Lutte contre les manipulations de l'information : le défi de la pluridisciplinarité

Le monde est tel que nous le façonnons*

Par leur influence sur les consciences, mais également par les défis qu'elles imposent à nos sociétés démocratiques, la désinformation et les manipulations de l'information sont une source majeure de déstabilisation classée par le World Economic Forum parmi les risques mondiaux prépondérants en 2024, aux côtés des risques climatiques et environnementaux.

En alliant un faible degré de sophistication et un large spectre de toxicité contaminant les sphères cognitives à l'échelle individuelle mais aussi les sphères informationnelles, sociales et politiques à l'échelle collective, elles figurent au rang des menaces les plus accessibles à leurs auteurs, tout en leur conférant une relative immunité.

Elles se placent donc au cœur de l'arsenal des attaques asymétriques et constituent pour nos démocraties un sujet de défense et un terrain d'engagement pour tous les acteurs mobilisés dans leur préservation et leur souveraineté.

Acteur majeur du numérique à l'échelle européenne, Sopra Steria est, par vocation, engagé à plus d'un titre dans la lutte contre ces phénomènes, en tant que premier partenaire du secteur public en France, mais aussi en tant que protagoniste de notre souveraineté numérique et industrielle auprès des écosystèmes de défense européens.

Sopra Steria : un engagement au-delà de l'écosystème cyber

Autour de Jean-Luc Gibernon et du général (2S) Bruno Courtois, Sopra Steria rassemble un pôle de collaborateurs et de partenaires experts pour approfondir la réflexion et accélérer la mise en place de solutions activables dans le cadre de la lutte contre la désinformation. Le groupe joue un rôle moteur au sein des initiatives les plus ambitieuses en France, en animant **le cercle Pégase** et auprès du **Pôle d'excellence cyber** mais également à l'échelle européenne, en participant au **Democratic Shield** auprès des institutions européennes.

L'une des grandes problématiques du phénomène est qu'il convoque, par son aspect protéiforme, une large diversité d'expertises et de disciplines. Il soulève des questions de libertés fondamentales et de droit, de relations internationales, de défense mais aussi de sciences cognitives en mobilisant des ressorts profondément individuels et humains.

Sopra Steria a donc pris le parti de relever **le défi de la pluridisciplinarité**, en élargissant autant que nécessaire les horizons du débat sur ce phénomène complexe et en rassemblant des experts issus des sphères économiques, politiques, académiques, médiatiques et réglementaires. Avec pour objectif d'initier, dès à présent, des solutions et des perspectives industrielles qui ne s'imposeront que par une analyse fine de la question dans ses différentes dimensions.

Cette approche s'est notamment illustrée lors de la conférence : **« Géopolitique numérique et cyber : les enjeux de la désinformation »** organisée par François Charles - Président de l'Institut de Recherche et de Communication sur l'Europe (IRCE), et qui a eu lieu à l'ECE (L'Ecole d'ingénieurs Campus de Paris).

> *Les manipulations de l'information figurent au rang des menaces les plus accessibles à leurs auteurs, tout en leur conférant une relative immunité.*

Des menaces plurielles, pas de réponse univoque

Pour répondre aux différents enjeux des manipulations de l'information, cette rencontre a réuni un panel d'experts issus d'horizons aussi divers que complémentaires :

Jean-Luc Gibernon

Vice-président "Entreprises" du Pôle d'excellence cyber et directeur du développement de Sopra Steria

Brunessen Bertrand

Professeure agrégée de droit public et titulaire de la Chaire Jean Monnet DataGouv sur la gouvernance des données

Sandrine Turgis

Maître de conférences en droit public et Co-directrice du Master 2 Affaires internationales à l'IODE CREC Saint-Cyr Coëtquidan

Julien Nocetti

Chercheur associé à l'IFRI et au centre GEODE

André Gattolin

Ancien sénateur et rapporteur d'une mission sur les influences étatiques extra-européennes

