GT OPS
LUTTE CONTRE LES MANIPULATIONS DE L'INFORMATION

Avril 2024

LES JEUNES IHEDN

Réalisé par intelligence artificielle

REMERCIEMENTS

Les membres du groupe de travail tiennent à remercier chaleureusement toutes celles et ceux qui ont accepté d'échanger avec nous afin d'enrichir nos réflexions.

Toutes les personnes sollicitées pour des entretiens et entendues dans ce cadre l'ont été à titre privé. Leurs propos n'engagent pas leurs employeurs respectifs.

De plus, ce document constituant la synthèse des réflexions menées par le groupe de travail, **la participation de ces personnes n'implique aucune sorte d'approbation de leur part quant à son contenu.**

Nos remerciements vont enfin à toutes les personnes qui ont contribué de près ou de loin à ce rapport, et sans qui celui-ci n'aurait pu voir le jour.

MEMBRES DU GROUPE DE TRAVAIL

Olivier Boulnois, responsable du groupe de travail et rédacteur, membre du Comité Armée du Futur des Jeunes IHEDN.

Julie Brezisky, contributrice, membre du Comité Armée du Futur des Jeunes IHEDN.

Vianney du Manoir, rédacteur, responsable régional de la délégation Grand Est des Jeunes IHEDN.

Laure Fanjeau, contributrice, membre du Comité Cyber et du Comité Sécurité Intérieure des Jeunes IHEDN.

Jeanne Guillermic, rédactrice, membre du Comité Cyber des Jeunes IHEDN.

Victor Merlet, rédacteur, membre du Comité Moyen-Orient & Monde Arabe des Jeunes IHEDN.

Arthur Pons, rédacteur, responsable adjoint du Comité Risques & Intelligence économique des Jeunes IHEDN.

Paul Tournerie, contributeur, membre du Comité Asie-Pacifique des Jeunes IHEDN.

PROPOS INTRODUCTIF

Ce document n'est pas un rapport comme les autres.

Il est le produit d'un Groupe de Travail Opérationnel — « GT Ops » — des Jeunes IHEDN. Convaincus que la société civile a un rôle à jouer dans la **Lutte contre les manipulations de l'information (LMI)**, nous y formulons quelques propositions en ce sens.

Ce rapport est aussi la première pierre de notre projet. Persuadés du bien-fondé de leurs recommandations, et soucieux de les voir aboutir, nos membres ont en effet poussé leur engagement jusqu'à souhaiter les mettre en oeuvre eux-mêmes.

Les recommandations de ce rapport se veulent donc simples et très pragmatiques, afin de sensibiliser le plus rapidement l'audience la plus large possible.

Les enjeux sont devenus existentiels pour notre mode de vie et notre liberté d'expression. Tous concernés, **il ne tient qu'à nous de devenir des acteurs actifs de cette lutte**.

Olivier Boulnois

SOMMAIRE

Introduction

« La France face aux manipulations de l'information en 2024 »

Manipulations de l'information : une définition

« Premièrement, il s'agit d'une campagne orchestrée, impliquant des acteurs étatiques, mais aussi non étatiques.

Deuxièmement, elle passe par la diffusion massive de nouvelles fausses ou biaisées, fabriquées à dessein, diffusion virale grâce à son automatisation et à sa coordination.

Troisièmement, cette action stratégique répond à un objectif politique hostile : domination, interférence et déstabilisation des populations, des institutions et des États ciblés, afin d'infléchir leurs choix, de porter atteinte à l'autonomie de leurs décisions et à la souveraineté de leurs institutions. »

Jean-Yves Le Drian, ex-ministre de l'Europe et des Affaires étrangères
2018

Enjeu majeur du XXIe siècle, les manipulations de l'information sont devenues notre quotidien et fragilisent les démocraties. Depuis les élections présidentielles de 2016 et le scandale ***Cambridge Analytica***, cette menace, qui s'appuie autant sur nos faiblesses humaines — nos biais cognitifs — que sur de puissants moyens technologiques, a considérablement évolué. Plusieurs tendances de fond se dégagent, qui expliquent cette évolution.

L'essor considérable des technologies du numérique en premier lieu, qui offrent désormais la possibilité de cibler de façon très précise n'importe quel individu dans le but de lui présenter un contenu personnalisé afin de l'influencer. Le recours massif à ces technologies provoque un enfermement cognitif à l'échelle individuelle ainsi que **l'instauration d'un doute systématisé**. À l'échelle de la Nation, ce repli sur soi de chaque individu réduit considérablement l'espace public commun et polarise la société, fragilisant ainsi le gouvernement qui en est l'émanation.

Deuxième tendance inquiétante, la perte de souveraineté qui s'accentue d'année en année, entraînant la **réduction de notre libre arbitre** et de nos capacités de résilience nationales. La production, le stockage, le transfert et la consommation de l'information se font presque exclusivement à travers des produits provenant de géants étrangers du numérique, principalement américains ou chinois. Par le truchement de l'extraterritorialité du droit, ces mêmes acteurs sont soumis aux lois de leur pays qui contreviennent aux intérêts des citoyens européens, et entrent parfois en contradiction avec les lois locales dans l'espace européen.

La dégradation du contexte géopolitique mondial pour finir, avec l'instauration d'une contestation perpétuelle qui pousse grandes puissances et puissances émergentes à s'affronter en permanence dans le milieu cyber, sous le seuil de conflictualité. Les populations des adversaires sont alors directement visées par des **campagnes d'influence et de désinformation**[1].

Dans ce contexte, l'année 2024 sera particulièrement dangereuse pour les démocraties, en particulier pour la France. La moitié de la population mondiale est en effet appelée aux urnes cette année, tandis que les JO 2024 se tiendront à Paris à la mi-année. Il est plus que jamais nécessaire de **sensibiliser la population française** à la lutte contre les manipulations de l'information et de la faire **monter en résilience**.

I. Méthodologie : le format « GT Ops »

Ce groupe de travail s'est donné pour mission de créer des recommandations concrètes et applicables à l'échelle de l'association et des dispositifs permettant à tous les âges d'appréhender la question des manipulations de l'information et de ses enjeux. Cette prise d'initiative résulte d'un constat : en dépit de la richesse des rapports et des ouvrages spécialisés sur la manipulation de l'information et ses effets, les enjeux concrets et surtout les bonnes pratiques pour s'en prémunir demeurent abscons pour une couche significative de la population.

Ainsi, ce rapport ne vise en aucun cas à dupliquer les travaux académiques spécialisés sur le thème de la lutte contre les manipulations ni à reproduire des recommandations déjà évoquées, telles que celles mentionnées par le rapport Bronner, publié en 2022. S'inscrivant néanmoins dans la continuité de ces travaux, les réflexions portées par le groupe de travail ambitionnent de participer à l'effort collectif pour prolonger les recommandations déjà créées afin d'innover et de proposer des dispositifs applicables à l'échelle locale.

Le projet s'étend sur deux années : parmi les dispositifs mentionnés dans ce rapport, certains feront l'objet d'une application directe l'année prochaine au sein de l'association.

