

L'impact économique mondial de la désinformation

Coûts financiers, sociaux et politiques :
comment les manipulations de l'information
dégradent l'économie

Rapport - mars 2026

L'impact économique mondial de la désinformation

Coûts financiers, sociaux et politiques :
comment les manipulations de l'information dégradent l'économie

ABSTRACT

Cette étude est née d'un paradoxe : chacun évoque la désinformation, mais personne ne sait vraiment combien elle coûte à nos entreprises, nos économies et nos démocraties.

Début 2024, le Forum économique mondial¹ classait le phénomène comme « risque majeur mondial » pour la deuxième année consécutive. En septembre 2025, le prix Nobel d'économie Philippe Aghion et dix économistes alertaient dans *Le Monde*² sur les dangers de la désinformation économique pour « la prospérité économique et le progrès humain ». Pourtant, aucune quantification rigoureuse de son coût économique n'a été réalisée depuis 2019³.

Notre travail comble ce vide en proposant la première estimation globale actualisée pour une année de référence : 2024. Trois ruptures majeures depuis 2019 justifient cette mise à jour : la pandémie de COVID-19 et son « infodémie », l'industrialisation de la désinformation par les outils d'intelligence artificielle (IA) générative et l'intensification de la guerre hybride.

Notre méthodologie s'inspire du GIEC avec trois scénarios – conservateur, médian, exploratoire – et décompose les coûts en trois verticales : financiers, sociaux et politiques. Les coûts **financiers** couvrent les fraudes, les arnaques et les manipulations de marchés. Nous entendons par coûts **sociaux** ceux qui englobent l'érosion de la confiance institutionnelle, la fragmentation du tissu social et les effets sur la santé. Les coûts **politiques** regroupent les

dépenses liées à l'atteinte à l'intégrité des processus démocratiques, aux opérations d'influence étrangère et aux ripostes mobilisées pour y faire face par les acteurs publics et privés (détection, modération, fact-checking, contre-opérations, etc.).

Sous l'impulsion d'un comité scientifique regroupant des experts multisectoriels, cette étude établit un protocole reproductible annuellement afin de quantifier le plus précisément possible le coût de la désinformation. Il s'agit d'un premier jalon que nous posons. Il s'établit sur la base de la transparence et d'une méthodologie ouverte, avec pour objectif d'affiner nos estimations d'année en année. Parce que prendre la mesure de l'adversaire est le premier pas vers une approche efficace et écosystémique de la riposte.

¹ *Global Risk Report 2024*, World Economic Forum, 2024

² *La crise mondiale de l'information représente une grave menace pour la prospérité économique et le progrès humain*, *Le Monde*, 2025

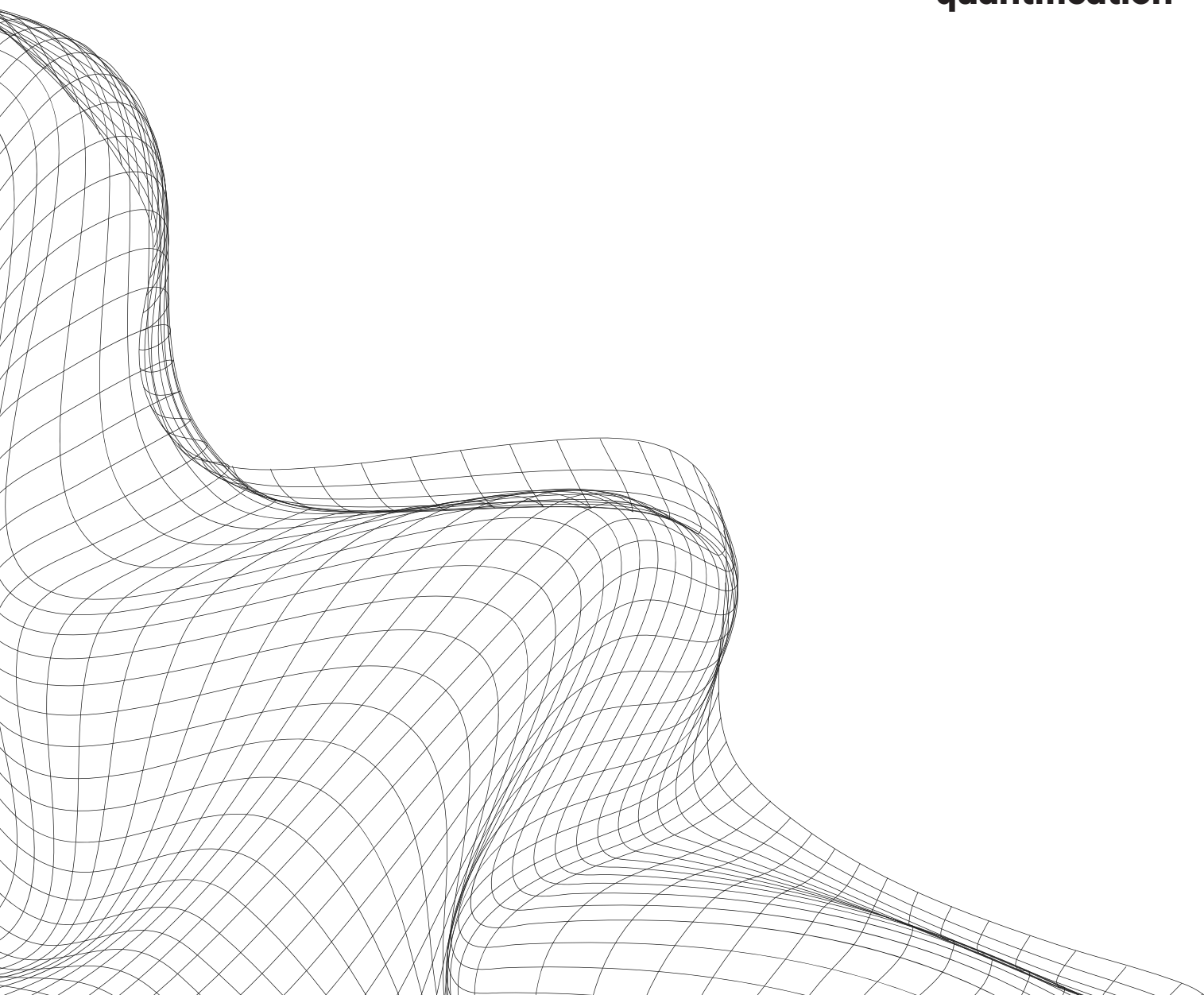
³ *The economic cost of bad actors on the Internet, Fake News*, CHEQ, 2019

ABSTRACT	3	3.3.1 Coûts de santé	14
1. INTRODUCTION - UNE ESSENTIELLE ET INÉDITE QUANTIFICATION	5	3.3.2 Coûts sociaux	14
1.1 Clarifier les termes : au-delà de la désinformation	6	3.3.3 Coût de la défiance	14
1.2 Notre périmètre : les manipulations informationnelles intentionnelles	6	3.3.4 Modélisation des coûts systémiques	15
1.3 Un paysage transformé : les ruptures de 2020-2024	6	3.4 Coûts politiques et de riposte	15
1.4 Le paradoxe : reconnaissance universelle, invisibilité économique	7	3.4.1 Dépenses publiques et privées de lutte contre la désinformation	15
2. CARTOGRAPHIER LE TERRAIN : CE QUE L'ON SAIT (ET CE QUE L'ON IGNORE) DU COÛT DE LA DÉSINFORMATION	8	3.4.2 Distinction FIMI/DIMI et périmètre d'analyse	15
2.1 Études englobantes de référence	9	3.4.3 Le marché de la « Confiance Numérique » (<i>Digital Trust</i>) : un indicateur	15
2.2 Impact sur les marchés financiers et la confiance	9	3.4.4 Estimation de la part « anti-désinformation »	15
2.3 Polarisation sociale et coûts politiques	9	3.4.5 Répartition public-privé	16
2.4 Technologies émergentes : le défi des <i>deepfakes</i>	9	3.4.6 Coût de la mobilisation des ressources humaines	16
2.5 Lacunes identifiées et positionnement de notre étude	9	4. LES CHIFFRES	17
3. ÉVALUER LE COÛT DE LA DÉSINFORMATION : UN DÉFI MÉTHODOLOGIQUE	11	4.1. Coûts financiers directs : l'hémorragie économique mesurable	18
3.1 Cadre méthodologique général	12	4.1.1 Scénario 1 (conservateur) : 353 milliards de dollars	18
3.1.1 Architecture des scénarios	12	4.1.2 Scénario 2 (médian) : 393,1 milliards de dollars	18
3.1.2 Hypothèse de non-interaction entre verticales	12	4.1.3 Scénario 3 (exploratoire) : 456,3 milliards de dollars ...	19
3.1.3 Modélisation des interactions de second ordre	12	4.2. Coûts sociaux : l'impact sur la santé et la cohésion sociale	19
3.1.4 Utilisation de la valeur de Shapley pour l'agrégation ...	12	4.2.1 Scénario 1 (conservateur) : 37 millions de dollars	19
3.1.5 Intégration de l'expertise	12	4.2.2 Scénario 2 (médian) : 9,8 milliards de dollars	19
3.1.6 Ajustements temporels et géographiques	13	4.2.3 Scénario 3 (exploratoire) : 19,9 milliards de dollars	20
3.1.7 Traitement des recouvrements sectoriels : monitoring et riposte du secteur privé	13	4.3. Coûts politiques et de riposte	20
3.2 Coûts financiers : traitement de la variabilité des marchés	13	4.3.1 Scénario 1 (conservateur) : 2,1 milliards de dollars	20
3.2.1 Modélisation des krachs : approche indicative	14	4.3.2 Scénario 2 (médian) : 14,22 milliards de dollars	20
3.3 Coûts de santé, sociaux et de la confiance	14	4.3.3 Scénario 3 (exploratoire) : 40,1 milliards de dollars	20
		4.4. Synthèse des trois domaines	21
		4.5. Les limitations	21
		5. CONCLUSION & ANNEXES	23
		5.1. Conclusion	24
		5.2. Sources, références et experts	25

1.

Introduction

**Une essentielle et inédite
quantification**



En 2025, pour la seconde année consécutive, le Forum économique mondial a classé la désinformation parmi les risques majeurs pour nos sociétés⁴, devant les catastrophes climatiques, les conflits armés ou la cybersécurité. 2024, c'est aussi l'année où près de 4 milliards de personnes se sont rendues aux urnes dans un contexte où la manipulation informationnelle menace l'intégrité même des processus démocratiques.

Malgré cette reconnaissance de la menace, le coût économique réel de la désinformation demeure pourtant largement invisible, relégué au rang des externalités négatives qu'aucun système comptable ne capture vraiment.

1.1 Clarifier les termes : au-delà de la désinformation

Le terme *fake news*, pensé pour qualifier la production des acteurs de la désinformation, est devenu au fil des années un outil de discrédit aux mains de certains acteurs politiques. Pour éviter cette confusion sémantique, la recherche académique s'est structurée autour d'une typologie plus rigoureuse, proposée en 2017 par Claire Wardle et Hossein Derakhshan dans leur rapport pour le Conseil de l'Europe⁵.