Jean-Noël de Galzain

PDG de Wallix et Président du groupement associatif Hexatrust

Sommaire

01 Désinformation, manipulations de l'information : des menaces ambigües aux effets délétères durables

02 Normes juridiques : contraintes ou opportunités pour les manipultaions de l'information ?

03 Les moyens de défense au service des luttes contre les manipulations de l'information : un défi stratégique, tactique et opérationnel

04 Conclusion : Une menace établie, un nouveau paradigme, de nouvelles ambitions

01 Désinformation, manipulations de l'information : des menaces ambigües aux effets délétères durables

Comme évoqué par Jean-Luc Gibernon, le cyberespace est un territoire avéré d'extension des conflits. Considéré depuis déjà plus de trois décennies par les armées comme un domaine de lutte, il est un territoire où s'exerce la conflictualité, dans sa dimension technique mais également dans sa dimension informationnelle.

Caractériser la menace

Les manipulations de l'information sont des menaces difficiles à définir de manière systématique. Contrairement aux attaques cyber, elles se caractérisent par de faibles niveaux de sophistication. Elles portent des messages qui ne sont pas nécessairement subversifs et jouent souvent sur les ambigüités en exploitant des failles dans l'opinion.

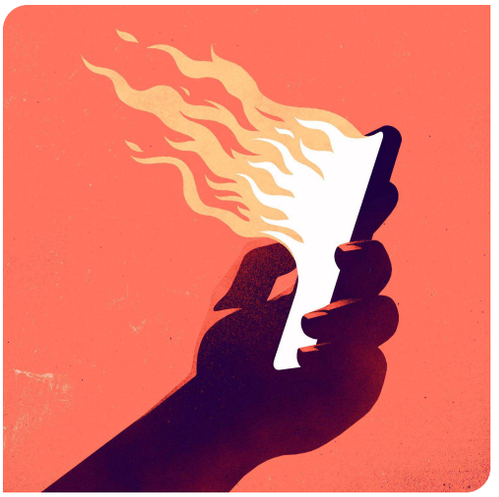
Le rôle de l'intelligence artificielle, en particulier de l'IA générative, est devenu prépondérant dans la génération, la diffusion massive et la viralité de ces contenus de désinformation qu'il s'agisse de textes, d'images ou de vidéos.

Ce sont donc **des menaces accessibles à de nombreux acteurs qui s'appuient sur des dispositifs relativement simples,** largement relayés via les réseaux sociaux, amplifiés par des bots générant de l'engagement artificiel et dont les victimes se font, parfois à leur insu, les vecteurs.

Ces attaques asymétriques dont l'origine reste artisanale et difficilement décelable, prennent de l'ampleur et entraînent des conséquences tangibles sur les processus de décision et les équilibres démocratiques. Déloyales par nature, **elles génèrent un certain niveau de nuisance et d'hostilité, sans nécessairement entrer dans le cadre d'un conflit ouvert.**

Dans le contexte géopolitique actuel, **elles s'immiscent dans les rivalités entre grands blocs :** Russie et Chine (dans une moindre mesure) contre les démocraties occidentales. Mais elles peuvent également s'insérer dans les interstices de conflits régionaux et de rapports avec les pays d'un « sud global » hétérogène et peu unifié.
Au-delà des acteurs identifiés sur ce terrain, il est intéressant de s'attarder sur les circonstances dans lesquelles ces menaces trouvent à s'épanouir.

> *Contrairement aux attaques cyber, les manipulations de l'information se caractérisent par de faibles niveaux de sophistication.*



Un terrain d'action privilégié : les fragilités de nos sociétés démocratiques

Ces manipulations s'attachent aux antagonismes du débat démocratique pour amplifier des clivages présents dans nos sociétés. C'est donc une affaire de rythme tout autant que de narratif, et l'on peut distinguer des effets variables selon les échéances, le contexte et les échelles.