La première année consistait tout d'abord à réaliser un état de l'art sur cette thématique afin de proposer des recommandations complémentaires et adaptées aux nouvelles menaces. Dans un deuxième temps, il s'agissait de confronter les dispositifs imaginés à l'expertise de personnes auditionnées. La sélection des personnes auditionnées fut l'objet d'une attention toute particulière avec l'objectif d'inclure l'ensemble des acteurs mobilisés par cette question, quel que soit leur secteur d'appartenance. Enfin, dans un troisième temps, les rédacteurs ont été amenés à confronter leurs recommandations initiales aux remarques de nos interlocuteurs.

La définition du public ciblé par ces dispositifs a été longuement débattue dans l'équipe : était-il légitime ou non de se restreindre à une population jeune, compte tenu de notre association ? Il a finalement été décidé que le rapport s'adresserait en premier lieu aux jeunes, sans toutefois se réduire à cette catégorie. De ces réflexions émergea un autre point saillant : celui du degré de connaissance des enjeux concernant la question des manipulations de l'information. Si d'aucuns sont familiers avec les concepts de fausses informations et de désinformation, ils sont moins nombreux à comprendre les phénomènes qu'ils recouvrent précisément. Plus obscures sont encore les bonnes pratiques à mettre en place pour s'en protéger. L'édiction de bonnes pratiques se distingue de celles des contenus : il ne s'agit pas de dériver vers un « Ministère de la Vérité ». Cette initiative sera d'autant plus capitale lors de deuxième année qui mènera à l'application de certains dispositifs.

Ainsi, le corps du rapport se divise en deux volets. Tandis que la première partie vise à sensibiliser, notamment les plus jeunes, à la question des manipulations de l'information, la seconde se concentre sur des publics plus avertis afin de les doter de moyens pour s'en protéger.

II. Liste des personnes auditionnées

Marc-Antoine Brillant

Chef du Service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM)

Au sein du ministère des Armées, Marc-Antoine Brillant a d'abord exercé différentes fonctions opérationnelles, et a notamment commandé des unités de combat au Proche et Moyen-Orient. Plus récemment, il a assuré la fonction de chef des opérations d'un groupement tactique au Sahel. En 2018, il a rejoint l'Agence nationale de la sécurité des systèmes d'information (ANSSI) en tant que conseiller anticipation auprès de la direction générale, chargé des affaires opérationnelles et stratégiques, avant d'être promu sous-directeur adjoint Stratégie.

En 2021, après avoir dirigé la *Task Force* Honfleur, Marc-Antoine Brillant est désigné préfigurateur du service à compétence nationale VIGINUM et adjoint au chef de service. Le 6 octobre 2023, Marc-Antoine Brillant est nommé Chef du service de vigilance et de protection contre les ingérences numériques étrangères, auprès du Secrétaire général de la défense et de la sécurité nationale.

Paul Charon

Directeur du département « Renseignement, anticipation et stratégies d'influence » de l'Institut de Recherche Stratégique de l'École Militaire (IRSEM)

Docteur en Études politiques de l'École des Hautes Études en Sciences Sociales (EHESS), titulaire d'un MBA à HEC, Paul Charon est actuellement directeur du département « Renseignement, anticipation et stratégies d'influence » de l'IRSEM. Il enseigne à Sciences Po Paris, Sciences Po Saint-Germain-en-Laye, l'université Panthéon-Assas, l'IHEDN et l'université Rey Juan Carlos de Madrid. Avant de rejoindre l'IRSEM, Paul Charon a travaillé plus de dix ans en qualité d'analyste du renseignement puis de conseiller prospective au sein du ministère des Armées. Il a

été chercheur associé de l'antenne franco-chinoise en sciences humaines et sociales de l'université Qinghua à Pékin. Il est également l'auteur de nombreux ouvrages portant sur les stratégies d'influence chinoises, la guerre de l'information et les méthodes d'analyse du renseignement.

David Colon
Enseignant et chercheur à l'Institut d'Études Politiques de Paris

Professeur agrégé d'histoire, David Colon enseigne l'histoire de la propagande et des techniques de communication persuasive aux étudiants de l'Institut d'Études Politiques de Paris, Sciences Po Paris. Il est également chercheur au Centre d'histoire de Sciences Po. David Colon est l'auteur de nombreux ouvrages portant sur la propagande, les manipulations de l'information et les ingérences étrangères. Son œuvre ***Propagande*** a notamment été récompensée par les prix Akropolis 2019 et Jacques Ellul 2020. En 2023, son dernier ouvrage ***La Guerre de l'information. Les États à la conquête de nos esprits*** a été publié aux éditions Tallandier, faisant l'objet de nombreuses conférences participant à la démocratisation des manipulations de l'information.

Mickaël Vallet
Sénateur

Élu sénateur de la Charente-Maritime le 27 septembre 2020, Mickaël Vallet siège au Sénat aux côtés du groupe Socialiste, Écologiste et Républicain. Il y assure la fonction de Secrétaire du Sénat.

Sensible aux questions de défense nationale, il est membre de la commission des affaires étrangères, de la défense et des forces armées. Il préside également la commission d'enquête sur l'utilisation du réseau social TikTok, son exploitation des données et sa stratégie d'influence. Ce groupe de travail vise à révéler les particularités de ce média social et à formuler des recommandations sur son utilisation et son encadrement en France.

III. Définition des concepts mentionnés

Bots et botnets

Comptes de réseaux sociaux pilotés par des machines. On parle de botnets quand ces comptes fonctionnent en réseaux coordonnés.

Bulles de filtre

Concept développé par le militant Eli Pariser en 2012 désignant le phénomène de filtrage de l'information par les algorithmes de « personnalisation » des moteurs de recherche et des réseaux sociaux, qui ne proposent à leurs utilisateurs que les contenus les plus proches de leurs attentes. Par extension, désigne aussi parfois la construction de réalités alternatives individuelles sur mesure, et l'état d'enfermement cognitif qui en résulte.

Deep fake

Vidéos générées ou modifiées par intelligence artificielle (IA).

Désinformation

Contenu d'information ou ensemble de contenus d'information faux ou inexact(s), créé(s) avec l'intention délibérée d'induire les gens en erreur.

Fausse information (ou mésinformation)

Contenu d'information faux ou inexact, ayant ou non été délibérément créé et usé pour induire les gens en erreur.

Guerre informationnelle

La guerre informationnelle désigne l'ensemble des champs informationnels et des méthodes y étant appliquées. Cette guerre se révèle, comme beaucoup d'autres, correspondre à tous les critères de définition édictés par Clausewitz, quand bien même de nouvelles stratégies ont vu le jour conjointement à son apparition.

Influence numérique étrangère

Opération informationnelle menée dans l'espace numérique (web, réseaux sociaux) par un acteur ou un groupe d'acteurs étrangers à des fins d'influence.

Infox (fake news)

Contenu d'information fabriqué de toute pièce ou extrêmement inexact publié sur Internet et mise en forme de manière à ressembler à un contenu d'information grand public légitime.

Ingérence numérique étrangère

Un phénomène inauthentique affectant le débat public numérique qui combine :

- une atteinte potentielle aux intérêts fondamentaux de la Nation ;
- un contenu manifestement inexact ou trompeur ;
- une diffusion artificielle ou automatisée, massive et délibérée ;
- l'implication, directe ou indirecte d'un acteur étranger (étatique, paraétatique ou non-étatique).

Manipulations de l'information

Expression consacrée en France pour décrire des campagnes numériques impliquant des acteurs étatiques, basées sur « la diffusion massive de nouvelles fausses ou biaisées, fabriquées à dessein », dans un but de « déstabilisation des populations, des institutions et des États ciblés ». Le service VIGINUM lui préfère l'expression « Ingérences numériques étrangères », qui explicite l'origine de ces campagnes.

