Recommandation 7 (moyenne) — Pilier 5 (Coopération internationale) : Intégrer l'Algérie dans les réseaux internationaux de lutte contre la désinformation. Le caractère transfrontalier de la menace (section 3.2) rend cette coopération indispensable, mais sa mise en œuvre dépend en partie de la consolidation préalable des capacités nationales.

Le tableau 10 ci-dessous décline l'ensemble de ces recommandations en actions concrètes, indicateurs de succès et acteurs institutionnels, sur trois horizons temporels.

Tableau 10 : Feuille de route stratégique pour la résilience informationnelle de l'Algérie

Horizon	Pilier	Actions prioritaires	Indicateurs de succès	Acteurs clés
Court terme (0-12 mois)	Éducation (R1) Volet jeunes (< 30 ans)	Programme de compétences pratiques en vérification et analyse critique des contenus numériques ; outils de signalement en arabe, en amazighe et en darija ; modules de formation dans les lycées et universités	> 3 millions de jeunes touchés (portée combinée TV/réseaux sociaux); 10000 enseignants du secondaire formés	MEN, MESRS, MPTIC, Société civile
Court terme (0-12 mois)	Éducation (R1) Volets adultes (≥ 30 ans)	Campagne nationale de sensibilisation au risque de désinformation ciblant les tranches d'âge supérieures ; ateliers communautaires ; capsules télévisées et radiophoniques	> 2 millions d'adultes touchés ; couverture de l'ensemble des 58 wilayas	MEN, MPTIC, Médias publics, Société civile
Court terme (0-12 mois)	Technologie (R2)	Cellule de veille informationnelle rattachée à	Cellule opérationnelle ;	ASSI, MPTIC, Universités

Désinformation et résilience informationnelle en Algérie : diagnostic des vulnérabilités
et cadre stratégique à la lumière du Global Risks Report 2026

		l'ASSI ; projet pilote de fact-checking multilingue (arabe, amazighe, darija)	premier rapport de veille publié	
Court terme (0-12 mois)	Médias (R3)	Fonds de soutien au journalisme d'investigation et au fact-checking ; label de qualité informationnelle	> 20 médias labellisés ; doublement du nombre d'articles de fact-checking par rapport à 2025	ARAV, Syndicats de presse, Partenaires internationaux
Court terme (0-12 mois)	Coopération (R7)	Adhésion au réseau IFCN ; partenariat technique avec l'UNESCO	Au moins 2 accords de coopération signés	MAE, MPTIC, UNESCO
Moyen terme (1-3 ans)	Cadre juridique et institutionnel (R4)	Loi-cadre sur l'intégrité informationnelle ; obligation de transparence algorithmique pour les plateformes	Loi adoptée ; premier rapport de conformité des plateformes	Parlement, Ministère de la justice, ARPCE
Moyen terme (1-3 ans)	Technologie (R5)	Développement d'outils de détection de deepfakes adaptés à l'arabe, à l'amazighe et au darija ; adoption de standards C2PA/watermarking, en cohérence avec la SNSSI 2025-2029	Au moins 2 outils opérationnels ; intégration dans la stratégie ASSI	ASSI, MPTIC, Universités, Startups
Moyen terme (1-3 ans)	Médias + Technologie (R3/R5)	Développement de corpus linguistiques et d'outils NLP pour l'amazighe et la darija ; création d'une plateforme de fact-checking dédiée aux langues algériennes ; partenariat avec les départements universitaires de linguistique et d'informatique	Au moins 1 corpus ouvert publié par langue ; 1 plateforme de fact-checking opérationnelle en arabe, en amazighe et en darija	MESRS, MPTIC, HCA, Universités, Startups
Long terme (3-5 ans)	Éducation (R1)	Intégration de l'EMI dans les curricula du primaire au supérieur ; création d'un master spécialisé en intégrité informationnelle	EMI dans les programmes nationaux ; premier master diplômant	MEN, MESRS, UNESCO
Long terme (3-5 ans)	Coopération (R7)	Co-développement d'outils de détection avec l'UE et l'UA ; participation active aux plateformes internationales	> 5 accords signés ; participation à au moins 3 plateformes internationales	MAE, MPTIC, Organisations régionales

Liste des abréviations :