A court terme et par des actions ponctuelles, elles peuvent entraîner des conséquences directes sur les processus de décision. En s'installant dans le moyen et le long terme, **elles interviennent en sapant la confiance du public dans les institutions, en alimentant les tensions entre communautés, entre États...**

En stimulant les débats et les rivalités politiques, les campagnes électorales favorisent logiquement ces attaques. Il faut cependant noter que la désinformation ne produira pas les mêmes effets selon les types de scrutins. **Les manipulations de l'information s'avèrent plus efficaces lors de scrutins bipolaires et circonscrits dans des périmètres nationaux ou régionaux.**

Les élections américaines présentent notoirement un risque dans un régime bipartisan avec un environnement médiatique relativement unifié et des clivages culturels et communautaires bien identifiés.

En stimulant les débats et les rivalités politiques, les campagnes électorales favorisent logiquement ces attaques.

Elles peuvent également s'avérer critiques lors de consultations ponctuelles et territoriales telles que le référendum sur l'indépendance de la Nouvelle-Calédonie en 2020, puis dans les troubles survenus en mai 2024 et sur lesquels pèsent de lourdes suspicions d'ingérences Azerbaïdjanaises.

Dans le cadre d'élections européennes en revanche, les effets de clivages profonds des opinions sur la durée sont plus à redouter que les effets d'interventions directes sur le processus démocratique pendant la campagne. Ce rendez-vous démocratique a convoqué cette année près de 400 millions de votants, issus de 27 pays s'exprimant en 23 langues, lors d'un scrutin proportionnel rassemblant des listes nationales très diversifiées. Des conditions qui rendent la production et la diffusion de narratifs ciblés extrêmement complexes et leurs résultats incertains.

Comme l'a rappelé André Gattolin, à l'échelle des institutions européennes, la plus grande vigilance doit prévaloir au cours de la séquence de désignation des « top jobs » (présidents de commissions, collège des commissaires, hauts représentants) dont les enjeux sont primordiaux et qui peuvent faire l'objet de campagnes de dénigrement ciblées.

02

Normes juridiques : contraintes ou opportunités pour les manipulations de l'information ?

Comme l'a précisé Julien Nocetti, les menaces informationnelles constituent une nouvelle « normalité » dans les relations internationales. Asymétriques, elles ciblent des démocraties qui, par souci moral et juridique, hésitent à s'autoriser les mêmes modes d'action ou de représailles.

Il s'agit néanmoins d'attaques caractérisées qui appellent des mesures de protection. D'un point de vue juridique, ces mesures s'appuient sur un édifice normatif sophistiqué qui doit, tout à la fois, garantir un droit fondamental - la liberté d'expression – et se prémunir contre son détournement et ses abus.

Liberté de communiquer, liberté d'informer : quel équilibre face à la menace ?

L'Union européenne présente la double particularité d'être une cible de menaces informationnelles et un espace institutionnel démocratique, garantissant la liberté d'expression.

Comme l'a rappelé Sandrine Turgis, la liberté d'expression s'articule dans la Charte des droits fondamentaux autour de deux éléments : **la liberté de communiquer et la liberté de s'informer.** Elle est garantie à plusieurs niveaux de la hiérarchie des normes juridiques : au niveau national en France, par la **Déclaration des droits de l'homme et du citoyen,** au niveau de l'Union européenne, par l'article 11 de la Charte des droits fondamentaux et par l'article 10 de la Convention européenne des droits de l'Homme. C'est enfin un droit universel reconnu par **la Déclaration universelle des droits de l'homme.** Ces dispositions garantissent la liberté de communiquer et de s'informer au-delà des frontières et sont le fondement du libre débat qui régit nos sociétés démocratiques.

L'Union européenne présente la double particularité d'être une cible de menaces informationnelles et

La première limite de ces normes est que les États démocratiques ne disposent pas d'instruments de contrainte proportionnée sur les États qui ne s'y conforment pas. Au sein de nos démocraties, l'édiction de normes restrictives peut également présenter un risque d'atteinte au principe de liberté d'expression ainsi qu'aux principes d'égalité et de proportionnalité.