La **désinformation** désigne un contenu intentionnellement faux, conçu pour causer un préjudice. Elle est motivée par trois facteurs principaux : le profit économique, l'influence politique (qu'elle soit d'origine étrangère ou domestique), ou simplement la volonté de semer le chaos. La **mésinformation**, en revanche, désigne une information fausse ou trompeuse partagée sans intention de nuire, souvent par des individus qui pensent sincèrement être utiles en la diffusant. Enfin, la **malinformation** concerne des informations véridiques, mais sorties de leur contexte ou utilisées de manière malveillante pour causer un préjudice tel que la diffusion de fuites d'emails privés ou de contenus intimes sans consentement.

Ces distinctions ne sont pas de simples subtilités académiques : elles déterminent les réponses appropriées. L'éducation peut atténuer la mésinformation : stopper les mécanismes économiques des arnaques peut réduire l'offre de désinformation. Dans tous les cas, l'impact du contenu faux ou trompeur, indépendamment des intentions, reste potentiellement le même : il désinforme les citoyens et génère des coûts économiques et sociaux massifs.

1.2 Notre périmètre : les manipulations informationnelles intentionnelles

Cette étude se concentre sur les manipulations informationnelles intentionnelles dont l'objectif, direct ou indirect, est d'influencer les opinions individuelles ou collectives.

Cela inclut :

- les fraudes financières et arnaques fondées sur de fausses informations (investissements frauduleux, arnaques aux investissements combinant manipulation affective et fraude financière appelés *pig butchering scams*, *deepfakes* utilisés pour des détournements de fonds) ;
- les manipulations de marchés via la diffusion de rumeurs ou de fausses nouvelles ;
- les campagnes de déstabilisation géopolitique, qui génèrent des coûts économiques mesurables (panique bancaire orchestrée, sabotage de la confiance institutionnelle) ;
- les coûts de riposte mobilisés par les acteurs publics et privés pour détecter et contrer ces menaces ;
- les coûts sociaux indirects (polarisation, érosion de la confiance, dépenses de santé) lorsqu'ils peuvent être liés à des impacts économiques quantifiables et lorsqu'ils sont liés à des manipulations informelles clairement identifiées.

Exclusions assumées : nous excluons de notre périmètre les formes de polarisation politique endogène non attribuables à des campagnes de désinformation coordonnées.

1.3 Un paysage transformé : les ruptures de 2020-2024

La dernière estimation globale du coût économique de la désinformation remonte à 2019, et évaluait ce coût à 78 milliards de dollars. Elle est le fruit d'une étude menée par l'entreprise de cybersécurité appliquée au marketing CHEQ associée au professeur d'économie Roberto Cavazos, alors enseignant à l'Université de Baltimore⁶.

Cinq ruptures majeures ont depuis transformé en profondeur le paysage informationnel :

1. La pandémie de COVID-19 (2020-2023) a provoqué une « infodémie » sans précédent⁷, dans laquelle l'accès à une information fiable est littéralement

4 The Global Risks Report 2024, World Economic Forum, *op. cit.*

5 Derakhshan H., Wardle C., *Les désordres de l'information : Vers un cadre interdisciplinaire pour la recherche et l'élaboration des politiques*, Conseil de l'Europe, 2017

6 The economic cost of bad actors on the Internet, Fake News, CHEQ, 2019

7 Gestion de l'infodémie sur la COVID-19, ONU, OMS, UNICEF, 2020

devenu une question de vie ou de mort. Les fausses informations sur les traitements, les vaccins et les mesures sanitaires ont généré des coûts humains et économiques considérables ;

2. **L'essor de l'intelligence artificielle générative** (2022-2024) a industrialisé la production de contenu trompeur. Les *deepfakes* et les contenus synthétiques ont amplifié la manipulation de l'information d'une manière qui peut déstabiliser individus, sociétés et économies ;
3. **L'intensification de la guerre hybride** et des tensions géopolitiques a fait de la manipulation informationnelle un outil stratégique central dans les affrontements entre États ;
4. **L'essor des cryptomonnaies** a créé un nouvel écosystème propice aux arnaques fondées sur la désinformation. La promesse de gains rapides et l'absence de régulation ont fait des cryptomonnaies un terrain fertile pour les manipulations informationnelles à grande échelle ;
5. **La dérégulation de la modération sur les réseaux sociaux** a fragilisé les garde-fous contre la désinformation. Le rachat de Twitter par Elon Musk en 2022 a inauguré une réduction massive des équipes Trust & Safety suivie de l'abandon par Meta début 2025 du fact-checking aux US.

1.4 Le paradoxe : reconnaissance universelle, invisibilité économique

La désinformation figure désormais au sommet des agendas politiques et stratégiques. Les gouvernements y allouent des budgets de riposte, les entreprises multiplient les investissements en protection de leur réputation, les citoyens déclarent ne plus savoir à qui faire confiance. Et pourtant : **personne ne sait vraiment ce que cela coûte**. Aucune comptabilité rigoureuse ne mesure son impact, et elle échappe aussi bien aux bilans financiers des entreprises privées qu'aux comptes publics.

Nous souhaitons participer à combler ce vide grâce à cette **quantification du coût total de la désinformation à l'échelle mondiale pour l'année 2024**. Notre méthodologie combine analyses quantitatives des données disponibles et modélisation paramétrique inspirée des approches du GIEC, avec trois scénarios : conservateur, médian, et exploratoire. Sur une question aussi complexe, multifactorielle et protéiforme, il nous semble que la rigueur impose l'humilité : nous documentons donc explicitement dans les pages qui suivent nos hypothèses, nos limites méthodologiques et nos incertitudes.

Ainsi, cette étude pourra être reproduite et augmentée chaque année.

LE COMITÉ SCIENTIFIQUE

Cette étude a été élaborée avec le concours d'un comité scientifique réunissant des expertises complémentaires en économie, data science et stratégie :

Clément Bénese (Opsci.ai) — Mathématicien et spécialiste de l'analyse de données appliquée à l'écosystème informationnel, il a piloté la collecte et la modélisation des données économiques.

Tiziana Assenza (Toulouse School of Economics) — Économiste, elle a apporté son expertise académique sur les méthodologies d'évaluation des coûts et la rigueur des estimations.

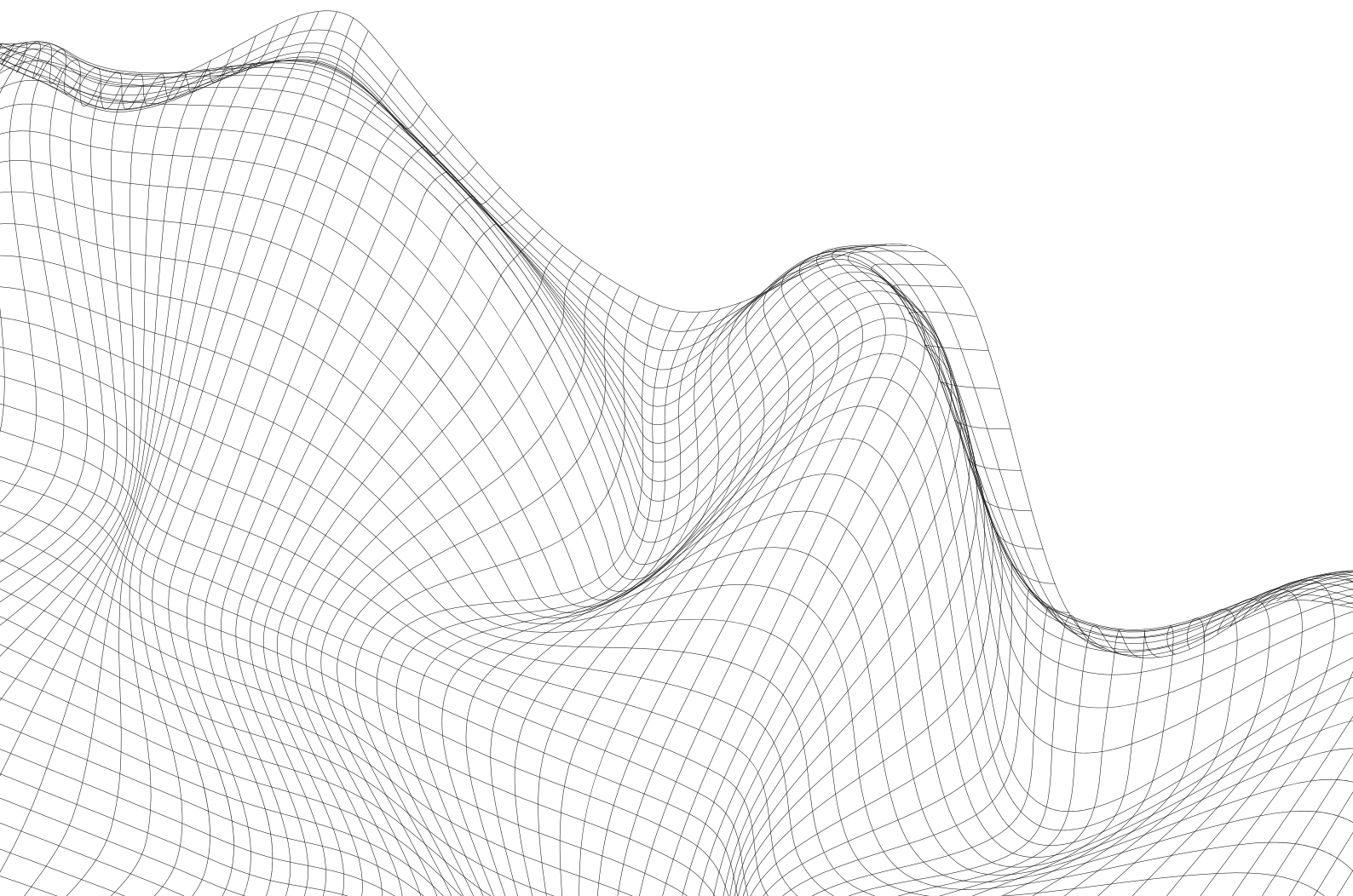
Cyril Rollinde (Citizing Consulting) — Economètre, il a contribué à l'analyse des coûts de riposte et des politiques publiques.

Le comité s'est réuni régulièrement afin de valider les hypothèses méthodologiques, discuter des fourchettes d'estimation et garantir la reproductibilité du protocole.

2.

Cartographier le terrain

**ce que l'on sait (et ce que l'on ignore)
du coût de la désinformation**



Les travaux existants abordent l'évaluation du coût de la désinformation selon diverses dimensions, bien que les méthodologies restent hétérogènes et les estimations souvent fragmentées par verticale ou par type de désinformation.

2.1 Études englobantes de référence

L'étude de référence en matière d'évaluation globale demeure celle menée par le professeur Robert Cavazos de l'Université de Baltimore en collaboration avec l'entreprise de cybersécurité CHEQ⁸ en 2019. Leurs travaux ont estimé le coût annuel de la désinformation à 78 milliards de dollars.

Cette analyse a identifié plusieurs vecteurs de coûts : les pertes boursières (39 milliards), les décisions financières erronées des consommateurs (17 milliards), les coûts de gestion de réputation (9,5 milliards) et la désinformation sanitaire (9 milliards). Une étude complémentaire de 2021⁹ par les mêmes auteurs a évalué l'impact des faux avis en ligne à 152 milliards de dollars pour le commerce mondial.