Ministère de la Vérité

Expression courante indiquant qu'un organisme reconnu par l'autorité publique déciderait de valider ou non les informations diffusées par des tiers (journaux, comptes sur les réseaux sociaux, chaînes de télévision). Lexique orwellien.

Propagande

Est composant d'une propagande tout élément permettant de jouer sur les leviers humains afin de rallier une partie de la population à une cause. Trop souvent perçue comme néfaste, la propagande peut aussi bien prendre forme pour des actions légitimes (droit de vote des femmes, démocratisation de l'art, …) qu'illégitimes (recrutement dans des organisations radicales, appel à la haine, …).

Trolls et usines à trolls

Individus réels qui relaient, saturent certains sites de commentaires, et/ou harcèlent.

IV. Brève analyse de la menace

Les manipulations de l'information s'inscrivent principalement dans le cadre de campagnes d'influence visant le champ des perceptions. Menées par des États, ces campagnes tentent d'imposer des narratifs dans l'opinion publique des États adverses ou alliés. Elles se caractérisent par un recours systématique aux technologies de l'information et de la communication (TIC) permettant la diffusion massive de contenus numériques dont certains sont « manifestement inexact[s] ou trompeur[s] »[2]. Qualifiées **d'ingérences numériques étrangères (INE)**[3] en France, elles impliquent de plus des moyens et des profils d'acteurs variés. Ce rapport, qui n'ambitionne pas de fournir une analyse exhaustive, n'en citera que quelques-uns afin d'illustrer les recommandations qui suivent.

1. Les moyens contribuant aux manipulations de l'information

Plusieurs techniques sont mises à profit pour tromper le consommateur de l'information. Certaines visent l'information en elle-même ; d'autres jouent sur les vecteurs de propagation des contenus numériques. Toutes sont pernicieuses car difficilement identifiables, même pour un internaute averti. Ces techniques font souvent appel à nos biais cognitifs dans le but de nous persuader ou nous pousser à partager l'information.

Ainsi, certains contenus cherchent à susciter des émotions négatives chez le lecteur — peur, colère — afin de l'inciter à réagir. D'autres sont tout simplement mensongers ou reposent sur des sophismes qui peuvent être difficiles à identifier dans le flux d'information continu auquel chaque individu est confronté. On assiste aussi régulièrement à des montages de contenus numériques anciens expurgés de leurs contextes spatio-temporels, de manière à créer artificiellement

des liens de corrélation inexistants[4]. Enfin, l'émergence d'outils grand public basés sur l'intelligence artificielle permet désormais la génération de textes, images et vidéos - les ***deep fakes*** - très réalistes, utilisées à dessein pour brouiller la frontière entre réalité et fiction et réduire la confiance de la population dans le numérique.
Du côté des vecteurs, la diffusion de l'information passe majoritairement par les réseaux sociaux, qui permettent de cibler et influencer rapidement des millions d'utilisateurs. Les ingérences numériques étrangères détournent de plus leurs puissants algorithmes à des fins manipulatoires.

Conçus pour proposer à la fois un accès personnalisé à l'information selon l'individu, et des capacités de micro-ciblage à des fins publicitaires, ces algorithmes exploitent les données personnelles de leurs utilisateurs. Le scandale Cambridge Analytica, qui éclata peu après les élections américaines de 2016, illustre le potentiel de nuisance lié à un usage détourné du micro-ciblage[5]. La personnalisation de l'expérience conduit de son côté à la création de réalités alternatives individuelles, les ***« bulles de filtres »***, dont l'effet pervers aboutit au repli sur soi et à la balkanisation des sociétés[6].

D'autres moyens sont régulièrement utilisés pour amplifier artificiellement la visibilité d'un contenu. Parmi eux, les ***« usines à trolls »***, telles l'Internet Research Agency (IRA)[7], qui paient des groupes d'individus pour relayer une information en ligne, commenter abondamment, voire harceler. On peut aussi citer le recours à des ***botnets***, comptes de réseaux sociaux pilotés par des machines, fonctionnant en réseaux coordonnés, dans le but de simuler l'activité d'un groupe important d'internautes.

2. Les acteurs derrière les manipulations de l'information

Les acteurs offensifs derrière ces campagnes peuvent quant à eux être répartis en trois catégories[8]:

- Les **acteurs étatiques**, composés des institutions et des médias directement dirigés par l'État ;
- Les acteurs « **non étatiques, semi-étatiques ou non officiels** », regroupant les entrepreneurs d'influence ou de désinformation en lien avec les États ;
- Les « **acteurs tiers** », relais d'influence dans la zone géographique ciblée qui facilitent, consciemment ou non, la pénétration des narratifs dans la population de cette zone.

Des acteurs secondaires contribuent cependant, parfois malgré eux, au succès des ingérences numériques étrangères. Les plateformes numériques en premier lieu, **moteurs de recherche** et **réseaux sociaux,** qui permettent respectivement d'indexer les contenus sur le Web pour les afficher sous forme d'annuaire interactif à l'utilisateur, et de partager de l'information au sein de communautés virtuelles. Selon l'Arcom, plus de la moitié du trafic internet en France en 2020 provenait ainsi de quatre fournisseurs, tous américains, dont Google et Facebook[9].

Si les algorithmes opaques de ces acteurs permettent la diffusion massive de contenus numériques, leur modèle économique privilégie de plus les contenus suscitant le plus de réactions.

Traditionnellement garants d'une information de qualité mais concurrencés par de nouveaux acteurs de l'information comme les réseaux sociaux et les influenceurs, les **journalistes** peuvent occasionnellement aussi être dupés. L'information fausse ou inexacte publiée gagne ainsi en crédibilité.

Enfin, tout individu qui réagit ou relaie des contenus numériques sans effectuer un minimum de vérifications se rend complice malgré lui de ces tentatives d'ingérences.

V. Les principaux acteurs liés à la LMI

De nombreux acteurs interviennent pour contrer cette menace au sein de l'espace informationnel français. Le réseau Internet utilisé pour les campagnes de manipulation de l'information étant par nature transnational, ces acteurs ne sont pas tous français. Certains sont étatiques ou supra étatiques, d'autres privés, d'autres enfin appartiennent à la société civile. Ici encore, nous ne mentionnerons que certains d'entre eux qui nous semblent pertinents pour la compréhension de ce rapport et de ses recommandations.

1. Les acteurs étatiques français

Plusieurs institutions françaises contribuent plus ou moins directement à la lutte contre les manipulations de l'information.

Le service **Viginum** en est l'émanation la plus visible aujourd'hui. Suite aux constats d'ingérences numériques étrangères lors des présidentielles américaines et françaises de 2016-2017, puis lors de la crise de la COVID, il est finalement créé en 2021 avec pour mission de « *détecter et de caractériser des ingérences numériques étrangères affectant le débat public numérique en France* »[10]. Dépendant du Secrétariat général de la défense et de la sécurité nationale (SGDSN), il est directement rattaché au Premier ministre.

Créée en 2017, le **COMCYBER** a pour principale mission *« la défense des systèmes d'information militaires ».* Pour ce faire, il assure une dimension de lutte contre les manipulations de l'information à l'encontre des troupes françaises à savoir *« la conception, la planification et la conduite des opérations militaires dans le cyberespace avec des actions de lutte information offensive (LIO) et de lutte informatique d'influence (L2I) »* [11]. Il est rattaché au ministère des Armées[12].