Cette ambivalence entre la volonté de contrôler les dérives manifestent qui se manifestent notamment sur les réseaux sociaux, et la nécessité de préserver la liberté d'expression s'est particulièrement illustrée en France, lors du vote de la loi Avia du 24 juin 2020. Le texte visait à lutter contre les contenus haineux sur internet mais il a été très largement censuré par le conseil constitutionnel, au titre de **la liberté d'expression dans le champ duquel entre la liberté d'offenser et de choquer.**

un espace institutionnel démocratique garantissant la liberté d'expression.

On observe que la plupart des manœuvres de déstabilisation identifiées ne relèvent pas directement d'opérations de désinformation mais le plus souvent, de manipulations de l'information visant à exacerber des clivages existants.

— Faits ou opinion ?

La distinction entre information factuelle et opinion rencontre cette même problématique de limite, d'équilibre et d'interprétation.

Comme l'a rappelé Brunessen Bertrand, on observe que la plupart des manœuvres de déstabilisation identifiées ne relèvent pas directement d'opérations de désinformation mais le plus souvent, de manipulations de l'information visant à exacerber des clivages existants, comme observé en France lors des manifestations des gilets jaunes. Ce sont des actions circonscrites, diverses, multiples et dont l'aspect répréhensible fait appel à l'analyse et l'interprétation. Dans ce cas précis, **la frontière entre la liberté d'expression et les abus qui peuvent en découler, est difficile à établir.**

Sur notre continent, c'est le Conseil de l'Europe qui garantit les libertés fondamentales. Faute de moyens clairs ou contraignants, le Conseil de l'Europe assure des actions que l'on pourrait apparenter au « soft law », telles que la formulation de recommandations, des actions de sensibilisation à la liberté de la presse, le soutien aux journalistes par le biais de sessions de formation à de bonnes pratiques... Il peut également soutenir financièrement les médias menacés ou exilés, comme en Biélorussie, pour garantir la pluralité de la presse et l'usage des plateformes en ligne.

Dans le cas de litiges, il revient en dernier ressort à la CEDH (Cour européenne des droits de l'homme) de trancher comme dans le cas de RT France, dans lequel la justice européenne a rejeté le 27 juillet 2022 la demande de la chaîne d'annuler la suspension de sa diffusion.

— De la « Task Force » de la Commission européenne au Digital Services Act : autorégulation et genèse d'un droit contraignant.

A la suite des élections européennes de 2019 et des dérives observées lors des élections américaines, la Commission européenne a réuni une task force destinée à établir un code de bonne conduite et une auto-régulation des plateformes - non contraignante et aléatoire dans son interprétation. Dans son application, elle posait notamment la question de l'équilibre entre abus de liberté d'expression et censure par excès de précaution.

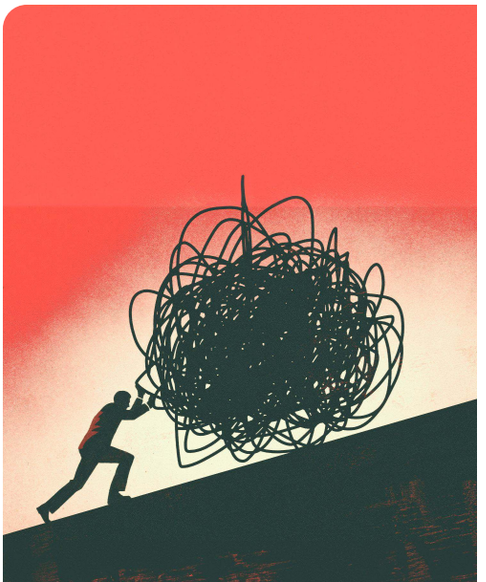
Le Digital Services Act (DSA) entré en vigueur en février 2024, introduit une logique plus coercitive sans changer la logique de responsabilité des opérateurs (fournisseurs d'accès internet, grandes plateformes, moteurs de recherche...) chargés de coopérer avec les autorités face aux contenus illicites pour protéger les utilisateurs, notamment mineurs. L'aspect contraignant est assuré par des mesures de sanctions graduées, en fonction de la taille des opérateurs, et il revient aux coordinateurs des services numériques présents dans chaque État membre, d'établir des sanctions sous forme d'amendes significatives ou, dans les cas les plus graves, de suspendre l'activité des plateformes.