Face à ce matériau, notre premier objectif est de mettre à jour les éléments avancés par ces études en documentant nos calculs. Nous avons également choisi de les compléter par d'autres typologies de coûts liés aux manipulations de l'information.

2.2 Impact sur les marchés financiers et la confiance

Plusieurs rapports sectoriels ont documenté des aspects spécifiques du phénomène. Le Forum économique mondial a identifié en 2021 que le système de notation et d'avis en ligne influence 89 % des revenus du e-commerce mondial¹⁰, rendant la manipulation de ces systèmes particulièrement coûteuse.

Fraudes et contrefaçons

Sur le front des fraudes, les données de la Federal Trade Commission¹¹ pour 2024 révèlent une augmentation alarmante : les consommateurs américains ont déclaré des pertes de 12,5 milliards de dollars, soit une hausse de 25 % par rapport à 2023. Les arnaques aux investissements

frauduleux représentent à elles seules 5,7 milliards de dollars. Cette tendance s'inscrit dans un contexte plus large de commerce illicite : l'OCDE a estimé en 2021¹² que les contrefaçons représentaient 467 milliards de dollars dans le commerce mondial.

2.3 Polarisation sociale et coûts politiques

Une dimension peu documentée a été explorée par Allianz Research en 2024. À travers la création d'un index de résilience sociale (*Social Resilience Index*), cette étude¹³ établit un lien entre polarisation sociale et performances économiques, estimant qu'une baisse de la confiance des consommateurs due à la polarisation politique pourrait réduire la consommation de 157 à 318 milliards de dollars aux États-Unis et en Europe à l'horizon 2027. Cette approche, qui reconnaît les coûts indirects et systémiques de la désinformation, élargit considérablement le périmètre d'analyse traditionnel.

2.4 Technologies émergentes : le défi des deepfakes

L'émergence des *deepfakes* et de l'intelligence artificielle générative a également conduit à des tentatives de quantification. Le Deloitte Center for Financial Services¹⁴ projette dans une étude de 2024 que les pertes liées aux fraudes facilitées par l'IA générative, incluant les *deepfakes*, pourraient atteindre 40 milliards de dollars aux États-Unis d'ici à 2027, contre 12,3 milliards en 2023, soit un taux de croissance annuel composé de 32 %. Néanmoins, cette projection présente des faiblesses méthodologiques notables : elle repose sur des extrapolations linéaires contestables et ne distingue pas clairement les *deepfakes* d'autres formes de fraudes assistées par IA.

2.5 Lacunes identifiées et positionnement de notre étude

Les travaux existants présentent donc plusieurs limitations que notre étude cherche à combler. Premièrement, aucune mise à jour globale n'a été publiée depuis 2019 sur l'ensemble des vecteurs de coûts, alors que la pandémie, les tensions géopolitiques et l'essor de l'IA ont profondément transformé le paysage de la désinformation.

8 The economic cost of bad actors on the Internet, Fake News, op. cit.

9 The economic cost of bad actors on the Internet, Fake Online Reviews 2021, CHEQ, 2021

10 Serrano J., What's the real cost of disinformation for corporations?, World Economic Forum, 2025

11 New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024, Federal Trade Commission, 2025

12 Global trade in fake goods reached USD 467 billion, posing risks to consumer safety and compromising intellectual property, OCDE, 2025

13 Little fires everywhere: How polarization is shaping the economy (and what to do about it), Allianz Research, 2024

14 Eudes R., Les entreprises sont-elles prêtes pour l'IA générative ?, Deloitte, 2025

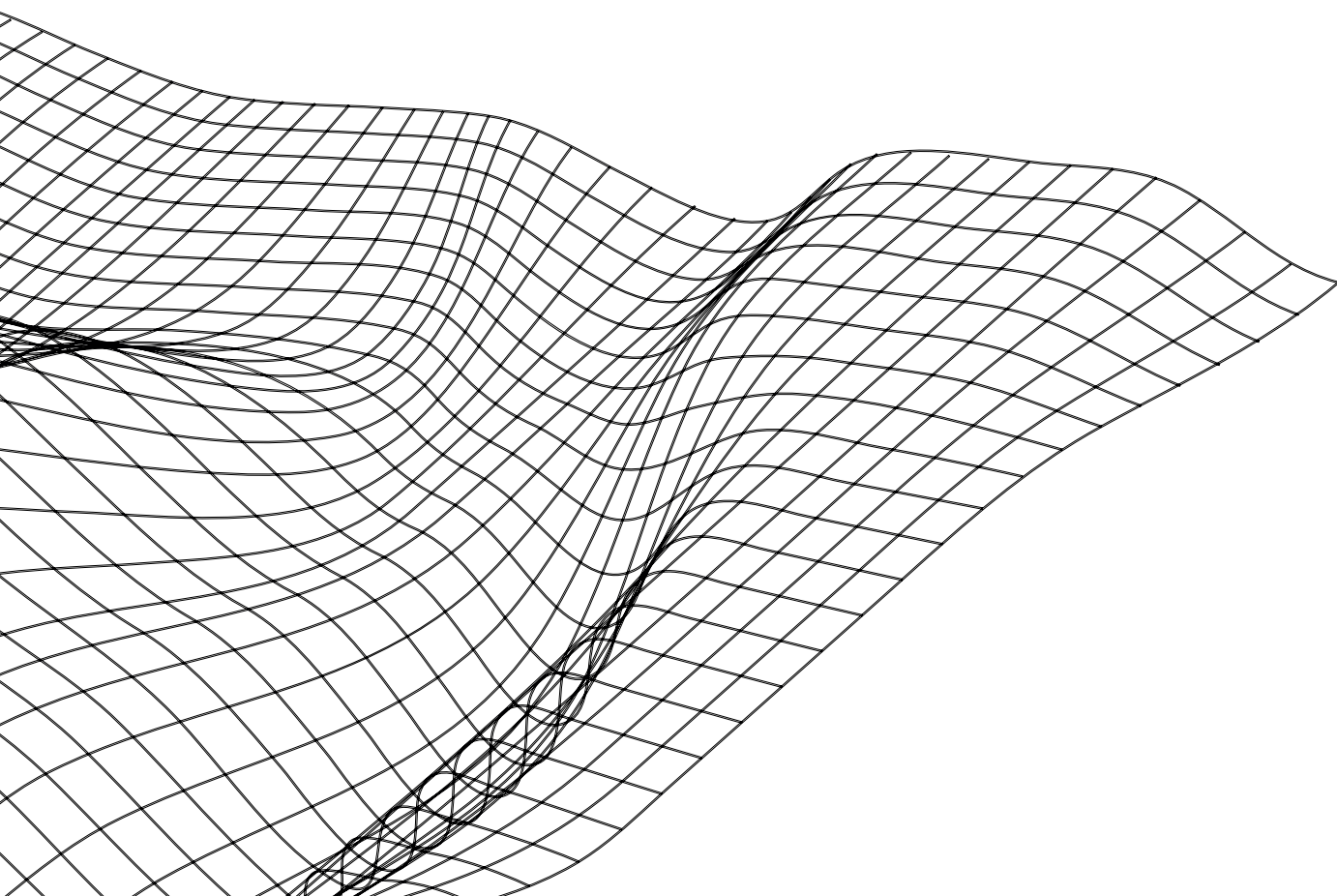
L'agrégation des études sectorielles sur le coût de la désinformation se heurte à un risque structurel de double comptage : un même phénomène, par exemple une campagne de désinformation sanitaire, peut être mesuré simultanément dans plusieurs études aux périmètres différents (santé publique, confiance institutionnelle, comportements électoraux), sans que leurs frontières soient clairement délimitées. Additionner ces chiffres sans précaution revient alors à comptabiliser plusieurs fois le même impact, gonflant artificiellement le total. Ce risque est d'autant plus difficile à neutraliser que les méthodologies varient d'une étude à l'autre : faute de définitions et d'unités de mesure communes, il est souvent impossible de déterminer si deux études quantifient des effets distincts ou des manifestations différentes du même phénomène.

Notre approche vise à proposer une synthèse actualisée pour l'année 2024, en combinant analyses quantitatives des données disponibles et évaluations qualitatives des lacunes persistantes, tout en reconnaissant explicitement les incertitudes méthodologiques inhérentes à cet exercice de quantification.

3.

Évaluer le coût de la désinformation

Un défi méthodologique



3.1 Cadre méthodologique général

Notre approche méthodologique repose sur une décomposition tripartite des coûts de la désinformation selon trois verticales majeures : **financier, social et politique** (qui inclut les budgets alloués à la défense et à la riposte informationnelle).

Cette segmentation permet d'analyser de manière granulaire les différents vecteurs d'impact tout en maintenant la cohérence globale de l'évaluation.

3.1.1 Architecture des scénarios

Pour chaque verticale, nous développons trois scénarios d'estimation :

- **Scénario conservateur** : estimation minimale fondée sur les données vérifiables et les impacts directs mesurables ;
- **Scénario médian** : estimation intermédiaire intégrant les coûts indirects documentés ;
- **Scénario exploratoire** : estimation haute incluant les effets systémiques et les coûts de long terme.

Cette approche par scénarios multiples permet de réduire l'incertitude inhérente à la quantification d'un phénomène aussi complexe et multidimensionnel que la désinformation.

3.1.2 Hypothèse de non-interaction entre verticales

Une hypothèse structurante de notre modèle est la **non-interaction entre les verticales principales** : nous considérons que les coûts financiers, sociaux et politiques peuvent être analysés de manière indépendante.

Cette simplification méthodologique signifie qu'un événement de désinformation dans la sphère financière (par exemple, une fraude boursière) n'est pas modélisé comme ayant un impact direct sur la polarisation sociale. Cette hypothèse, bien que réductrice, permet une agrégation plus rigoureuse des résultats et évite les doubles comptages.

3.1.3 Modélisation des interactions de second ordre

Nous limitons explicitement notre modélisation au sein de chaque verticale aux **interactions de second ordre**, c'est-à-dire aux effets synergiques entre deux verticales seulement. Cette restriction permet d'encoder l'ensemble des interactions dans une **matrice d'interaction**, où chaque cellule représente le coefficient de synergie (ou d'antagonisme) entre deux verticales. Par exemple, dans la verticale financière, une cellule pourrait capturer l'amplification des arnaques par les *deepfakes*.

Cette matrice présente l'avantage de l'**interprétabilité** : les experts et décideurs peuvent comprendre et valider les hypothèses d'interaction sans nécessiter une expertise poussée en modélisation mathématique. Les interactions d'ordre supérieur (trois verticales ou plus) sont négligées, ce qui constitue une limitation reconnue mais nécessaire pour la tractabilité du modèle.

3.1.4 Utilisation de la valeur de Shapley pour l'agrégation

Pour combiner à l'intérieur de chaque verticale les valeurs obtenues tout en tenant compte des **interactions de second ordre** lorsqu'elles sont identifiables, nous mobilisons le concept de **valeur de Shapley**, issu de la théorie des jeux coopératifs.

Introduite par Lloyd Shapley en 1953, cette méthode permet de distribuer équitablement un gain (ou un coût) total entre différents « joueurs » (ici, nos verticales) en fonction de leur contribution marginale.