MPTIC — Ministère de la Poste et des Télécommunications

MAE — Ministère des Affaires étrangères et de la Communauté nationale à l'étranger

MESRS — Ministère de l'Enseignement supérieur et de la Recherche scientifique

MEN — Ministère de l'Éducation nationale

HCA — Haut Commissariat à l'Amazighité

ASSI — Agence de la Sécurité des Systèmes d'Information

ARPCE — Autorité de Régulation de la Poste et des Communications Électroniques

ARAV — Autorité de Régulation de l'Audiovisuel

IFCN — International Fact-Checking Network

C2PA — Coalition for Content Provenance and Authenticity

EMI — Éducation aux médias et à l'information

SNSSI — Stratégie Nationale de Sécurité des Systèmes d'Information

Source : Élaboration de l'auteur à partir de WEF (2026) ; UNESCO (2020) ; SNSSI 2025-2029

8. Conclusion:

Cet article a analysé le risque de désinformation tel que caractérisé par le WEF 2026 — classé au 2^e rang mondial à court terme et au 4^e rang à long terme — en évaluant ses implications spécifiques pour l'Algérie. En croisant les données du GRPS 2025-2026 et de l'EOS 2025 avec les indicateurs de l'écosystème informationnel algérien, notre analyse a mis en évidence un paradoxe stratégique préoccupant : alors que la désinformation constitue une menace systémique de premier ordre à l'échelle mondiale, elle demeure absente du top 5 des risques perçus par les décideurs économiques algériens, révélant un biais perceptuel qui fragilise la posture nationale face à cette menace.

Le diagnostic multidimensionnel a permis d'identifier quatre catégories de vulnérabilités, parmi lesquelles la littératie médiatique et numérique constitue la seule vulnérabilité de niveau critique. Ce constat converge avec les conclusions du WEF, qui place l'éducation et la sensibilisation publiques au premier rang des mesures d'atténuation. Les trois autres vulnérabilités — fragilité de l'écosystème médiatique, limites du cadre normatif et faibles capacités de détection des contenus synthétiques — voient leur impact démultiplié par cette carence structurelle en compétences informationnelles. À cela s'ajoute une vulnérabilité spécifique mise en évidence par notre analyse : l'absence quasi totale d'outils de modération, de détection et de vérification adaptés à la langue amazighe et au darija, qui constitue un angle mort stratégique exploitable par les acteurs de désinformation.

L'analyse des interconnexions systémiques a confirmé le rôle de la désinformation comme "nœud à influence élevée", fonctionnant en boucle de rétroaction avec la polarisation sociétale et alimentant un cercle vicieux menant aux inégalités, à la violence intra-étatique et à l'érosion des libertés civiques. Dans un pays où 77% de la population est connectée à Internet et où 93% des utilisateurs de réseaux sociaux déclarent avoir été exposés à de fausses informations, cette dynamique revêt une acuité particulière. L'effet multiplicateur de l'IA, dont les résultats négatifs enregistrent la progression la plus forte parmi les 33 risques évalués par le WEF — passant du 30^e rang à court terme au 5^e rang à long terme — amplifie encore cette menace en réduisant considérablement le coût et le temps nécessaires à la production de propagande ciblée.

Face à ces constats, nous avons proposé un cadre stratégique de résilience informationnelle articulé autour de cinq piliers complémentaires — éducation, médias, cadre juridique et institutionnel, technologie et coopération internationale (section 5) — dont la déclinaison opérationnelle a été détaillée sous la forme de sept recommandations hiérarchisées et d'une feuille de route sur trois horizons temporels (section 7). Ce cadre s'inscrit dans une logique de cyberrésilience dynamique, dépassant les approches sectorielles et statiques pour embrasser une vision systémique et adaptative, en cohérence avec la stratégie nationale de sécurité des systèmes d'information 2025-2029. L'originalité de cette approche réside dans l'articulation entre, d'une part, le changement de paradigme de la cybersécurité classique vers la cyberrésilience informationnelle (section 5.1) et, d'autre part, l'intégration de la dimension de souveraineté linguistique informationnelle — notamment pour l'arabe, l'amazighe et la darija — comme condition préalable à toute stratégie crédible de résilience.