Le rôle du DSA est également d'inciter les grandes plateformes américaines à établir des collaborations et des partenariats avec des acteurs européens ou locaux pour adapter la cybersécurité et la gouvernance des contenus aux contraintes de chaque pays.

Orienté vers les effets systémiques, il fait enfin appel à la vigilance des plateformes qui disposent de l'accès en temps réel aux données, pouvant indiquer la propagation de contenus de désinformation.

Le DSA est donc une initiative à suivre avec attention dans le cadre de la désinformation car il est le premier échelon d'un dispositif dédié avec des moyens d'action identifiés. A défaut de marquer un coup d'arrêt aux phénomènes, il permettra d'impliquer les plateformes et de constituer un socle évolutif.

Orienté vers les effets systémiques, le DSA fait appel à la vigilance des plateformes qui disposent de l'accès en temps réel aux données, pouvant indiquer la propagation de contenus de désinformation.



— Une mobilisation et une montée en tension très sensible auprès des législateurs nationaux et européens.

Les ingérences étrangères n'ont plus rien d'anecdotique pour les pouvoirs publics qui les appréhendent désormais comme une menace prioritaire. En France, **le 5 juin 2024, l'Assemblée nationale a adopté la proposition de loi visant à renforcer l'arsenal législatif contre les ingérences étrangères.** Cette initiative survient dans un contexte marqué par une cyberattaque en Nouvelle-Calédonie et des soupçons d'ingérences de l'Azerbaïdjan. La loi prévoit plusieurs mesures importantes telles qu'un registre national de l'influence obligatoire géré par la Haute Autorité pour la transparence de la vie publique (HATVP) et recensant les représentants d'intérêts étrangers en France. Elle introduit également le gel des avoirs de personnes, entreprises ou entités impliquées dans des activités d'ingérence.

Elle intègre enfin une surveillance algorithmique élargie prolongeant la logique appliquée à la lutte contre le terrorisme.

A l'échelle de l'Union européenne, la question des ingérences étrangères est devenue une réalité tangible à la suite du Qatar Gate au Parlement européen.

Abordée en 2022 et 2023 par la commission spéciale INGE du Parlement européen, la question des ingérences étrangères semble désormais inscrite durablement à l'agenda législatif et figure en bonne place dans les thématiques des élections européennes ainsi que dans le débat pour la présidence de la Prochaine Commission européenne qui en découlera.

A ce titre, Ursula von der Leyen, présidente de la Commission européenne et candidate, a annoncé le 14 mai 2024, son intention de créer un **"Bouclier démocratique européen"** dans le cadre de sa campagne de réélection.

Ce projet vise à **renforcer les capacités européennes de lutte contre les ingérences étrangères, en s'inspirant de l'agence française VIGINUM.** En s'appuyant sur les moyens développés par les états membres, elle a souligné la nécessité de créer des capacités communes au niveau européen par une structure dédiée à la lutte contre ces menaces et capable de se coordonner avec les agences nationales existantes.

Le Conseil européen a, quant à lui, lancé une task force temporaire pour centraliser la surveillance et le partage d'informations sur les tentatives d'ingérences, en vue de créer un système permanent après les élections européennes de juin.

Abordée en 2022 et 2023 par la commission spéciale INGE du Parlement européen, la question des ingérences étrangères semble désormais inscrite durablement à l'agenda législatif

03

Les moyens de défense au service des luttes contre les manipulations de l'information : un défi stratégique, tactique et opérationnel

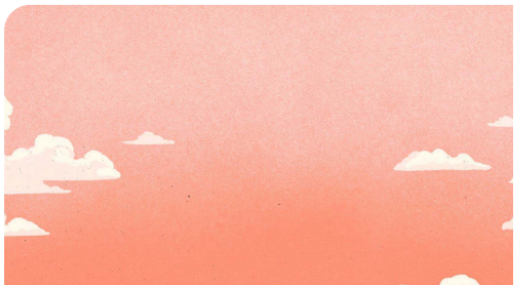
Les manipulations de l'information constituent un phénomène ancien qui a atteint une portée nouvelle et sans précédent, nécessitant des réponses stratégiques pour sauvegarder l'intégrité de nos institutions.