L'Arcom est l'organisme issu de la fusion entre l'**ARCEP, le CSA** et **l'Hadopi**, en 2022. Il a pour principales missions de *« veiller aux responsabilités démocratiques et sociétales des médias audiovisuels et des plateformes en ligne, de garantir le pluralisme des médias audiovisuels d'information et l'indépendance de l'audiovisuel public »*[13].

Récupérant les charges de l'ARCEP, elle doit aussi lutter contre *« toutes les formes d'entraves qui pourraient menacer la liberté d'échanger sur les réseaux, et s'intéresse à ce titre aux intermédiaires que sont les terminaux et les grandes plateformes internet »*[14].

Créée en 1978, la **CNIL** est « *le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits* »[15]. Elle a aussi un rôle de contrôle et peut sanctionner tout manquement au respect de la loi.

En France, c'est elle qui assure l'application du Règlement général sur la protection des données (RGPD), mis en place en 2018 au sein de l'Union européenne afin de lutter contre les abus d'exploitation de données personnelles par les fournisseurs de services numériques.

2. Les institutions européennes

La lutte contre les manipulations de l'information se retrouve aussi au niveau des instances européennes.

L'Agence de l'Union européenne pour la cybersécurité (**ENISA**) a pour mission de « *garantir un niveau élevé commun de cybersécurité dans toute l'Europe* »[16]. Créée en 2004, elle coopère avec les États membres et les organes de l'Union. Dans ce cadre, elle est amenée à contribuer à l'effort européen de lutte contre les manipulations de l'information, concomitant à celui sur la cybersécurité.

Le Service européen pour l'action extérieure (**SEAE**) a pour objectif de « *renforcer la cohérence et l'efficacité de la politique étrangère de l'UE, et d'accroître ainsi l'influence de l'Europe dans le monde* »[17].

Dès 2015, il se dote de ***task forces*** pour lutter contre les campagnes de désinformations extérieures : l'***East StratCom Task Force*** puis la ***Task Force South*** et la ***Western Balkans Task Force***. Le Plan d'action contre la désinformation — ***Action Plan against Disinformation*** — ajoute en 2018 un nouvel outil à l'action de lutte contre la désinformation du SEAE, avec la création d'un Système d'alerte rapide — ***Rapid Alert System***[18].

3. Les Centres européens et otaniens

Membre de l'OTAN et de l'UE, la France bénéficie des activités de celles-ci contribuant à la lutte contre la désinformation dans l'espace européen.

Le Centre d'excellence pour la cyberdéfense en coopération — ***CCD CoE*** — voit le jour à Tallinn en 2008.

Il a pour mission principale de soutenir ses nations membres et l'OTAN par une « *expertise interdisciplinaire unique* » dans le domaine de la recherche en cyberdéfense[19].

C'est en 2016, à Helsinki, que naît le Centre d'excellence européen pour la lutte contre les menaces hybrides — ***Hybrid COE***.

Son activité principale est de renforcer les capacités de ses États membres à « *prévenir et contrer les menaces hybrides* », dont la définition très large inclus les manipulations de l'information mais aussi « *les cyberattaques, l'influence ou à la coercition économique, les manoeuvres politiques secrètes, la diplomatie coercitive ou les menaces d'usage de la force militaire* »[20].

4. Les plateformes numériques

En 2018, dans la continuité du Plan d'action contre la désinformation, les efforts conjoints de l'Union européenne et des plateformes en lignes conduisent à un **Code de bonnes pratiques contre la désinformation**[21]. Les signataires de ce Code s'engagent dans une démarche volontaire à mieux contrôler leurs placements publicitaires, à fournir plus de transparence envers leurs utilisateurs et à agir contre les faux comptes et l'activité des bots sur leurs services[22].

Deux ans plus tard, la Commission européenne publie le ***Digital Markets Act (DMA)***[23] et le ***Digital Services Act (DSA)***[24], afin de réguler l'activité des plus grandes plateformes en ligne, considérées comme des « contrôleurs d'accès » à l'information sur les marchés numériques.

En réaction, les plateformes investissent dans des mécanismes de modération de leurs services et de leurs contenus dans l'espace numérique européen. En parallèle, des partenariats sont construits avec certains médias traditionnels afin de vérifier les contenus proposés — ***fact checking***.

Des services de signalement sont aussi proposés sur certains réseaux, ainsi que l'affichage d'informations supplémentaires sur l'auteur ou l'origine des contenus présentés, dans le cadre de mesures de transparence[25] [26].

5. La société civile française

> ***« L'autonomie d'appréciation et de décision de nos citoyens passe par la préservation de la sincérité du débat démocratique, face au phénomène émergent de manipulation de l'information par des puissances étrangères. Le rôle de la société civile reste essentiel, l'État pouvant fournir des outils pour lutter contre ces manipulations, notamment en période électorale. »***
>
> **Claire Landais, ex-Secrétaire générale de la Défense et de la Sécurité nationale**
> **2019**

Les Jeunes IHEDN sont la première association européenne et générationnelle sur les questions d'engagement, de défense et de sécurité.

Placée sous le double parrainage du ministre des Armées, M. Sébastien Lecornu, et du chef d'état-major des armées, le général d'armée Thierry Burkhard, elle regroupe, depuis 1996, les auditeurs jeunes formés par l'Institut des hautes études de défense nationale (**IHEDN**) et s'ouvre à l'ensemble de la jeunesse[27].

Portée par des membres très engagés dans la sensibilisation aux enjeux de sécurité et de défense, elle choisit cette année de mettre en valeur le sujet des manipulations de l'information.

Reporters sans frontières (RSF) est une organisation internationale à but non lucratif régie par des principes de gouvernance démocratique.

Fondée en 1985 à Montpellier par quatre journalistes, RSF est aux avant-postes de la défense et de la promotion de la liberté de l'information. Reconnue d'utilité publique en France depuis 1995, RSF est dotée d'un statut consultatif auprès de l'Organisation des Nations unies, de l'Unesco, du Conseil de l'Europe et de l'Organisation internationale de la Francophonie (OIF).

En 2018, Reporters sans frontières lance la **Journalism Trust Initiative (JTI),** une *« norme internationale [...] pour mettre en valeur et avantager un journalisme digne de confiance, dans le but de contrer la « concurrence directe de contenus manipulatoires qui prolifèrent dans l'espace digital : propagande, publicité, désinformation » ».*

V. Recommandations

AXE 1 : Sensibiliser aux manipulations de l'information

Pourquoi vouloir sensibiliser la société alors que des termes « fake news », « désinformation », « manipulation de l'information » submergent les espaces numériques et publics ? Serait-ce superfétatoire puisque plusieurs dispositifs viennent déjà s'ajouter à de nombreux discours sur le sujet ?

Cette multiplicité des termes pour désigner les manipulations de l'information témoigne tout à la fois du manque de consensus pour caractériser les phénomènes découlant des nouvelles technologies et de la rapidité avec laquelle l'espace numérique se renouvelle, notamment avec l'intelligence artificielle, entravant sa bonne compréhension. Effectivement, le changement de dimension affecte l'ensemble de la société requérant des adaptations par l'ensemble des publics, tels que les secteurs de la Défense, de la recherche scientifique ou encore celui de l'enseignement. Ces deux défis reflètent ainsi la nécessité de sensibiliser le plus grand nombre aux enjeux résultant des manipulations de l'information.