La valeur de Shapley pour un joueur i dans un jeu coopératif est définie comme :

$$\varphi_i(v) = \sum_{S \subset N \setminus \{i\}} \frac{|S|! \cdot (n - |S| - 1)!}{n!} [v(S \cup \{i\}) - v(S)]$$

où N est l'ensemble des joueurs, S une coalition, et $v(S)$ la valeur de cette coalition.

Dans notre contexte, cette formule permet de calculer la contribution de chaque verticale au coût total de sa verticale en prenant en compte toutes les combinaisons possibles de secteurs. L'avantage de cette approche est qu'elle satisfait quatre propriétés axiomatiques fondamentales : **efficacité** (la somme des valeurs égale le coût total), **symétrie** (deux secteurs ayant le même impact reçoivent la même valeur), **additivité** (pour les jeux composites) et **joueur nul** (un secteur sans contribution reçoit une valeur nulle).

Bien que nous l'utilisions dans un régime plus réduit que le cadre général, puisque nous ne considérons pas les coalitions de plus de deux éléments, cela nous permet de stabiliser notre approche dans un cadre bien défini.

3.1.5 Intégration de l'expertise

Nous incorporons l'avis d'experts sectoriels interrogés via des **intervalles de confiance** sur les coefficients de synergie de la matrice d'interaction. Ces intervalles permettent de quantifier l'incertitude sur l'ampleur des interactions entre secteurs.

La méthodologie « semi-manuelle » que nous adoptons consiste à :

1. Solliciter des estimations d'experts sur les bornes inférieures et supérieures des coefficients de synergie ;
2. Utiliser ces intervalles pour paramétrer les trois scénarios (conservateur utilise les bornes basses, médian les valeurs centrales, exploratoire les bornes hautes) ;
3. Propager ces incertitudes à travers le calcul de la valeur de Shapley pour obtenir des intervalles de confiance sur les coûts agrégés.

3.1.6 Ajustements temporels et géographiques

Les données mobilisées ne correspondent pas toujours exactement à l'année 2024 ou à l'échelle mondiale. Pour pallier ces décalages, nous utilisons des **taux d'actualisation** et des **facteurs de normalisation géographique**.

Pour l'ajustement temporel, nous appliquons un taux d'actualisation basé sur l'inflation et la croissance du PIB mondial, ainsi que sur des indicateurs spécifiques à la digitalisation (croissance du commerce en ligne, adoption d'Internet, volume de données numériques).

La formule générale est :

$$V_{2024} = V_t \cdot (1 + r)^{(2024-t)}$$

où V_t est la valeur mesurée à l'année t , et r le taux d'actualisation.

Pour l'ajustement géographique, lorsqu'une étude ne couvre qu'une région spécifique (par exemple, les États-Unis), nous extrapolons à l'échelle mondiale en utilisant des pondérations fondées sur le PIB.

3.1.7 Traitement des recouvrements sectoriels : monitoring et riposte du secteur privé

Une question méthodologique complexe concerne les **secteurs inclus dans d'autres** : comment traiter un coût qui pourrait être classifié dans plusieurs catégories ? Par exemple, les dépenses des entreprises privées dans la lutte contre la désinformation relèvent-elles du coût financier ou du coût de riposte ?

Il nous a semblé pertinent d'inclure les coûts de riposte des entreprises privées à la verticale coûts politiques. L'idée

sous-jacente est que dans le cadre d'une approche *whole of society*, chaque composante de la société a sa part à jouer dans la lutte contre les manipulations informationnelles.

3.2 Coûts financiers : traitement de la variabilité des marchés

La modélisation des coûts financiers soulève une question théorique particulière : **la variabilité elle-même constitue-t-elle un coût ?** Lorsque la désinformation amplifie la volatilité des marchés sans nécessairement causer de perte nette, doit-on comptabiliser un impact économique ?

Notre position méthodologique est la suivante : nous distinguons les **pertes réalisées** (fraudes, chutes de valorisations, décisions d'investissement erronées) des **coûts de volatilité** (primes de risque accrues, liquidité réduite, coûts de couverture).

L'étude Baltimore de 2019¹⁵ estimait les pertes sur les marchés boursiers mondiaux à **39 milliards de dollars annuels**, soit 0,05 % de la capitalisation mondiale. Ce chiffre reposait sur l'analyse d'événements dans lesquels de fausses informations avaient provoqué des mouvements anormaux. Le cas emblématique reste le hack du compte Twitter d'Associated Press en avril 2013¹⁶ : un faux tweet annonçant que Barack Obama avait été blessé dans une explosion à la Maison-Blanche avait fait perdre **136 milliards de dollars** au S&P 500 en deux minutes. Bien que l'indice ait retrouvé son niveau trois minutes plus tard, cet épisode a révélé la fragilité structurelle des marchés face à la désinformation.

Au-delà des fluctuations sur les marchés, les entreprises subissent des dommages directs mesurables. En 2022, un faux tweet depuis un compte piraté annonçant que le laboratoire Eli Lilly fournirait l'insuline gratuitement a fait chuter l'action de **15 milliards de dollars** en une nuit¹⁷.

Ces cas illustrent une réalité structurelle : la vitesse d'exécution des marchés et la désintermédiation des décisions d'investissement (via applications mobiles et réseaux sociaux) créent un terrain fertile pour des manipulations à effet quasi immédiat. Ces coûts de volatilité méritent d'être mentionnés à titre indicatif : ils comprennent les primes de risque accrues exigées par les investisseurs face à l'incertitude informationnelle, la réduction de la liquidité sur certains marchés lors d'épisodes de désinformation, et les coûts de couverture (*hedging*)

¹⁵ The economic cost of bad actors on the Internet, Fake News, op. cit.

¹⁶ Serrano J., What's the real cost of disinformation for corporations?, World Economic Forum, 2025

¹⁷ Grossman T., The Battle Against Brand Disinformation: Preparing the Communications Industry for 2025, Truepoint, 2025

engagés par les acteurs financiers pour se prémunir contre ces risques. Ces coûts indirects, difficiles à isoler de la volatilité ordinaire des marchés, pourraient représenter plusieurs milliards de dollars annuels à l'échelle mondiale.

Les pertes réalisées sont intégrées dans les trois scénarios. Les coûts de volatilité ne sont pas inclus dans le chiffre agrégé final pour les raisons mentionnées dans le paragraphe suivant.

3.2.1 Modélisation des krachs : approche indicative

Les krachs boursiers induits ou amplifiés par la désinformation (par exemple, les krachs éclairs causés par de fausses informations sur les réseaux sociaux) posent un défi méthodologique majeur. Nous avons choisi de ne pas les inclure dans notre estimation principale pour deux raisons :

1. **Attribution causale complexe** : distinguer la part du krach imputable à la désinformation de celle liée aux fondamentaux économiques est méthodologiquement périlleux ;
2. **Effet temporaire** : les corrections de marché sont souvent transitoires, et les pertes « sur papier » ne se matérialisent pas toujours en pertes réelles.

3.3 Coûts de santé, sociaux et de la confiance

3.3.1 Coûts de santé

Les études disponibles documentent des ordres de grandeur considérables : plusieurs analyses post-COVID évaluent à des centaines de milliards de dollars les coûts liés à la sous-vaccination ou aux traitements inefficaces promus par de faux contenus. Mais ces estimations reposent sur des chaînes causales longues et difficilement isolables. Comment distinguer la part de vaccino-hésitance imputable à de la désinformation coordonnée de celle produite par la défiance ordinaire envers les institutions, les inégalités d'accès aux soins ou la communication défailante des autorités sanitaires elles-mêmes ? Cette question d'attribution est, à ce stade, sans réponse méthodologiquement satisfaisante.

Notre approche retient donc un principe strict : ne comptabiliser en coûts médicaux que les cas où le lien

entre une campagne de désinformation identifiée et un coût sanitaire documenté est établi par des sources institutionnelles robustes. Un seul cas répond à ces critères dans les données accessibles pour 2024 : l'épidémie de rougeole alimentée par les campagnes anti-vaccination, dont les coûts directs (hospitalisations, traitements, riposte sanitaire) sont chiffrés à 12,4 millions de dollars par Johns Hopkins¹⁸. Ce chiffre est faible en valeur absolue ; il est en revanche solide en termes d'attribution causale.

Les coûts de santé mentale font l'objet d'un traitement distinct et particulièrement prudent, en raison de l'absence quasi totale de bases de données gouvernementales permettant une imputation fiable à la désinformation. Nous y revenons dans la section suivante.

3.3.2 Coûts sociaux

Les coûts sociaux de la désinformation se manifestent par des mécanismes systémiques : réduction de la consommation via la polarisation et la défiance, baisse de la participation civique, fragmentation du lien social augmentant les coûts de transaction. Pour les quantifier, nous nous appuyons sur les travaux d'Allianz Research¹⁹, qui modélisent l'effet d'un choc de confiance des consommateurs sur la consommation privée aux États-Unis et en zone euro sur quatre ans. Nous en extrapolons la part attribuable aux impacts sociaux (25 % du total) et la ramenons à l'année 2024 à l'échelle mondiale.

3.3.3 Coût de la défiance

L'enquête de l'OCDE sur les déterminants de la confiance dans les institutions publiques²⁰ (novembre 2023, près de 60 000 répondants dans 30 pays) constitue notre principale référence empirique pour ce troisième volet. Elle révèle que seulement 39 % des citoyens déclarent faire confiance à leur gouvernement national, et que la proportion de personnes affichant une confiance faible ou nulle (44 %) dépasse celle exprimant une confiance modérée ou élevée. Bien que le lien causal entre désinformation et perte de confiance soit complexe, plusieurs études^{21 22} établissent une corrélation robuste entre exposition à des contenus manipulateurs et baisse de la confiance institutionnelle. Ce poste, difficile à isoler quantitativement, est intégré dans notre modélisation via les paramètres de coûts sociaux systémiques.

18 Willens V., *Estimating the Financial Costs of Measles Outbreaks*, Johns Hopkins, 2025

19 Little fires everywhere: How polarization is shaping the economy (and what to do about it), *op. cit.*

20 Enquête de l'OCDE sur les déterminants de la confiance dans les institutions publiques – résultats 2024 : *Instaurer la confiance dans un contexte complexe*, Éditions OCDE, 2024

21 Aitken, B., Hoes, E., Zhang, J. et al. Prominent misinformation interventions reduce misperceptions but increase scepticism. *Nature Human Behavior*, 2024

22 Naviguer dans les désordres de l'information, Bureau du scientifique en chef du Québec, 2025

3.3.4 Modélisation des coûts systémiques

Les coûts sociaux de la désinformation se manifestent principalement à travers des **mécanismes systémiques** difficilement quantifiables, mais économiquement significatifs :

1. **Réduction de la consommation** : la polarisation et la défiance réduisent la propension à consommer, comme l’a documenté Allianz Research²³ ;
2. **Baisse de la participation civique** : le désengagement démocratique génère des coûts d’opportunité en termes de qualité des politiques publiques^{24 25} ;
3. **Fragmentation sociale** : l’effritement du capital social réduit la coopération économique et augmente les coûts de transaction²⁶.

Pour quantifier ces effets, nous nous appuyons sur les travaux d’Allianz Research qui estiment qu’une baisse de la confiance des consommateurs due à la polarisation pourrait réduire la consommation de 157 à 318 milliards de dollars sur quatre ans aux États-Unis et en Europe. Nous extrapolons ces chiffres à l’échelle mondiale et les actualisons pour l’année 2024 uniquement.