Il convient toutefois de souligner que notre analyse repose principalement sur des données secondaires. Des recherches futures, fondées sur des enquêtes de terrain, permettraient de mesurer le niveau de littératie médiatique selon les tranches d'âge et les régions linguistiques, d'évaluer l'efficacité des dispositifs réglementaires existants et de tester empiriquement le cadre stratégique proposé.

En définitive, La désinformation tend aujourd'hui à dépasser le statut de simple risque périphérique pour s'imposer comme un véritable levier stratégique au cœur de la guerre de quatrième génération. Pour l'Algérie, construire une résilience informationnelle durable n'est pas un choix, mais un impératif de souveraineté. Le passage d'une posture réactive et fragmentée à une posture de résilience structurée et anticipative déterminera la capacité du pays à préserver sa cohésion sociale, sa confiance institutionnelle et son espace informationnel souverain face aux défis de la décennie à venir.

Références bibliographiques

1. Agence de la sécurité des systèmes d'information [ASSI]. (2026). Stratégie nationale de la sécurité des systèmes d'information. https://www.mdn.dz/assi/nsiss_fr.pdf
2. Banque mondiale. (2018). Literacy rate, adult total (% of people ages 15 and above) — Algeria [Jeu de données]. <https://data.worldbank.org/indicator/SE.ADT.LITR.ZS?locations=DZ>
3. Batista Cabanas, L. (2025, 19 février). Young Europeans face rising threat from misinformation as social media becomes main news source. Euronews. <https://www.euronews.com/my-europe/2025/02/19/young-europeans-face-rising-threat-from-misinformation-as-social-media-becomes-main-news-s>
4. BBC Media Action. (2021, juillet). Understanding Algerian social media users' experiences of false and misleading information. <https://www.bbc.co.uk/mediaaction/publications-and-resources/research/summaries/social-media-algeria-july2021>
5. Benkler, Y., Faris, R., et Roberts, H. (2018). Network propaganda: Manipulation, disinformation, and radicalization in American politics. Oxford University Press. <https://pdfcoffee.com/download/benkler-yochai-faris-robert-roberts-hal-network-propaganda-manipulation-disinformation-and-radicalization-in-american-politics-2018-oxford-university-press-pdf-free.html>
6. Bostrom, R. P. et Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective. Part I: The Causes. MIS Quarterly, 1(3), 17–32. <https://www.jstor.org/stable/248710>
7. Bradshaw, S., et Howard, P. N. (2019). The global disinformation order: 2019 global inventory of organised social media manipulation (Working Paper 2019.3). Oxford Internet Institute. <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf>
8. Chesney, R., et Citron, D. K. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. California Law Review, 107(6), 1753-1820. <https://doi.org/10.2139/ssrn.3213954>
9. Chio, C., et Freeman, D. (2018). Machine learning and security: Protecting systems with data and algorithms. O'Reilly Media.
10. Clough, J. (2014). A World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation. Monash University Law Review, 40(3), 698–736.
11. Conti, M., Dehghantanha, A., Franke, K., et Watson, S. (2018). Internet of Things security and forensics: Challenges and opportunities. Future Generation Computer Systems, 78(2), 544-550. <https://arxiv.org/pdf/1807.10438>
12. Dennehy, F. (2024, 2 juillet). 9 in 10 concerned about deepfakes affecting election results. The Alan Turing Institute. <https://www.turing.ac.uk/news/9-10-concerned-about-deepfakes-affecting-election-results>
13. Dou, A. (2023). A factual content analysis of Facebook infodemic in Algeria. International Journal of Media and Information Literacy, 8(2), 305–314. <https://doi.org/10.13187/ijmil.2023.2.305>
14. European Parliament. (2025). Youth survey 2024 (Flash Eurobarometer FL013EP). Directorate-General for Communication, Youth Outreach Unit. <https://europa.eu/eurobarometer/surveys/detail/3392>
15. Fonds des Nations Unies pour la population. (2022). Évaluation finale du 6ème Programme UNFPA-Algérie 2017-2021 : Annexes. UNFPA. [https://www.unfpa.org/sites/default/files/2022-11/CPE Algerie Annexes 0.pdf](https://www.unfpa.org/sites/default/files/2022-11/CPE%20Algerie%20Annexes%200.pdf)

16. Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., et Sedova, K. (2023). Generative language models and automated influence operations: Emerging threats and potential mitigations. arXiv preprint. <https://doi.org/10.48550/arXiv.2301.04246>
17. Gursky, J., Riedl, M. J., et Woolley, S. (2021, 19 mars). The disinformation threat to diaspora communities in encrypted chat apps. Brookings TechStream. <https://www.brookings.edu/articles/the-disinformation-threat-to-diaspora-communities-in-encrypted-chat-apps/>
18. Hadid, N. (2021a, 6-7 mars). La guerre de quatrième génération et ses conséquences sur la sécurité et la stabilité des États [Communication]. Journées d'études "Guerre de l'information". Institut National d'Études de Stratégie Globale (INESG), Alger.
19. Hadid, N. (2021b, 9 février). La cybercriminalité : ses causes et ses motivations [Communication]. Journée parlementaire sur la cybercriminalité et la sécurité de l'État. Commission de la Défense nationale, Assemblée Populaire Nationale, Alger.
20. Hadid, N. (2022, 24 juillet). La cyberrésilience : une nécessité vitale pour les entreprises et les institutions étatiques [Communication]. Journée d'étude sur la cybersécurité. Institut National d'Études de Stratégie Globale (INESG), Alger.
21. Hadid, N. (2024a). Cybercriminalité et espionnage industriel : enjeux stratégiques et réponses intégrées pour la sécurité des entreprises et des États. Revue algérienne des études de sécurité nationale (AJNASS), 137-159.
22. Hadid, N. (2024b, 29 février). Intelligence artificielle, désinformation et démocratie [Communication]. Journée d'étude "L'intelligence artificielle et son impact sur la démocratie". Faculté des Sciences Politiques et des Relations Internationales / Laboratoire politique de défense, Université d'Alger 3, Algérie.
23. Ireton, C., et Posetti, J. (Eds.). (2018). Journalism, 'fake news' et désinformation: Handbook for journalism education and training. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000265552>
24. Kemp, S. (2024, 23 février). Digital 2024: Algeria. DataReportal. <https://datareportal.com/reports/digital-2024-algeria>
25. Kemp, S. (2025, 3 mars). Digital 2025: Algeria. DataReportal. <https://datareportal.com/reports/digital-2025-algeria>
26. Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. Journal of Global Information Technology Management, 22(2), 77-81. <https://doi.org/10.1080/1097198X.2019.1603527>
27. Lind, W. S., Nightengale, K., Schmitt, J. F., Sutton, J. W., et Wilson, G. I. (1989). The changing face of war: Into the fourth generation. Marine Corps Gazette, 73(10), 22-26. https://d-n-i.net/FCS_Folder/4th_gen_war_gazette.htm
28. Loi n° 20-06 du 28 avril 2020 modifiant et complétant le code pénal. JORADP, n° 25, 10-12. <https://www.joradp.dz/FTP/jo-francais/2020/F2020025.pdf>
29. Mauslein, J. A., et Pickering, J. (2021). Rivalry type and cyber operations: "Hot" rivalries, "cold" rivalries, and cyber incidents, 1990–2009. Peace Economics, Peace Science and Public Policy, 27(2), 169–195. <https://doi.org/10.1515/peps-2020-0046>
30. Newman, N., Arguedas, A. R., Robertson, C. T., Nielsen, R. K., et Fletcher, R. (2025). Reuters Institute Digital News Report 2025. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-06/Digital_News-Report_2025.pdf
31. Newman, N., Fletcher, R., Kalogeropoulos, A., Levy, D. A. L., & Nielsen, R. K. (2018). Reuters Institute Digital News Report 2018. Reuters Institute for the Study of