Certes, les utilisateurs peuvent avoir connaissance de certaines pratiques d'acteurs mais cela ne signifie pas qu'ils sont convaincus de leurs effets réels. Ce doute transparaît dans les tendances au relativisme : il peut naître du sentiment que les acteurs dans leur globalité participent à manipuler les informations ; que se cacherait derrière la lutte d'influence et informationnelle, une simple lutte de pouvoir ; que les opinions se valent toutes et que la connaissance de la vérité deviendrait inaccessible.

Cet attrait pour le relativisme découle en partie de lacunes dans la maîtrise des concepts de logique. L'attrition du déficit de cadres logiques chez les plus jeunes est un problème séculaire. Ce dernier se voit néanmoins appuyé par nombre de contenus numériques diffusant de fausses informations, avançant ainsi à peine dissimulées.

La vitesse de propagation de ces contenus ainsi que leur volume, combinés à la perte de confiance d'une partie de la population envers les institutions distillent des incertitudes néfastes pour la formation des jeunes sur le long terme.

À court terme, les événements d'importance capitale, en premiers desquels les Jeux Olympiques et Paralympiques de 2024, les élections européennes ainsi que présidentielles, requièrent une action urgente, visant le public le plus large possible.

C'est pourquoi les recommandations suivantes ont toutes trois l'ambition de s'adresser au plus grand nombre et d'interagir avec les participants. Les trois propositions complémentaires auront pour objectif de montrer les effets concrets des manipulations de l'information et de transmettre les éléments fondamentaux de logique nécessaire. Les recommandations 1 et 2 ciblent un public plus jeune sans s'y réduire, visant essentiellement à décrire les effets généraux concrets des manipulations de l'information tout en dotant les lecteurs de la distance critique raisonnable et plus particulièrement, des différences de valeur entre opinion, information, connaissance.

S'inscrivant dans la continuité des deux autres recommandations, la troisième vise à présenter les effets réels de la manipulation de l'information encourageant la transmission de contenus spécialisés portant sur les manipulations de l'information.

- **<u>Recommandation 1</u> : Mener une campagne visuelle de sensibilisation à la lutte contre les manipulations de l'information**

Diffuser des affiches avec un QR code à scanner menant à un kit d'information sur la lutte contre les manipulations de l'information.

Face à l'accès de plus en plus jeune des populations aux réseaux sociaux et à la massification des informations, dans un contexte national et international d'accumulation des crises, il semble central de sensibiliser les citoyens à la manipulation des faits et des informations dont ils peuvent être la cible. Les autorités françaises ont ainsi récemment mis en garde contre les tentatives d'ingérence étrangère d'acteurs internationaux, particulièrement pressantes à la veille des Jeux Olympiques de Paris.

Nous proposons ainsi la création d'un kit sensibilisant aux risques des manipulations de l'information, sous forme de questions / réponses : qu'est-ce qu'une fausse information ? qu'est-ce que la manipulation de l'information ? qui est touché par ce phénomène ? par quels moyens ce phénomène se répand-il ? Le kit contiendra des conseils pour s'informer via des sources fiables. Seront ainsi proposées une définition de « source fiable », une liste de médias et journaux considérés comme digne de confiance — journaux, chaînes de télévision, de radio, comptes Instagram, chaînes Youtube — tout en rappelant que cette liste n'est pas exhaustive, et que le public est toujours encouragé à vérifier une information en combinant les sources. Un tutoriel complètera le kit, permettant au public de tester la fiabilité d'une information (nature de la source d'information, nature de l'information, effet recherché, temporalité, ...).

Ce kit sera diffusé via une série d'affiches avec une identité visuelle impactante : couleurs, phrases percutantes, composition iconographique qui attire le regard (reprise du format « ***I want you*** » avec le doigt pointé vers le public), en comprenant éventuellement des personnalités ou des influenceurs numériques proches des jeunes.

Ce format visuel a pour objectif d'interpeller les jeunes et de les inciter à flasher le QR Code. Ces affiches seront accrochées en ville dans les espaces dans lesquels l'affichage est libre, dans les collèges, lycées et universités, ainsi que dans les centres sportifs et Maisons de la jeunesse sous réserve d'un accord des collectivités locales concernées.

- **<u>Recommandation 2</u> : Éveiller les plus jeunes à ces enjeux grâce à un manga**

Publier un manga dans lequel le lecteur pourra s'identifier à un jeune héros confronté à des exemples concrets de manipulations de l'information.

En 2023, 39,6 millions d'exemplaires de mangas ont été vendus en France selon l'institut GfK. Bande dessinée japonaise, le manga est extrêmement populaire auprès des jeunes lecteurs et peut être lu dès l'âge de 6 ans, d'où l'intérêt d'utiliser ce support pour sensibiliser une population exposée de plus en plus jeune aux manipulations de l'information. Cette recommandation aura vocation à être déclinée selon l'âge du lecteur, et prendra en compte sa maturité et sa conscience du danger environnant.

Des études ont ainsi montré que les enfants (entre 6 et 10 ans) apprécient les mangas simples et colorés contrairement aux préadolescents (entre 10 et 14 ans) qui préfèrent lire des histoires d'aventure plus complexes avec des personnages et des paysages plus travaillés. Passé le seuil de l'adolescence (entre 14 et 18 ans) et l'arrivée dans la période post-adolescence (entre 18 et 25 ans), le dessinateur aura un éventail plus large, tant sur le choix des couleurs que des formes. Il est toutefois primordial de conserver en mémoire que, même si la forme est très importante dans un manga, dans notre cas, le fond l'est encore plus.

L'accès aux informations diffère selon l'âge, le niveau scolaire de l'enfant et son appétence vis-à-vis du monde qui l'entoure. Un personnage qui grandit en même temps que le lecteur permettrait donc à ce dernier de mieux identifier les situations qu'il pourrait rencontrer au cours de son adolescence jusqu'à la vie estudiantine.

Ainsi, il pourrait y avoir plusieurs tomes composés de la même façon : une histoire, un lexique, un récapitulatif des bons gestes à connaître, une bibliographie avec la liste des sites à clés selon ses besoins, des tests ludiques avec les réponses et des rappels.

Le scénario devrait être basé sur l'actualité et sensibiliser sur le mode de la manipulation des informations (absence ou faible modération sur certains réseaux sociaux, effets de « bulles de filtres » importants sur certains réseaux sociaux).

- ***Tome 1 - lecteur ayant entre 6 et 12 ans ou entre 10 et 12 ans***
  Premier surf sur la toile.
- ***Tome 2 - lecteur ayant entre 12 et 14 ans***
  Premières recherches sur la toile seul(e) ou avec des amis.
- ***Tome 3 - lecteur ayant entre 14 et 18 ans***
  Accès aux forums de discussion et aux réseaux sociaux.
- ***Tome 4 - lecteur ayant entre 18 et 25 ans***
  Recherches universitaires, accès à un flux d'informations avec le risque d'être la cible de manipulation informationnelle et de véhiculer, malgré soit, de la désinformation.