Dans le cadre des opérations (pro-)russes, on observe un dépassement de la « guerre hybride » dont l'une des caractéristiques repose sur l'ambigüité de l'origine de la menace.

— Quelle doctrine face à quelles opérations?

Comme l'a souligné Julien Nocetti, ces manipulations ont une double dimension : ce sont des actes délibérés, visant à nuire, mais ce sont aussi des actes clandestins dont la victime est censée ignorer l'existence.

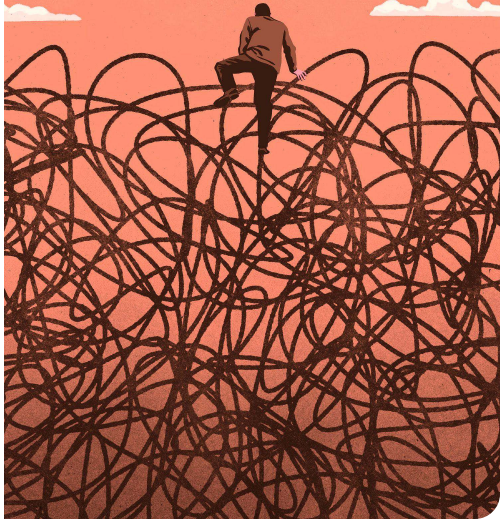
Dans le cadre des opérations (pro-)russes, on observe un dépassement de la « guerre hybride » dont l'une des caractéristiques repose sur l'ambigüité de l'origine de la menace. Un rapport de la VIGINUM sur l'activité d'un réseau (pro-)russe « Portal Kombat » révèle une attitude désormais assumée de l'agresseur qui ne dissimule plus l'origine de ses attaques, identifiables par l'hébergement des sites et les récits mobilisés. Parallèlement, les autorités françaises, habituellement



prudentes et discrètes sur la désignation des attaques, ont tendance à communiquer de manière plus ouverte sur le phénomène.

Pour apporter des réponses proportionnées, il convient de s'interroger sur l'impact de ces opérations et sur le seuil d'intervention nécessaire. **Faut-il s'engager dans une dynamique de dissuasion minimale ou dans une défense active impliquant des contre-mesures ?**

La perception de ces opérations par nos pouvoirs publics a évolué, notamment après les élections américaines. **Le cyber et l'informationnel étaient jusqu'alors des domaines scindés** et traités de manière différenciée. On constate **désormais une imbrication entre ces deux domaines avec une influence sur le champ des perceptions** générant une incertitude politique sur le long terme et créant des interférences auprès d'opinions publiques largement numérisées.



— L'enjeu industriel : créer une large convergence entre acteurs.

Dans la lutte contre la désinformation, Sopra Steria agit en catalyseur pour accélérer la convergence entre les pouvoirs publics à l'échelle nationale et européenne, et les écosystèmes d'innovation digitale constitués de startups, de PME et de grands acteurs industriels.

Au niveau de l'Union européenne, le groupe contribue notamment à l'initiative **Democratic Shield, portée par Make.org** et rassemblant une dizaine d'acteurs de la société civile, pour mettre en œuvre des stratégies de protection des élections contre les ingérences étrangères. Sopra Steria est en train de développer avec ses partenaires, pour beaucoup des start-ups, une solution de détection et de réaction de bout-en-bout aux attaques informationnelles, notamment générées à l'aide d'intelligence artificielle, à destination des entreprises.
Le dispositif s'appuie sur 4 principaux leviers :

- Analyser et vérifier la transparence, l'intégrité et la provenance des contenus en vue de les certifier.
- Cartographier et mesurer les tendances sur les réseaux sociaux et détecter le plus tôt possible les contenus présentant un risque élevé de viralité,
- Vérifier les contenus inconnus pour évaluer leur niveau de confiance et la véracité des contenus générés par l'IA (Fact checking),
- Developer la compréhension et la culture nécessaires à l'adoption des meilleures pratiques pour lutter contre les deepfakes et la désinformation.