3.4 Coûts politiques et de riposte

3.4.1 Dépenses publiques et privées de lutte contre la désinformation

L’évaluation des coûts de riposte nécessite de quantifier les ressources mobilisées par les acteurs publics et privés pour contrer la désinformation. Cette dimension constitue un coût direct et mesurable, contrairement aux coûts d’opportunité ou systémiques.

3.4.2 Distinction FIMI/DIMI et périmètre d’analyse

Pour circonscrire notre périmètre d’analyse, nous adoptons la distinction entre **FIMI** (*Foreign Information Manipulation and Interference*, manipulation informationnelle étrangère) et **DIMI** (*Domestic Information Manipulation and Interference*, manipulation informationnelle domestique).

Notre étude se concentre principalement sur les **FIMI**, c’est-à-dire les opérations de désinformation coordonnées par des acteurs étrangers (États, organisations). Cela signifie

que nous incluons dans notre analyse les coûts liés à des campagnes comme celles attribuées à des médias contrôlés par des États étrangers (par exemple, RT), mais nous **excluons** la désinformation produite par des médias domestiques partisans (par exemple, Fox News aux États-Unis ou certains médias nationaux en Europe).

Ce choix méthodologique présente des avantages et des inconvénients :

Avantages :

- périmètre plus clair ;
- données de meilleure qualité sur les FIMI (traçabilité, attribution) ;
- consensus scientifique plus large sur la caractérisation des FIMI comme désinformation.

Inconvénients :

- sous-estimation potentielle significative des coûts totaux ;
- frontière FIMI/DIMI parfois floue (coordination entre acteurs étrangers et domestiques, média domestique ayant une influence importante à l’international).

3.4.3 Le marché de la « Confiance Numérique » (Digital Trust) : un indicateur

Le marché mondial de la Confiance Numérique (*Digital Trust*) constitue un indicateur particulièrement pertinent pour estimer ces dépenses. Ce marché est évalué à 118,71 milliards de dollars en 2024²⁷, couvrant un large spectre de solutions : cybersécurité, détection de fraudes, vérification des faits et technologies d’intégrité des données, etc.

Cependant, ce marché englobe des dimensions bien plus larges que la seule lutte contre la désinformation. Il inclut également la protection contre les cyberattaques techniques, la conformité réglementaire (RGPD, etc.) et d’autres aspects de la sécurité numérique. Pour isoler la part spécifiquement dédiée à la lutte contre la désinformation, nous devons affiner notre analyse.

3.4.4 Estimation de la part « anti-désinformation »

Sur la base d’entretiens préliminaires avec des professionnels du secteur et d’analyses sectorielles, nous

²³ Little fires everywhere: How polarization is shaping the economy (and what to do about it), op. cit.

²⁴ Navigating Apathy: A Data-Backed Analysis of Public Disengagement in Political and Economic Spheres, Yorkshire Popular Front, 2025

²⁵ Braconnier C., Mayer N., Les dynamiques du décrochage civique illustrées par la hausse de l’abstention aux scrutins nationaux, 2024

²⁶ Durante R., Mastroiocco N., Minale L. and Snyder J. M., *Unpacking Social Capital*, The Economic Journal, 2025

²⁷ Digital Trust Market (2025 - 2033), Grand View Research, 2025

estimons que 10 à 15 % du marché global du *digital trust* est directement ou indirectement consacré à la lutte contre la désinformation ou à la protection de la surface informationnelle. Cette fourchette permet de situer l'investissement actuel entre 12 et 18 milliards de dollars en 2024.

Cette estimation repose sur les éléments suivants :

1. **Veille et détection** : outils de surveillance des réseaux sociaux, détection automatique ou manuelle de contenus suspects ;
2. **Vérification des faits** : fact-checking, services de modération de contenu ;
3. **Technologies d'intégrité** : authentification de contenu, détection de *deepfakes* ;
4. **Formation et sensibilisation** : programmes d'éducation aux médias pour les employés ;
5. **Résilience organisationnelle** : plans de gestion de crise, assurance réputation.

3.4.5 Répartition public-privé

Les entreprises investissent dans la protection de leur réputation et de leurs opérations, tandis que les États concentrent leurs efforts sur la régulation, la recherche et les campagnes de sensibilisation publique.

Pour le secteur public, nous compilons les données budgétaires disponibles sur :

- les agences de sécurité nationale et de renseignement²⁸ ;
- les programmes de l'UE (Europe Creative²⁹, Erasmus +, CERV, Horizon Europe^{30, 31, 32}, EDMO³³).

Pour le secteur privé, nous nous appuyons sur :

- les rapports annuels des plateformes (Meta³⁴, Google³⁵) décrivant leurs investissements en modération dans un contexte électoral particulier aux États-Unis ;
- les analyses de marché sur les dépenses en cyber-sécurité et gestion de réputation ;
- les données sectorielles (BFSI, santé, médias) sur les dépenses de protection contre la désinformation.

3.4.6 Coût de la mobilisation des ressources humaines

Nous évaluons également le coût de la mobilisation de ressources humaines pour la détection et la riposte. Bien que difficile à chiffrer précisément, ce coût est estimé dans notre scénario médian à 28 millions de dollars. Cette estimation est fondée sur le budget de fonctionnement de l'agence gouvernementale française en charge de la détection des ingérences étrangères, estimé à 14 millions de dollars en 2021³⁶.

28 Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide - Rapport, Sénat, 2024

29 La Commission met à disposition 16 millions d'euros de fonds pour soutenir le journalisme et l'éducation aux médias dans toute l'Europe, Commission européenne, 2024

30 Cooperating with fact-checkers, civil society, media and academia, European Commission, 2025

31 Facts not Fakes Tackling disinformation, strengthening information integrity, OECD, 2024

32 Kallioniemi P., *Beyond Defence: A Proactive Strategy for the West in the Information Domain*, ICDS Estonia, 2025

33 Observatoire européen des médias numériques - EDMO, Commission européenne, 2025

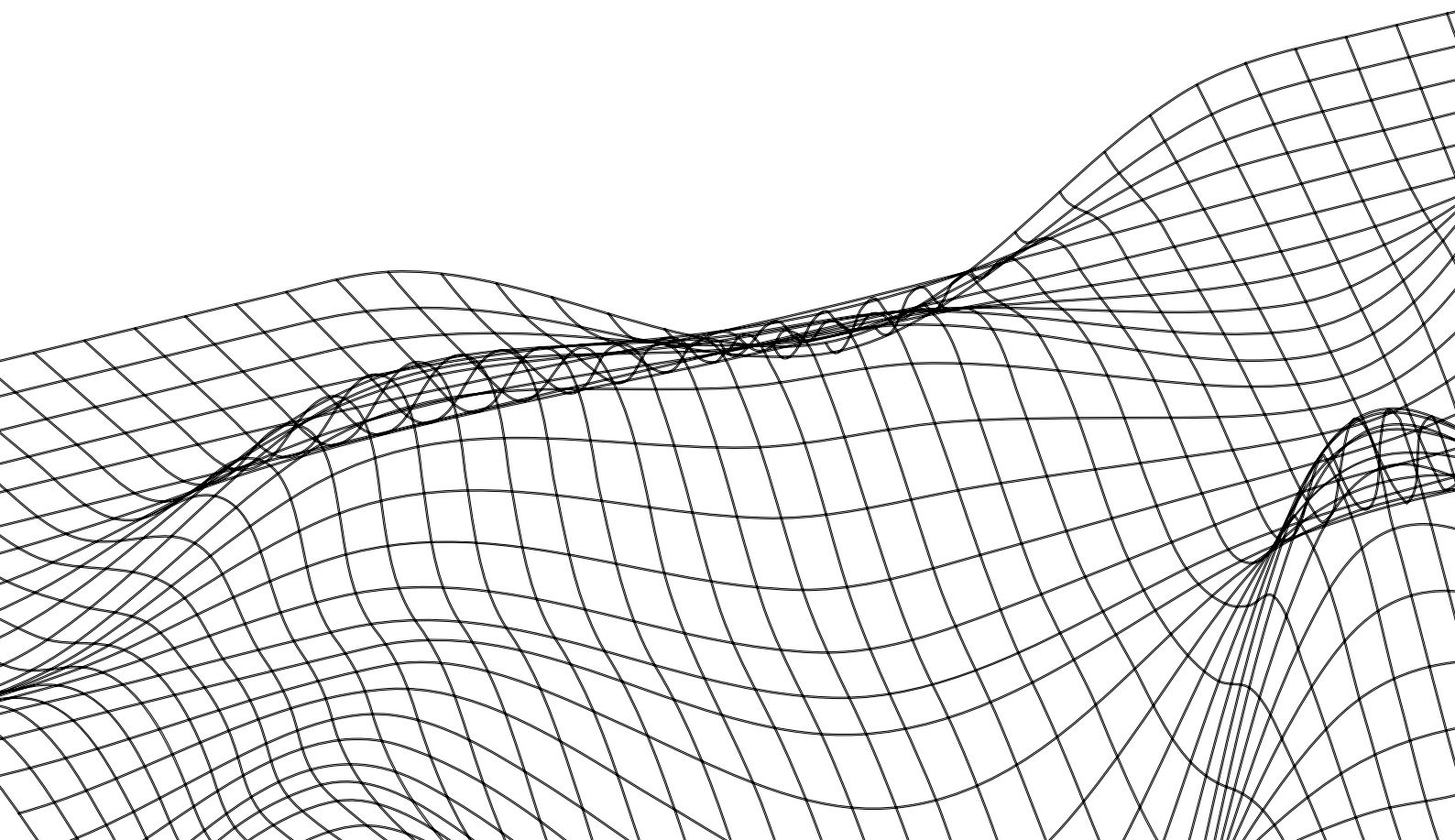
34 Trzun Z., *Analyzing the cost and necessity of the fight against disinformation from the national security perspective*, 2024

35 Feldman B., Ma O., *How Google and YouTube are investing in fact-checking*, 2022

36 Muckensturm B., *Viginum, un service pour détecter les tentatives d'ingérence sur les réseaux sociaux*, Radio France, 2021

4.

Les chiffres



4.1. Coûts financiers directs : l'hémorragie économique mesurable

4.1.1 Scénario 1 (conservateur) : 353 milliards de dollars

Notre estimation conservatrice repose sur les données les plus robustes et directement vérifiables. Les *pertes en capitalisation boursière mondiale* s'élèvent à **60,40 milliards de dollars**, chiffre actualisé avec les chiffres de capitalisation boursière globale de 2024 selon la méthodologie de l'étude de Baltimore³⁷ (i.e. pertes de 0,05 % de la capitalisation mondiale imputables à la désinformation).

L'économie de la désinformation elle-même génère des flux financiers considérables. Les *faux avis en ligne* représentent à eux seuls **227 milliards de dollars**, selon notre actualisation des calculs issus de l'étude CHEQ associée au professeur d'économie Roberto Cavazos (2019) fondée sur le montant total du e-commerce en 2024³⁸.