L'histoire doit évoluer selon l'âge du lecteur, comme l'expliquait David Colon dans son entretien. Nous pourrions dans un premier temps nous pencher sur le matraquage d'informations erronées et fausses, puis sur le problème de la confiance accordée par le lecteur à la source de l'information.

La conception du manga ne doit pas être prise à la légère car il y va autant de la crédibilité du message que nous souhaitons véhiculer que de l'image des Jeunes IHEDN sur un sujet intergénérationnel et d'actualité. Un partenariat pourrait être envisagé avec les responsables du Trinôme académique, qui sont régulièrement au contact de nos cibles, ou encore avec l'Éducation nationale.

- **<u>Recommandation 3</u> : Produire des publications de vulgarisation scientifique pour rendre accessibles les concepts les plus complexes**

Permettre à des individus conscients et intéressés par les questions de manipulation de l'information de consulter des contenus issus d'études scientifiques sous différents formats afin de développer leur socle de connaissance à ce sujet.

Constatant la faible quantité de contenus de vulgarisation scientifique grand public en langue française sur le sujet, Les Jeunes IHEDN se proposent d'y remédier en s'associant à différents acteurs.

Il ne s'agit pas ici d'inventer de nouveaux concepts, ni de porter un discours partisan sur le monde informationnel. Plutôt, il est question de rendre accessible des connaissances techniques qui sortent rarement du vase clos scientifique et qui peuvent de ce fait être mystifiées. Pour ce faire, nous privilégions trois formats qui, graduellement, impliquent de plus en plus les agents pour les motiver à passer de « personne intéressée » à « personne engagée ».

Chaque mois, un cycle est ouvert sur un thème de la LMI (les ingérences étrangères dans les élections nationales par exemple). Trois formats se relaient, et se nourrissent mutuellement.

En premier lieu, une série de courts articles. Chaque cycle comporterait entre cinq et dix articles de façon à publier un voire deux articles par semaine afin de maintenir une présence. Le format court convient à notre objectif car sa production et sa consommation demandent un effort moindre que de plus longs articles. Ensuite, adossée au cycle d'articles, une série de podcasts. Dans un format d'environ dix minutes, un expert est accueilli par un hôte pour expliquer simplement et à l'aide d'exemples un de ses derniers travaux. L'idéal serait de créer un (voire deux) podcasts par cycle. Enfin, pour conclure le cycle entamé en début de mois, une conférence mensuelle avec un ou plusieurs chercheurs

permettrait de mobiliser plus concrètement les personnes intéressées par la LMI, et de les encourager à participer aux actions évoquées dans les recommandations suivantes.

La diffusion des premiers contenus, et des comptes rendus des conférences établis à la discrétion des intervenants, bénéficierait de coopération avec d'autres acteurs engagés dans un projet similaire au nôtre. Dans ce cadre, l'association [DEMOS], média en ligne sur Instagram et Facebook composé de plusieurs comptes spécialisés et engagé dans la démocratisation de l'information, pourrait devenir un partenaire de choix. De même, l'association Open Facto, avec sa spécialisation en renseignement d'origine sources ouvertes (***OSINT***), pourrait être à la fois un partenaire dans la conception et la production des contenus que nous avons évoqués.

Un premier plan sur dix mois pourrait être établi au plus tôt, afin de lancer le projet courant septembre 2024.

AXE 2 : Faire monter en résilience par la diffusion de bonnes pratiques

Dans cette seconde partie, les recommandations s'adressent à un public déjà conscient de la menace que représentent les manipulations de l'information, et sensibilisé aux enjeux du combat visant à contenir leurs effets sur les populations. Dans un contexte de recomposition géopolitique et de tensions accrues à l'échelle nationale et internationale, divers acteurs (adversaires, compétiteurs, opposants) mènent des campagnes de manipulations de l'information. Utilisant des méthodes toujours plus sophistiquées, ils conduisent ainsi les spécialistes de diverses disciplines à étudier la réémergence ou *a minima* le renouvellement de ces pratiques malveillantes. À ce titre, le rapport codirigé par le CAPS et l'IRSEM alerte sur les nouvelles pratiques de nos adversaires stratégiques, bénéficiant de l'essor du cyberespace et des réseaux sociaux. La crise sanitaire et l'invasion russe en Ukraine ont constitué des cas concrets pour analyser ces manipulations de l'information à des fins d'influence, ainsi que leurs effets.

La publication de multiples ouvrages et rapports sur la désinformation et les ingérences numériques ont facilité la mise à l'agenda politique des questions de manipulations de l'information. La création de dispositifs pour y remédier, tels que des boîtes à outils, s'est ensuivie. Le programme ***Facts4All MOOC: Schools tackling disinformation*** (2022) et le kit pédagogique ***Combattre et identifier la désinformation*** (2021) à destination des professeurs, respectivement financés et conçus par la Commission européenne, s'inscrivent dans cette perspective.

L'éducation aux médias et à l'information (EMI), discipline obligatoire depuis 2021, se décompose en divers dispositifs nationaux tels que la semaine de la presse et des médias à l'École, un concours et des supports à destination des professeurs. Fait notable, la société civile s'est également saisie de la question en diffusant des contenus de vulgarisation ou bien en créant des plateformes de réfutation.

Toutefois, ces dispositifs rencontrent d'une part, des limites éthiques, et d'autre part, des limites dans leur application, se confrontant alors à un manque d'efficacité, quand ils ne se montrent pas contre-productifs. De ce fait, les publics avertis quant aux enjeux des manipulations informations se multiplient, sans pour autant disposer de méthodes, techniques et procédures concrètes pour s'en prémunir. Dès lors, les recommandations de cette partie ont pour objectif de doter les publics, avertis à des divers degrés, de nouveaux moyens de lutter contre les manipulations de l'information.

Par ailleurs, l'éducation aux médias se réduit aux dangers et risques liés au numérique : les risques en matière de fausses informations et d'atteinte réputationnelle, ou encore la nécessité de mettre en place des bonnes pratiques d'hygiène informatique. Cette tendance entraîne dans certains cas un effondrement de la confiance dans les médias, ainsi qu'une obsession pour le relativisme. Cette approche centrée sur les aspects techniques néglige les dimensions culturelle et individuelle selon le médiateur au numérique Vincent Bernard, spécialisé en éducation aux médias.

Il est effectivement nécessaire d'étudier la manière dont les audiences s'approprient les contenus à travers ces technologies. S'appuyant sur les travaux qui analysent les contenus de vulgarisation luttant contre la désinformation, l'engagement des audiences s'accroît, non selon des critères institutionnels, mais bien par l'adoption de normes et valeurs propres aux chaînes. C'est pourquoi il convient d'admettre une approche interactive et ludique pour l'ensemble de nos recommandations.

- **<u>Recommandation 1 :</u> Former les publics sensibilisés aux bonnes pratiques contre les manipulations de l'information**

Proposer des ateliers pour former le grand public aux bonnes pratiques dans le domaine informationnel.

Le cyberespace a conduit à trois ruptures stratégiques selon Marangé et Quessard : un renouvellement de la notion d'espace-temps sur le théâtre des opérations, une saturation des espaces de l'information et la fin de la primauté américaine en matière technologique. De ces trois ruptures stratégiques, résulte le défi de la transmission des connaissances. L'effet de bulles de filtres, conjugué à la saturation de l'espace informationnel et aux pratiques malveillantes visant à cibler directement l'esprit humain, fragilise la transmission des informations.