A l'échelle nationale, c'est au sein de cet environnement, de ces startups et PME qu'il faut **aller puiser l'innovation qui permettra de créer les outils de lutte, tout en préservant notre souveraineté numérique.** A ce titre, il est essentiel de s'appuyer sur les ressources d'un écosystème cyber très agile et dynamique, rassemblé notamment autour du groupement associatif Hexatrust, représenté par Jean-Noël de Galzain.

> *Sopra Steria agit en catalyseur pour accélérer la convergence entre les pouvoirs publics à l'échelle nationale et européenne, et les écosystèmes d'innovation digitale*

> *Au-delà du cyberespace, les réseaux physiques liés à l'espionnage et à la contre-ingérence, jouent un rôle stratégique*

— Investir pour sauvegarder notre stabilité démocratique

Face à un problème désormais largement identifié, le manque de moyens en France est très sensible par rapport à nos homologues européens et nos adversaires. Le développement d'une approche pertinente nécessite des ressources substantielles et des effectifs dans des domaines jusqu'alors peu investis.

Au niveau des pouvoirs publics, une coordination accrue entre les différents services et administrations s'impose pour assurer une réponse cohérente et efficace à un phénomène protéiforme. Au-delà du cyberespace, les réseaux physiques liés à l'espionnage et à la contre ingérence, jouent un rôle stratégique. Une meilleure compréhension des différents secteurs d'ingérence et une collaboration soutenue avec les organismes internationaux spécialisés, seront essentielles pour mieux armer nos démocraties et assurer leur résilience.

Au-delà des grands événements internationaux, qui augmentent les risques à court terme, **l'enjeu est désormais de développer une stratégie globale sur le long terme,** face à une menace désormais implantée et durable.

04

Conclusion : Une menace établie, un nouveau paradigme, de nouvelles ambitions

Les manipulations de l'information ne sont pas une simple hypothèse alimentée par des événements anecdotiques, mais une menace constante qui polarise et fragmente les sociétés démocratiques.

Leur montée en puissance nous est rapportée chaque jour,
en Nouvelle-Calédonie, dans la perspective des Jeux Olympiques,
face aux positions politiques de nos dirigeants dans le conflit ukrainien...
Et si certaines d'entre elles peuvent paraître grossières,
leur multiplication dissipe les frontières entre faits et fictions,
et induit une défiance systématique dans l'opinion. Leur objectif :
amener les citoyens à douter de tout, y compris des faits.

Si plus personne ne croit en rien ou si chacun croit en ce qu'il veut,
notre capacité à débattre sur des fondamentaux communs disparaît,
c'est-à-dire l'essence même de notre démocratie.

Il est désormais acquis que nous entrons dans un nouveau paradigme où ces manipulations sont utilisées comme un arsenal conventionnel.

Bien que l'enjeu soit clairement identifié et suscite une mobilisation politique à l'échelle nationale et européenne, un dispositif unifié capable d'apporter une réponse concrète, proportionnée et coordonnée, reste à bâtir notamment d'un point de vue technologique.

C'est toute l'ambition portée par Sopra Steria avec le Cercle Pégase, véritable enceinte de décloisonnement et d'innovation, qui mobilise les compétences et capacités opérationnelles françaises pour lutter contre la désinformation.

Cercle Pegase

Le Cercle Pégase est un think tank dédié à la lutte informationnelle, dont l'ambition est de contribuer à la réflexion et la construction d'une stratégie française sur le sujet critique de la désinformation. Animée par le général (2S) Bruno Courtois, le think tank entend contribuer à la résilience de la Nation dans la lutte informationnelle.

https://www.linkedin.com/company/cercle-p%C3%A9gase/posts/?feedView=all