Ce chiffre reflète l'impact des avis frauduleux sur les décisions d'achat des consommateurs : selon le Forum économique mondial³⁹, 89 % des revenus du e-commerce mondial sont influencés par les systèmes de notation en ligne. Les faux avis créent ainsi une **distorsion massive du marché**, où des produits de qualité inférieure ou qui ne respectent pas les législations locales bénéficient d'une visibilité induite, tandis que des offres légitimes sont pénalisées. Ce phénomène touche particulièrement les plateformes comme Amazon, TripAdvisor ou l'écosystème Google, dans lesquels la confiance dans les avis de tiers partageant leur expérience constitue un pilier du modèle économique.

Les revenus publicitaires captés par les sites de désinformation atteignent **2,6 milliards de dollars** en 2024 (NewsGuard⁴⁰), tandis que les amendes infligées aux plateformes totalisent **153 millions de dollars** (États-Unis⁴¹, Canada⁴², Australie^{43 44}, Brésil⁴⁵). Un phénomène particulièrement préoccupant concerne les bénéfices indirects des grandes plateformes : Meta aurait ainsi généré

16,45 milliards de dollars de revenus publicitaires sur des contenus frauduleux en 2024, représentant environ 10 % de ses revenus publicitaires totaux (Reuters⁴⁶).

Les *fraudes directes* constituent le troisième pilier de ce scénario conservateur. La Federal Trade Commission (FTC⁴⁷) rapporte **12,5 milliards de dollars** de pertes déclarées dues aux fraudes en 2024. Dans le domaine des cryptomonnaies, les *pig butchering scams* et autres arnaques ont généré **5,5 milliards de dollars** de pertes (Cyvers⁴⁸).

Les produits contrefaits, dont une proportion significative repose sur de fausses informations concernant leur origine ou leur qualité, représentent un marché de 467 milliards de dollars en 2021 selon l'OCDE⁴⁹. Nous appliquons un taux d'actualisation de 5 % jusqu'à 2024 pour parvenir à un total de 567 milliards de dollars. À partir de notre estimation 2024, l'application d'un coefficient prudent de 5 % à ce total pour isoler la part attribuable à la désinformation intentionnelle porte le montant à **28,38 milliards de dollars**.

Enfin, les cas particuliers d'entreprises illustrent l'impact direct sur les revenus : Netflix a perdu **33 millions de dollars** en résiliations d'abonnements suite à des campagnes de désinformation⁵⁰.

4.1.2 Scénario 2 (médian) : 393,1 milliards de dollars

Le scénario médian intègre l'*effet catalyseur des deepfakes*, estimé à 15 % de surcoût sur l'ensemble des fraudes et manipulations financières. Cette technologie a en effet démultiplié l'efficacité des arnaques au PDG, des manipulations d'identité et des fraudes à l'investissement.

En plaçant le coefficient des produits contrefaits à 10 %, et appliqué à notre base conservatrice, ce multiplicateur porte les coûts financiers directs à **393,1 milliards de dollars**.

37 List of countries by stock market capitalization, Wikipedia, 2026

38 Nguyen T. H., *Factors Affecting Consumer's Online Shopping Behavior During the Covid-19 Pandemic: An Integrative Model*, 2023

39 Serrano J., *What's the real cost of disinformation for corporations?*, World Economic Forum, 2025

40 Skibinski M., *Special Report: Top brands are sending \$2.6 billion to misinformation websites each year*, NewsGuard, 2025

41 Décisions SEC 2024 (greenwashing / ESG) : Keurig / WisdomTree / Invesco Advisers, U.S. Securities and Exchange Commission, 2024

42 Décisions canadiennes 2024 : Sirius / Cineplex, Gouvernement du Canada, 2024

43 Décisions australiennes ACCC 2024 : Qantas / Secure Parking / Mazda, Australian Competition & Consumer Commission, 2024

44 Décisions australiennes ASIC 2024 : Mercer / Vanguard, Australian Securities & Investments Commission, 2024

45 La Cour suprême ordonne la levée de la suspension du réseau social X au Brésil, Le Monde, 2024

46 Horwitz J., *Meta is earning a fortune on a deluge of fraudulent ads, documents show*, Reuters, 2025

47 New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024, Federal Trade Commission, 2025

48 Turner L., *\$5.5 Billion Stolen: Pig Butchering Scams Explode in Crypto, Cyvers Report Reveals*, Crypto Ninjas, 2025

49 Enquête de l'OCDE sur les déterminants de la confiance dans les institutions publiques - résultats 2024 : *Instaurer la confiance dans un contexte complexe*, op. cit.

50 Baruchin R., *2024 Brand Crisis Round-Up - Part 2*, op. cit.

4.1.3 Scénario 3 (exploratoire) : 456,3 milliards de dollars

Notre scénario exploratoire porte l'effet catalyseur des deepfakes à 20 %, reflétant leur capacité à transformer radicalement le paysage de la fraude. Cette estimation suppose une adoption généralisée de ces technologies par les acteurs malveillants et une adaptation encore limitée des systèmes de détection, et mène le total à **396,8 milliards de dollars**.

Enfin, ce scénario explore les effets de second ordre : détérioration accélérée de la confiance dans les institutions financières, augmentation des coûts de transaction liés à la vérification accrue, impact sur les décisions d'investissement et d'épargne. Bien que ces effets soient difficiles à quantifier précisément (voir section 5), nous les estimons à 15 % additionnels, ce qui correspond à un surcoût de **59,6 milliards de dollars** pour l'année 2024.

4.2. Coûts sociaux : l'impact sur la santé et la cohésion sociale

Le domaine social englobe les coûts liés à la santé publique et mentale, ainsi qu'aux dégradations du lien social directement attribuables à des campagnes de désinformation identifiées.

4.2.1 Scénario 1 (conservateur) : 37 millions de dollars

Dans notre approche conservatrice, nous nous limitons aux coûts sanitaires directement mesurables et renseignés. L'épidémie de rougeole liée aux campagnes anti-vaccination a généré des coûts directs de **12,4 millions de dollars** en 2024 (Johns Hopkins⁵¹, OMS⁵², gouvernement canadien⁵³). Ces chiffres incluent les hospitalisations, les traitements et les mesures de riposte sanitaire dans les régions affectées. Cette épidémie, aujourd'hui en expansion aux États-Unis, constitue le « canari dans la mine » du coût de la désinformation en matière de santé.

Les *coûts de santé mentale* constituent un second volet (difficilement) quantifiable : peu de gouvernements donnent accès à des bases de données robustes qui permettent de documenter le sujet.

Néanmoins, au Canada, les antidépresseurs ont représenté un coût de **219 millions de dollars en 2022**⁵⁴, qui équivaut après actualisation en 2024 à **254 millions de dollars**. En isolant la part attribuable aux effets de la désinformation sur la polarisation et l'anxiété sociale (que nous estimons à 10 %), nous obtenons un coût estimé de **25 millions de dollars** pour 2024. Cette estimation prudente est fondée sur les études liant l'exposition aux contenus polarisants et anxiogènes sur les réseaux sociaux à l'augmentation des troubles anxieux et dépressifs, notamment chez les jeunes adultes.

Il est à noter que nous n'avons pas identifié de données probantes concernant les coûts des *campagnes de prévention* spécifiquement dédiées à contrer la désinformation sanitaire.

4.2.2 Scénario 2 (médian) : 9,8 milliards de dollars

Le scénario médian intègre les effets systémiques de polarisation documentés par le rapport Allianz⁵⁵. Sur les **157 à 318 milliards de dollars** de coûts identifiés pour les États-Unis et l'Europe à l'horizon 2027, nous estimons que **25 %** sont attribuables à des impacts sociaux (le reste relevant du domaine financier et politique). Cela représente, pour la seule année 2024 et à l'échelle mondiale, environ **9,8 milliards de dollars**.

Pour établir ces estimations, Allianz Research mobilise trois niveaux d'analyse. D'abord, un *Social Resilience Index* (SRI) couvrant 185 pays, qui agrège des indicateurs structurels de fragilité politique, institutionnelle et sociale (croissance économique, inégalités, participation au marché du travail, dépenses publiques, stabilité monétaire). Ensuite, une mesure de la polarisation politique via l'indice Dalton, calculé à partir des données électorales de l'UE et de l'OCDE, qui quantifie l'écartement idéologique entre partis selon leur position sur l'axe gauche-droite et leur poids électoral. Enfin, une modélisation macroéconomique testant deux scénarios de choc de confiance des consommateurs (-10 % et -20 % sur une période), dont les effets sur la consommation privée sont projetés sur quatre ans aux États-Unis et en zone euro, les deux zones géographiques pour lesquelles les données sont jugées suffisamment robustes.

51 Willens V., *Estimating the Financial Costs of Measles Outbreaks*, op. cit.

52 La Région européenne rapporte le plus grand nombre de cas de rougeole depuis plus de 25 ans - UNICEF, OMS/Europe, OMS, 2025

53 Measles and rubella weekly monitoring report, Gouvernement du Canada, 2025

54 Dépenses en médicaments prescrits au Canada, 2023 : regard sur les régimes publics d'assurance médicaments - 100 principales catégories de médicaments, 2022, tableaux de données, Institut canadien d'information sur la santé, 2023

55 Little fires everywhere: How polarization is shaping the economy (and what to do about it), op. cit.

4.2.3 Scénario 3 (exploratoire) : 19,9 milliards de dollars

Le rapport Allianz, dans sa borne haute, suggère des coûts pouvant atteindre les **318 milliards de dollars** à l'horizon 2027 pour les seuls États-Unis et Europe. Notre extrapolation mondiale, à hauteur de 25 % du total, porte la contribution sociale de la désinformation à **19,9 milliards de dollars** pour l'année 2024.

4.3. Coûts politiques et de riposte

Le domaine politique regroupe les coûts liés à l'intégrité des processus démocratiques, aux opérations d'influence étrangère et aux ripostes institutionnelles et privées mobilisées pour y faire face.

4.3.1 Scénario 1 (conservateur) : 2,1 milliards de dollars

Notre scénario conservateur se limite aux *coûts électoraux directement mesurables*. Le cas roumain, où l'élection présidentielle a été annulée suite à des interférences massives identifiées, illustre de manière frappante l'impact systémique de la désinformation. Le coût de cette annulation et de la nouvelle organisation électorale s'élève à **280 millions de dollars** (Europa Libera Romania⁵⁶). Ce chiffre ne représente probablement qu'une fraction du coût politique réel, puisqu'il exclut la perte de confiance institutionnelle et les dommages de long terme au processus démocratique roumain.

Les dépenses en opérations de désinformation pure constituent un second poste quantifiable. La propagande russe identifiée représente **1,5 milliard de dollars** pour l'année 2024 (sources gouvernementales russes⁵⁷). Cette estimation, déjà considérable, exclut les opérations non attribuées ou menées par d'autres acteurs étatiques et non étatiques.