Parmi l'ensemble de la population, les jeunes utilisent davantage les réseaux sociaux que les autres canaux de communication : en 2018, 71 % des 15-34 ans déclarent utiliser quasi quotidiennement les réseaux sociaux pour s'informer. Or, ne disposant pas des outils de logique d'esprit critique nécessaires, ces jeunes apparaissent plus démunis. Par ailleurs, la jeunesse ne constituant pas un groupe monolithique, les jeunes entretiennent une relation à l'information différente selon leurs caractéristiques socio-culturelles. À ce titre, les populations les plus défavorisées seraient plus enclines à la non-information qu'à la désinformation d'une part, tandis que les étudiants issus des milieux les plus favorisés sélectionneraient leur contenu dans une démarche de distinction sociale.

Néanmoins, l'âge ne constitue pas l'unique déterminant : à cet égard, les plus de 65 ans peuvent être des catalyseurs de fausses nouvelles plus puissants que les jeunes. En outre, nombre d'acteurs interagissent avec le champ informationnel en produisant du contenu en ligne, à l'instar des médias. Or, les producteurs de ces contenus ne disposent pas nécessairement du temps et des capacités pour se former aux risques de manipulations de l'information.

C'est pourquoi, les recommandations ci-dessous ciblent en priorité deux types de publics : les Jeunes, consommateurs d'une part, les entreprises et les médias, créateurs de contenus, d'autre part.

- **<u>Recommandation 1.a :</u> Investir le secteur éducatif**

Proposer des ateliers en milieu scolaire et professionnalisant pour former interactivement à la détection et à la lutte contre les manipulations de l'information.

Des ateliers autour des manipulations de l'information auront vocation à s'adapter à un public large d'étudiants, au sein de collèges, lycées et écoles de journalisme. Le mode interactif propre à ces ateliers facilitera l'assimilation des connaissances, ayant pour objectif de renforcer la résilience des élèves face aux risques que représentent les manipulations de l'information, développer leur esprit critique et promouvoir un comportement responsable en ligne.

Deux exemples d'ateliers ont d'ores et déjà été envisagés : un jeu de rôle inspiré du « loup-garou » et un concours ouvert à plusieurs classes de lycéens.

Le jeu de rôles inspiré du « loup-garou » aura pour objectif de susciter des débats entre les participants afin qu'ils détectent ensemble des manipulations de l'information et cultivent leur esprit critique. Au travers de l'incarnation de divers rôles tels que le Manipulateur de l'information (équivalent du Loup-garou), l'Utilisateur (équivalent du Villageois), la Chercheuse (équivalent de la Sorcière), le Concepteur d'applications de rencontre (équivalent du Cupidon, pouvant choisir son algorithme) ; le participant sera sensibilisé aux modes opératoires des attaquants dans le domaine informationnel. Ce jeu interactif et collaboratif permettra la stimulation intellectuelle et le partage d'expériences entre les joueurs autour des manipulations de l'information.

Le concours visera quant à lui à faire travailler des élèves en groupes pendant plusieurs mois sur un sujet lié à la LMI, avant de présenter leur projet devant les autres groupes et un jury. La présence d'acteurs publics dans ce jury serait l'opportunité d'un dialogue privilégié avec la jeunesse, participant à restaurer le lien de confiance entre la société civile et les institutions. Étant donné la différence de compétences entre les classes de collèges, lycées et l'enseignement supérieur, le concours pourra regrouper plusieurs projets aux exigences et intérêts adaptés. L'objectif consiste toujours à inciter le plus grand nombre de groupes de jeunes à s'impliquer dans la lutte contre les manipulations.

Dans la perspective de pouvoir organiser ce type d'interventions à plusieurs reprises, il s'agirait d'adapter ces ateliers aux divers événements citoyens. À titre d'exemple, ces ateliers pourraient être intégrés aux formations des SNU, des Cycles Jeunes et des divers comités des Jeunes IHEDN.

- **<u>Recommandation 1.b :</u> Investir les sphères entrepreneuriales et médiatiques**

Établir, au sein d'entreprises et de médias, des extensions du jeu de rôles pour former interactivement à la détection et à la lutte contre les manipulations de l'information.

Les différents scénarios auront vocation à s'adapter à un public appartenant à un autre secteur. En s'appuyant sur le jeu de rôles susmentionné, les participants seront amenés à incarner différents personnages afin de refléter les modes opératoires des attaquants sur la couche informationnelle dans leur secteur particulier.

S'inscrivant dans la lignée de la précédente recommandation, les suivantes s'adressent à un public averti maîtrisant les méthodes, les techniques ainsi que les procédures propres aux campagnes de désinformation. Sous contrainte de temps, les participants seront obligés de proposer des solutions afin de défendre une organisation contre les manipulations de l'information.

- **<u>Recommandation 2 :</u> Organiser un atelier immersif visant à doter les publics avertis de techniques et méthodes défensives face aux manipulations de l'information**

Établir des scénarios pour un public averti mais ne disposant pas des compétences et des connaissances pour se défendre concrètement contre les manipulations de l'information. Cet atelier simulera une attaque ciblée afin que les participants acquièrent de manière concrète et efficace les bonnes pratiques.

Sur le modèle des « ***Red Team / Blue Team*** » et des jeux de guerre « ***Wargames*** », les participants devront suivre un scénario pour apprendre à gérer une attaque informationnelle ciblant une entité. Les joueurs seront invités à prendre conscience des risques d'une telle attaque, ainsi qu'à détecter et à analyser les effets de manipulations de l'information. Des contre-mesures pour y remédier pourront également être proposées. Les scénarios utilisés pourront s'appuyer sur les notes diffusées par la Direction du renseignement et de la sécurité de la Défense (DRSD) et le ministère des Armées. Dans le but d'élargir le public cible, ils pourront par ailleurs s'inspirer de scénarios historiques de LMI tels que la diffusion du SIDA ou la guerre en Irak. Des partenariats pourront être conclus avec des administrations publiques ou bien des sociétés privées.

Deux formats peuvent être envisagés selon le nombre de participants. Si le nombre est réduit (au maximum : six acteurs), les participants seront réunis dans une même équipe bleue défensive jouant contre le plateau incarnant les attaquants. Si le nombre de participants est plus élevé et que leur expérience est jugée suffisante, deux équipes s'affrontent : une équipe dite « bleue » doit formuler des réponses à l'encontre d'une équipe « rouge » mène l'attaque.

Il s'agira d'un format long d'une journée pour doter les personnes d'outils et de bonnes pratiques afin de faire monter les joueurs en compétences. S'appuyant sur le jeu de rôles (recommandation 2), cet atelier immersif comprendra des règles

supplémentaires. La réponse apportée par l'équipe bleue dépendra des connaissances des participants, mais également du niveau de préparation de l'entité supposée et de la maturité de l'attaquant.

L'exercice s'adressera à des étudiants et jeunes professionnels déjà sensibilisés, c'est-à-dire connaissant les modes opératoires des attaquants les plus connus et sachant identifier certaines campagnes de manipulation de l'information. Cet atelier visera à doter les participants des techniques défensives, et d'acquérir les bonnes pratiques à appliquer.

Cet atelier interactif de mise en situation permettra aux participants de s'approprier les bonnes pratiques dans un cas concret, plus efficacement que dans le cadre d'une présentation simple. Par ailleurs, cette recommandation vient compléter les précédentes (formation en ligne, sensibilisation par manga, campagne de sensibilisation sur les réseaux, etc.).