- Journalism, University of Oxford. <https://ora.ox.ac.uk/objects/uuid:6a97a7c6-31fb-48e6-8915-f1cdc3e12c08>
32. NIST. (2024). The NIST Cybersecurity Framework (CSF) 2.0. <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>
33. Office National des Statistiques [ONS]. (2019). Démographie algérienne 2018 (Données Statistiques n° 853). <https://www.ons.dz/IMG/pdf/demographie2018.pdf>
34. Paris, B., et Donovan, J. (2019). Deepfakes and cheap fakes: The manipulation of audio and visual evidence. Data et Society Research Institute. <https://datasociety.net/library/deepfakes-and-cheap-fakes/>
35. Peace Research Institute Oslo [PRIO]. (2025, 9 juin). New data shows conflict at historic high. <https://www.prio.org/news/3616>
36. Posetti, J., et Bontcheva, K. (2020). Balancing act: Countering digital disinformation while respecting freedom of expression. UNESCO. <https://unesdoc.unesco.org/ark:/48223/pf0000379015>
37. Sadok, M., Alter, S. et Bednar, P. (2020). It is not my job: Exploring the disconnect between corporate security policies and actual security practices in SMEs. Information and Computer Security, 28(3), 467–483. <https://doi.org/10.1108/ICS-01-2019-0010>
38. Schneier, B. (2008, January 18). The psychology of security. Schneier on Security. https://www.schneier.com/essays/archives/2008/01/the_psychology_of_se.html
39. Schneier, B. (2018). Click Here to Kill Everybody: Security and Survival in a Hyper-Connected World. New York : W. W. Norton et Company.
40. Schwab, K. (2016). The Fourth Industrial Revolution. World Economic Forum. https://law.unimelb.edu.au/_data/assets/pdf_file/0005/3385454/Schwab-The_Fourth_Industrial_Revolution_Klaus_S.pdf
41. Shahid, F., Elswah, M., et Vashistha, A. (2025). Think outside the data: Colonial biases and systemic issues in automated moderation pipelines for low-resource languages. <https://ojs.aaai.org/index.php/AIES/article/download/36719/38857/40794>
42. Simon, F., Nielsen, R. K., et Fletcher, R. (2025, 7 octobre). Generative AI and news report 2025. Reuters Institute for the Study of Journalism. <https://reutersinstitute.politics.ox.ac.uk/generative-ai-and-news-report-2025-how-people-think-about-ais-role-journalism-and-society>
43. Slovic, P. (2000). The perception of risk. Earthscan Publications. <https://www.taylorfrancis.com/books/edit/10.4324/9781315661773/perception-risk-paul-slovic>
44. Sunstein, C. R. (2017). #Republic: Divided democracy in the age of social media. Princeton University Press. <https://doi.org/10.1515/9781400884711>
45. Tucker, J. A., Guess, A., Barberá, P., Vaccari, C., Siegel, A., Sanovich, S., Stukal, D., et Nyhan, B. (2018). Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature. Hewlett Foundation. <https://doi.org/10.2139/ssrn.3144139>
46. UNESCO. (2020, 28 octobre). Media and information literacy is first line of defence against disinformation. <https://www.unesco.org/en/articles/media-and-information-literacy-first-line-defence-against-disinformation>
47. UNESCO. (2023). Media and information literacy: A practical guidebook for trainers. <https://unesdoc.unesco.org/ark:/48223/pf0000384922>
48. Vosoughi, S., Roy, D., et Aral, S. (2018). The spread of true and false news online. Science, 359(6380), 1146-1151. https://www.science.org/doi/suppl/10.1126/science.aap9559/suppl_file/aap9559_vosoughi_sm.pdf

49. Wang, Q. (2016). A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe. Doctoral Thesis, Erasmus University Rotterdam. <https://repub.eur.nl/pub/94604/PROOF-Qianyun-Wang-BW-1-.pdf>
50. Wardle, C., et Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policy making (Rapport DGI(2017)09). Conseil de l'Europe. <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>
51. Woolley, S. C., et Howard, P. N. (Eds.). (2019). Computational propaganda: Political parties, politicians, and political manipulation on social media. Oxford University Press. <https://doi.org/10.1093/oso/9780190931407.001.0001>
52. World Economic Forum [WEF]. (2023). The Global Risks Report 2023 (18th ed.). https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf
53. World Economic Forum [WEF]. (2024). The Global Risks Report 2024 (19th ed.). https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf
54. World Economic Forum [WEF]. (2025). The Global Risks Report 2025 (20th ed.). https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf
55. World Economic Forum [WEF]. (2026). The Global Risks Report 2026 (21st ed.). https://reports.weforum.org/docs/WEF_Global_Risks_Report_2026.pdf
56. World Justice Project. (2025). WJP Rule of Law Index® 2025. Washington, DC: World Justice Project. <https://worldjusticeproject.org/rule-of-law-index/downloads/WJPIndex2025.pdf>