Les *coûts de riposte institutionnelle* mobilisés par les États et les organisations internationales incluent :

- 250 millions de dollars pour les États-Unis⁵⁸ ;
- 27,1 millions d'euros pour l'Union européenne (projets et initiatives institutionnelles⁵⁹) ;

- 15,2 millions de dollars canadiens pour le Canada⁶⁰ ;
- entre 460 000 et 2,05 millions de dollars pour l'Indonésie selon les estimations (ResearchGate⁶¹) ;
- 16,6 millions d'euros pour les programmes d'éducation aux médias à l'échelle européenne^{62 63} ;
- 100 millions de dollars pour l'ensemble des initiatives de vérification de l'information dans le monde⁶⁴

4.3.2 Scénario 2 (médian) : 14,22 milliards de dollars

Les nombres indiqués ci-dessus concernent seulement les pays qui documentent de façon transparente leurs efforts de lutte contre les manipulations informationnelles. Nous estimons que d'autres pays ont des coûts similaires. Les investissements publics dans la lutte contre la désinformation, en dehors de ceux précédemment présentés, sont de l'ordre de 120 millions de dollars.

De plus, nous supposons que le secteur privé est aussi concerné par les sujets de riposte face aux attaques informationnelles. Incluse dans la catégorie Digital Trust & Safety, cette part de marché se situerait autour de 12 à 18 milliards de dollars.

4.3.3 Scénario 3 (exploratoire) : 40,1 milliards de dollars

Ce scénario explore également les coûts de long terme de l'érosion démocratique : diminution de la participation électorale liée à la défiance, augmentation des coûts de sécurisation des processus électoraux, nécessité de réformes institutionnelles pour restaurer la confiance.

Ces effets systémiques, bien que difficilement quantifiables avec précision, sont estimés, en reprenant le rapport Allianz⁶⁵ et en supposant un effet politique équivalent à l'effet social, à **19,9 milliards de dollars** pour l'année 2024.

Enfin, ce scénario intègre une intensification des investissements de riposte : doublement des budgets de fact-checking, des programmes d'éducation aux médias.

56 Cărlugea S., *Calendarul alegerilor prezidențiale 2024. Costurile alegerilor: prezidențiale – 1,4 miliarde, parlamentare – 880 de milioane*, Europa Libera Romania, 2024

57 Michałowska A. and Kubś J., *Coining lies. Kremlin spends 1.5 Billion per year to spread disinformation and propaganda*, Debunk.org, 2022

58 Dinan S., *Government spending to combat 'misinformation' jumped massively under Biden*, The Washington Post, 2024

59 Les agences de sécurité nationale et de renseignement et les programmes de l'UE (Horizons Europe et EDMO), op. cit. [Section 3.4 / Répartition public-privé]

60 Facts not Fakes Tackling disinformation, strengthening information integrity, OECD, 2024

61 Alamsyah P., Nul Hakim L., Wijaya G., Wicaksono A., *Debunking disinformation on YouTube : a fact check on the 2024 Indonesian election*, Jurnal Studi Komunikasi, 2024

62 La Commission met à disposition 16 millions d'euros de fonds pour soutenir le journalisme et l'éducation aux médias dans toute l'Europe, op. cit.

63 Cooperating with fact-checkers, civil society, media and academia, op.cit.

64 International Fact-Checking Network, *State of the fact-checkers report*, Poynter, 2025

65 Little fires everywhere: How polarization is shaping the economy (and what to do about it), op. cit.

Ces ripostes, bien que nécessaires, constituent elles-mêmes un surcoût économique par rapport au scénario précédent, estimé à 320 millions de dollars.

4.4. Synthèse des trois domaines

Le tableau ci-dessous récapitule nos estimations pour chaque domaine selon les trois scénarios :

Domaine	Scénario 1	Scénario 2	Scénario 3
Financier	353,5 Md\$	393,1 Md\$	456,4 Md\$
Social	0,03 Md\$	9,8 Md\$	19,9 Md\$
Politique	2,1 Md\$	14,2 Md\$	40,1 Md\$
Total	355,6 Md\$	417,1 Md\$	516,4 Md\$

Il est important de noter que ces chiffres, bien que conséquents, représentent probablement une sous-estimation du coût réel de la désinformation en 2024.

Comme détaillé dans la section 5 sur nos limitations méthodologiques, plusieurs postes n’ont pu être quantifiés, faute de données probantes : l’impact sur l’épargne et les décisions d’investissement, les coûts de réputation des entreprises non attribuables à des campagnes spécifiques et les effets macroéconomiques diffus de la défiance généralisée.

De même, notre focus sur les FIMI (*Foreign Information Manipulation and Interference*) plutôt que sur l’ensemble des manipulations informationnelles implique que nous excluons de fait une part significative des coûts liés aux DIMI (*Domestic Information Manipulation and Interference*).

Néanmoins, même dans notre scénario le plus conservateur, le coût économique mondial de la désinformation pour l’année 2024 se chiffre en centaines de milliards de dollars, confirmant la qualification du Forum économique mondial, qui place ce phénomène au rang des risques majeurs de notre époque.

4.5. Les limitations

Tout exercice de quantification du coût de la désinformation se heurte à des difficultés structurelles que la rigueur méthodologique peut atténuer, mais non supprimer. Les suivantes sont constitutives de notre approche et doivent être gardées à l’esprit dans l’interprétation des résultats.

Attribution causale

La limitation la plus fondamentale est celle du lien de causalité. Pour rappel : nous avons appliqué un principe d’attribution stricte, en n’intégrant que les coûts pour lesquels ce lien est documenté par des sources institutionnelles ou académiques robustes.

Sécurité de l’épargne

Il est extrêmement probable que la désinformation ait un impact négatif sur la qualité et la sécurité de l’épargne (via les fraudes et les mauvais choix d’investissement) et potentiellement sur son volume (en cas de perte de confiance massive dans l’économie). Toutefois, une preuve simple et généralisable reliant directement « l’ensemble des fake news » à « la variation du taux d’épargne » est complexe à établir scientifiquement en raison de la multiplicité des facteurs économiques en jeu. On observe plutôt des corrélations fortes au niveau des comportements individuels et des coûts macroéconomiques importants liés à la désinformation (estimés à plusieurs milliards de dollars pour l’économie mondiale, selon certaines études).

L’évolution rapide du paysage

L’essor des contenus synthétiques générés par IA (deepfakes audio, vidéo, texte à grande échelle) et la reconfiguration des plateformes en 2024 (retrait de programmes de modération chez Meta, réduction des équipes Trust & Safety) modifient structurellement les conditions de production et de diffusion de la désinformation. Les données et études sur lesquelles nous nous appuyons reflètent un état du paysage qui évolue plus vite que les cycles de recherche académique.

Les coûts non retenus

Plusieurs postes de coûts potentiellement significatifs ont été délibérément exclus faute de données d’attribution fiables : la sous-vaccination COVID-19, les effets de la désinformation sur les comportements d’épargne et d’investissement individuels, les coûts de santé mentale liés à l’exposition prolongée à des contenus anxiogènes ou polarisants, et les externalités négatives sur les marchés

du travail. Ces exclusions sont documentées et justifiées dans les sections méthodologiques correspondantes ; elles signifient que notre estimation constitue un plancher, non un plafond.

Le biais de disponibilité des données

Notre modélisation ne peut quantifier que ce qui a été mesuré. Les données disponibles sont concentrées sur les États-Unis et l'Europe occidentale, et sur les vecteurs les plus visibles de la désinformation (réseaux sociaux, campagnes identifiées). Les effets dans les pays du Sud global, les zones de conflit informationnel actif ou les espaces numériques moins documentés restent largement hors de portée. Le chiffre produit est donc moins un coût mondial qu'une projection à partir d'un échantillon géographiquement et structurellement biaisé.

La temporalité et les effets cumulatifs

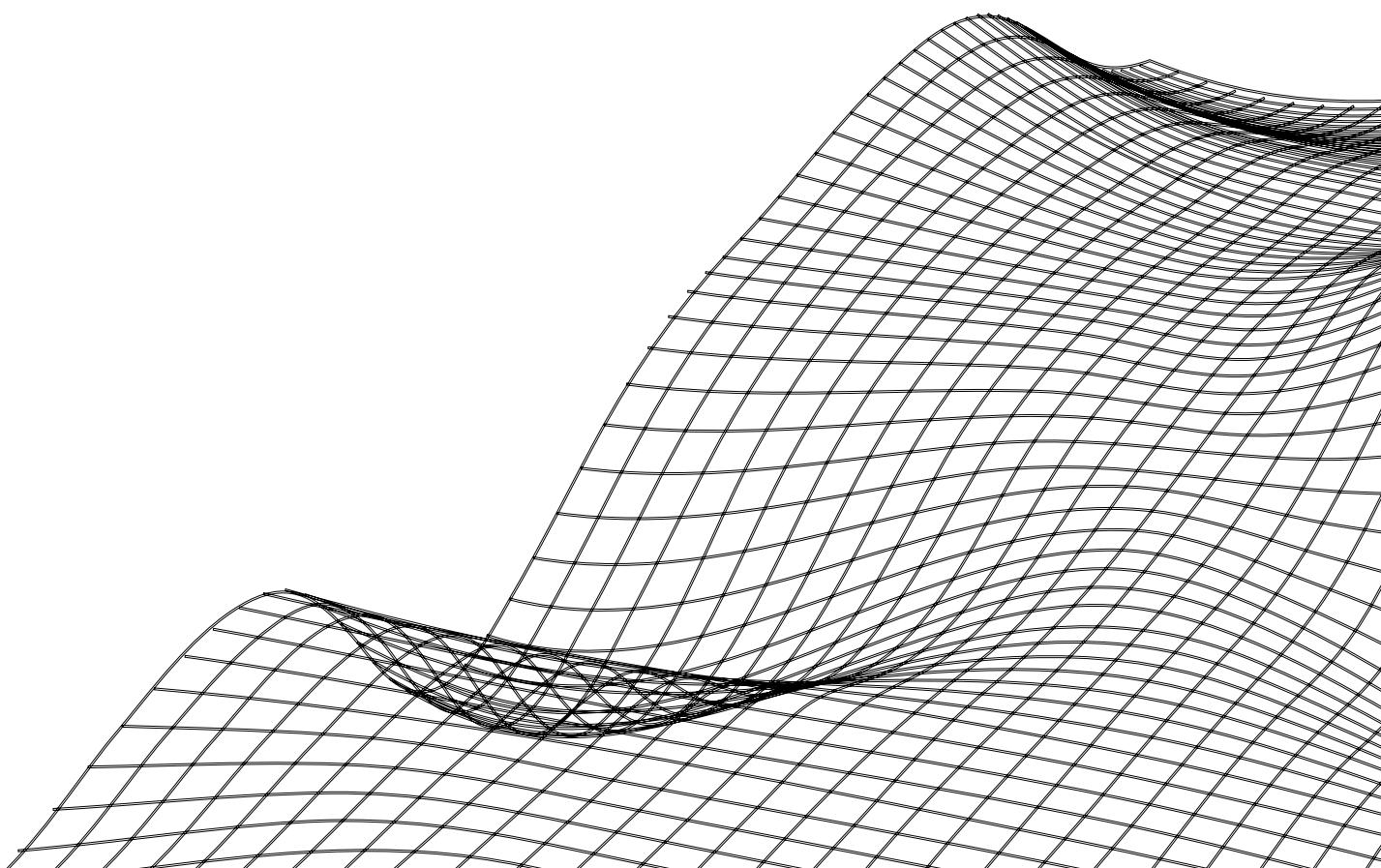
Notre étude produit une estimation pour l'année 2024. Elle est donc soumise, pour certains phénomènes, à une mise à jour des coûts de ceux-ci utilisant un taux d'actualisation fixé selon les méthodologies classiques d'économétrie. De plus, elle ne capture pas les effets cumulatifs de la désinformation sur le long terme : érosion progressive de la confiance institutionnelle, dégradation durable du débat public, effets générationnels sur les comportements civiques et de consommation. Ces effets de second ordre, bien documentés dans la littérature, sont par nature impossibles à intégrer dans un chiffrage annuel.

La focalisation sur les FIMI

Notre périmètre d'analyse couvre, lorsque c'est pertinent, principalement les opérations d'ingérence informationnelle étrangère (FIMI), au détriment des manipulations domestiques (DIMI). Ce choix est méthodologiquement justifié, les FIMI sont mieux tracées et attribuées, mais il conduit à exclure une part probablement majoritaire de la désinformation en circulation, notamment celle produite par des acteurs politiques ou médiatiques nationaux. Les coûts réels sont donc vraisemblablement supérieurs à nos estimations.

5.

Conclusion & annexes



5.1. Conclusion

Agir ou subir, par Ayman Awada

Cette étude mesure avec méthode l'impact des manipulations informationnelles sur nos économies et nos démocraties. Il reste évidemment des zones d'ombre à éclaircir.

La perte de confiance institutionnelle d'abord. C'est un actif que vous ne trouverez dans aucun bilan, mais dont l'effondrement paralyse toute velléité de réforme, toute décision de long terme. Ensuite, les 417 milliards de dollars perdus à cause des manipulations informationnelles alimentent une infrastructure criminelle dont l'influence réelle sur l'économie reste encore largement sous-estimée. Enfin, nous sommes entrés dans une nouvelle ère : celle de l'IA et de ses effets multiplicateurs.

Il y a vingt ans, la cybersécurité était perçue comme un risque technique, marginal, géré par quelques experts. Aujourd'hui, c'est une fonction stratégique dotée de budgets, de gouvernance et de régulation. La lutte contre la désinformation suit la même trajectoire, avec le même retard à combler. Les *deepfakes* constituent l'alerte : ils effacent la frontière entre attaque informatique et attaque informationnelle, et imposent une réponse à la hauteur.

Face à l'ampleur de ces attaques et à l'asymétrie des moyens actuels consacrés à la riposte, il pourrait être compréhensible de constater les dégâts sans agir. Or, pour protéger nos démocraties et nos économies, il nous semble que l'une des clés réside dans une mobilisation collective. Notre étude propose d'y contribuer en donnant des clés de lecture sur les moyens à mettre en œuvre. Ils sont aussi bien technologiques qu'organisationnels, et doivent se déployer à tous les niveaux de nos sociétés.

Alors que la propagande et le faux s'étendent à grande échelle, la défense de la vérité pourrait bien devenir le premier investissement économique du XXI^e siècle.

5.2. Sources, références et experts

Comité scientifique

- Tiziana Assenza — Professeure d'économie, Toulouse School of Economics
- Clément Bénése — Mathématicien, spécialiste de l'analyse de données, Opsci.ai
- Cyril Rollinde — Économètre, Citizing Consulting

Experts sectoriels

- Maya Atig — Directrice générale, Fédération Bancaire Française
- Claire Atkin — Co-fondatrice et CEO, Check My Ads Institute
- Ayman Awada — Head of Financial Services Industry, Sopra Steria
- Bruno Courtois — Conseiller Défense, coordinateur du Cercle Pégase, Sopra Steria
- David Colon — Historien et professeur, Sciences Po
- Alexandre Eich Gozzi — Head of Product Management Financial Services, Sopra Steria
- Ziad Gebran — Group Head of PR & Reputation, AXA
- Kévin Limonier — Professeur des Universités, Institut Français de Géopolitique (Paris 8) ; Directeur adjoint, GEODE
- Maud Quessard — Directrice du domaine « Europe, Espace Transatlantique, Russie », IRSEM (École Militaire)
- Jacob Sims — Visiting Fellow, Asia Center, Harvard University ; Visiting Expert on Transnational Crime, US Institute of Peace
- François Volpoet — Directeur Général France, Chainalysis
- Ilesha White — Director of Intelligence, Check My Ads Institute
- Mung Ki Woo — Chief Operations Officer, Financial Services, Sopra Steria Group

Bibliographie et sources

- Aghion P. et al., La crise mondiale de l'information représente une grave menace pour la prospérité économique et le progrès humain, *Le Monde*, sept. 2025
- Aitken B., Hoes E., Zhang J. et al., Prominent misinformation interventions reduce misperceptions but increase scepticism, *Nature Human Behavior*, 2024
- Alamsyah P. et al., Debunking disinformation on YouTube: a fact check on the 2024 Indonesian election, *Jurnal Studi Komunikasi*, 2024
- Baruchin R., 2024 Brand Crisis Round-Up - Part 2, *Cyabra*, 2024
- Braconnier C., Mayer N., Les dynamiques du décrochage civique illustrées par la hausse de l'abstention aux scrutins nationaux, 2024
- Cărlugea S., Calendarul alegerilor prezidențiale 2024. Costurile alegerilor, *Europa Libera Romania*, 2024
- Cooperating with fact-checkers, civil society, media and academia, *Commission européenne*, 2025
- Décisions australiennes ACCC 2024 : Qantas / Secure Parking / Mazda, *Australian Competition & Consumer Commission*, 2024
- Décisions australiennes ASIC 2024 : Mercer / Vanguard, *Australian Securities & Investments Commission*, 2024
- Décisions canadiennes 2024 : Sirius / Cineplex, *Gouvernement du Canada*, 2024
- Décisions SEC 2024 (greenwashing / ESG) : Keurig / WisdomTree / Invesco Advisers, *U.S. Securities and Exchange Commission*, 2024
- Derakhshan H., Wardle C., Les désordres de l'information : Vers un cadre interdisciplinaire pour la recherche et l'élaboration des politiques, *Conseil de l'Europe*, 2017
- Digital Trust Market (2025-2033), *Grand View Research*, 2025
- Dépenses en médicaments prescrits au Canada, 2023, *Institut canadien d'information sur la santé*, 2023
- Dinan S., Government spending to combat 'misinformation' jumped massively under Biden, *Washington Times*, 2024
- Durante R., Mastroiocco N., Minale L., Snyder J. M., Unpacking Social Capital, *The Economic Journal*, 2025
- Enquête de l'OCDE sur les déterminants de la confiance dans les institutions publiques - résultats 2024, *Éditions OCDE*, 2024
- Eudes R., Les entreprises sont-elles prêtes pour l'IA générative ?, *Deloitte*, 2025
- Facts not Fakes Tackling disinformation, strengthening information integrity, *OCDE*, 2024
- Feldman B., Ma O., How Google and YouTube are investing in fact-checking, *Google Blog*, 2022
- Gestion de l'infodémie sur la COVID-19, *ONU/OMS/UNICEF*, 2020
- Global Risk Report 2024, *World Economic Forum*, 2024
- Global trade in fake goods reached USD 467 billion, *OCDE*, 2025
- Grossman T., The Battle Against Brand Disinformation: Preparing the Communications Industry for 2025, *Truepoint*, 2025
- Horwitz J., Meta is earning a fortune on a deluge of fraudulent ads, documents show, *Reuters*, 2025

- *International Fact-Checking Network, State of the fact-checkers report, Poynter, 2025*
- *Kallioniemi P., Beyond Defence: A Proactive Strategy for the West in the Information Domain, ICDS Estonia, 2025*
- *La Commission met à disposition 16 millions d'euros de fonds pour soutenir le journalisme et l'éducation aux médias dans toute l'Europe, Commission européenne, 2024*
- *La Cour suprême ordonne la levée de la suspension du réseau social X au Brésil, Le Monde, 2024*
- *La Région européenne rapporte le plus grand nombre de cas de rougeole depuis plus de 25 ans, OMS/UNICEF Europe, 2025*
- *Little fires everywhere: How polarization is shaping the economy (and what to do about it), Allianz Research, 2024*
- *List of countries by stock market capitalization, Wikipedia, 2026*
- *Lutte contre les influences étrangères malveillantes. Pour une mobilisation de toute la Nation face à la néo-guerre froide, Sénat, 2024*
- *Measles and rubella weekly monitoring report, Gouvernement du Canada, 2025*
- *Michatowska A., Kubś J., Coining lies. Kremlin spends 1.5 Billion per year to spread disinformation and propaganda, Debunk.org, 2022*
- *Muckensturm B., Viginum, un service pour détecter les tentatives d'ingérence sur les réseaux sociaux, Radio France, 2021*
- *Navigating Apathy : A Data-Backed Analysis of Public Disengagement in Political and Economic Spheres, Yorkshire Popular Front, 2025*
- *Naviguer dans les désordres de l'information, Bureau du scientifique en chef du Québec, 2025*
- *New FTC Data Show a Big Jump in Reported Losses to Fraud to \$12.5 Billion in 2024, Federal Trade Commission, 2025*
- *Nguyen T. H., Factors Affecting Consumer's Online Shopping Behavior During the Covid-19 Pandemic, ResearchGate, 2023*
- *Observatoire européen des médias numériques (EDMO), Commission européenne, 2025*
- *Serrano J., What's the real cost of disinformation for corporations?, World Economic Forum, 2025*
- *Skibinski M., Special Report: Top brands are sending \$2.6 billion to misinformation websites each year, NewsGuard, 2025*
- *The economic cost of bad actors on the Internet, Fake News, CHEQ, 2019*
- *The economic cost of bad actors on the Internet, Fake Online Reviews 2021, CHEQ, 2021*
- *Trzun Z., Analyzing the cost and necessity of the fight against disinformation from the national security perspective, ResearchGate, 2024*
- *Turner L., \$5.5 Billion Stolen: Pig Butchering Scams Explode in Crypto, Cyvers Report Reveals, Crypto Ninjas, 2025*
- *Willens V., Estimating the Financial Costs of Measles Outbreaks, Johns Hopkins, 2025*

Direction de la publication :

Mathilde Richard

Direction de la recherche :

Thomas Delorme

Opsci.ai

Comité éditorial :

Mathilde Richard

Guillaume Ledit

Thomas Delorme

Aurélien Flaugnatti

Direction artistique :

Maxime Rocher

Contact presse :

Aurélien Flaugnatti

À propos de Sopra Steria

Sopra Steria, acteur majeur de la Tech en Europe, avec 51 000 collaborateurs dans près de 30 pays, est reconnu pour ses activités de conseil, de services et solutions numériques. Il aide ses clients à mener leur transformation digitale et à obtenir des bénéfices concrets et durables. Le Groupe apporte une réponse globale aux enjeux de compétitivité des grandes entreprises et organisations, en combinant une connaissance approfondie des secteurs d'activité et des technologies à une approche collaborative. Sopra Steria place l'humain au cœur de son action et s'engage auprès de ses clients à tirer le meilleur parti du numérique pour construire un avenir positif. En 2025, le Groupe a réalisé un chiffre d'affaires de 5,6 milliards d'euros.

Sopra Steria (SOP) est coté sur Euronext Paris (Compartiment A) - Code ISIN : FR0000050809

Pour plus d'informations, retrouvez-nous sur www.soprasteria.com/fr

**Le monde est tel que nous le façonnons*

Copyright tous droits réservés