De fait, son objectif premier ne consiste pas à toucher directement le plus grand nombre, mais bien à faire de cet atelier de simulation, visant à être reconduit et pérennisé par l'association, une référence dans le domaine de la LMI. L'objectif consisterait à diffuser cette mise en situation à un plus large public (particuliers, classes scolaires, universités, entités souhaitant organiser leur propre formation sur l'appui d'un jeu à finalité pédagogique). Cette recommandation complémentaire demeure hypothétique, en raison de son coût, son usage et de l'intérêt incertains des publics ciblés.

Tandis que cette deuxième recommandation vise à analyser et à contenir des campagnes de manipulation de l'information, la troisième ambitionne de doter les participants de capacités pédagogiques, dans le but d'en faire des vecteurs de transmission de connaissances.

- **<u>Recommandation 3</u> : Former les Jeunes IHEDN pour agir face aux manipulations de l'information**

Faire monter en compétences et en connaissances les membres de l'association dans le but de les armer face aux manipulations de l'information.

Des ateliers de formation contre les manipulations de l'information au sein des Jeunes IHEDN auraient pour mission de renforcer la dimension opérationnelle des membres sur ces thématiques. Dans le cadre des événements organisés par l'association, la mise en place de mesure en amont et en aval desdits événements et l'adoption des bons réflexes par les membres permettrait d'instaurer un cadre attentif à ces thématiques. D'autant plus que l'association des Jeunes IHEDN, par les sujets qu'elle traite, ses partenaires et son positionnement transversal sur les questions de défense, se doit d'être armée face à la question de la manipulation de l'information.

De fait, il pourrait être intéressant d'étoffer l'offre de formation interne des Jeunes en proposant un volet concernant la lutte contre les manipulations de l'information. Cette initiative pourrait prendre la forme d'ateliers, pilotés par des membres ou par des intervenants extérieurs, permettant la montée en compétences des membres. Lors de ces ateliers, des formations en recherche en source ouverte (ROSO) ou l'étude de campagne de manipulation de l'information dévoilée par le passé pourraient être proposées aux membres.

De plus, il serait pertinent de favoriser le développement d'une maîtrise sur des outils et des logiciels, tel que la matrice DISARM, récemment traduite en français par Viginum, organisme qui « ***a fait le choix d'exploiter cette matrice dans une volonté de standardisation des pratiques et de partage de la connaissance au sein de la communauté de la lutte contre les manipulations de l'information (LMI)*** ». Une connaissance technique de cette matrice permettra aux Jeunes IHEDN de s'inscrire au cœur de cette communauté, permettant de renforcer les possibilités de partenariat.

PLACE À L'ACTION !

Vous êtes intéressés par nos travaux ? Vous souhaitez nous aider dans la mise en place de nos recommandations ? Vous avez des idées à nous soumettre ?

N'hésitez pas à nous écrire : **gtops.lmi@jeunes-ihedn.org**

Notes de bas de page

[1]InterStats. *Indurant la sécurité et délinquance en 2022 : une première photographie - Interstats Analyse N°54*. Ministère de l'Intérieur et des Outre-mer, janvier 2023.

[2] SGDSN. *Service de vigilance et protection contre les ingérences numériques étrangères* [En ligne]. SGDSN, 17 novembre 2022 [Consulté le 23/03/24]. Disponible sur : https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

[3] Ibid.

[4] AFP France « Non, cette série de photos ne montre pas le sauvetage mis en scène d'une petite fille à Gaza ». *AFP Factual* [En ligne], 30 octobre 2023 [Consulté le 23/03/24]. Disponible sur : https://factuel.afp.com/doc.afp.com.33ZD4H8

[5] Jeangene Vilmer, Jean-Baptiste et al. *Les Manipulations de l'information : un défi pour nos démocraties*. Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, août 2018, p. 148.

[6] Bulnois, Olivier. *La souveraineté numérique face aux manipulations de l'information en France de 2011 à 2021*. Université Jean Moulin Lyon III, mémoire de master, 2021.

[7] « The Internet Research Agency (IRA) carried out [...] a social media campaign designed to provoke and amplify political and social discord in the United States », *in :* U.S. Department of Justice. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* [En ligne]. DoJ, Vol. I à III, mars 2019 [Consulté le 23/03/24]. Disponible sur : https://www.justice.gov/archives/sco/file/1373816/download.

[8] Audinet, Maxime. « L'appareil de désinformation russe ». *Aerion 24* [En ligne], 29 janvier 2024 [Consulté le 23/03/24]. Disponible sur : https://www.areion24.news/2024/01/29/lappareil-de-desinformation-russe/.

[9] Arcep-CSA. *Référentiel des usages numériques* [En ligne]. Le pôle numérique, 4 février 2021 [Consulté le 23/03/2024]. Disponible sur : https://www.csa.fr/content/download/260089/806852/version/1/file/Arcep-CSA%20-%20R%C3%A9f%C3%A9rentiel%20des%20usages%20num%C3%A9riques.pdf.

[10] SGDSN. *Service de vigilance et protection contre les ingérences numériques étrangères* [En ligne]. SGDSN, 17 novembre 2022 [Consulté le 23/03/24]. Disponible sur : https://www.sgdsn.gouv.fr/notre-organisation/composantes/service-de-vigilance-et-protection-contre-les-ingerences-numeriques.

[11] Commandement de la cyberdéfense. *Éléments publics de doctrine militaire de lutte informatique d'influence (L2I)* [En ligne]. Ministère des Armées, 2021 [Consulté le 24/03/2024]. Disponible sur : https://www.defense.gouv.fr/comcyber/nos-operations/lutte-informatique-dinfluence-l2i.

[12]Coustillère, Arnaud et Leroy, Aude. *Soldat de la cyberguerre*. Talllendier, 2024

[13] Arcom. *Découvrir l'institution* [En ligne]. Arcom, 2024 [Consulté le 23/03/2024]. Disponible sur : https://www.arcom.fr/nous-connaitre/decouvrir-linstitution.

[14] ARCEP. *Le manifeste de l'Arcep* [En ligne]. Arcep, 11 juillet 2023 [Consulté le 23/03/2024]. Disponible sur : https://www.arcep.fr/larcep/le-manifeste-de-larcep.html.

[15] CNIL. *Les missions de la CNIL* [En ligne]. CNIL, 2024 [consulté le 23/03/2024]. Disponible sur : https://cnil.fr/fr/les-missions-de-la-cnil.

[16] ENISA. *À propos de l'ENISA - L'Agence de l'Union européenne pour la cybersécurité* [En ligne]. ENISA, 2024 [Consulté le 23/03/2024]. Disponible sur : https://www.enisa.europa.eu/about-enisa/about/fr.

[17] Union européenne. *Service européen pour l'action extérieure (SEAE)* [En ligne]. Union européenne, 2024 [Consulté le 23/03/2024]. Disponible sur : https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-external-action-service-eeas_fr.

[18] Haut representant de l'Union pour les affaires étrangères et la politique de sécurité. *Plan d'action contre la désinformation* [En ligne]. Commission européenne, 5 décembre 2018 [Consulté le 23/03/2024]. Disponible sur : https://eeas.europa.eu/sites/default/files/plan_daction_contre_la_desinformation.pdf.

[19] CCDCOE. *About us* [En ligne]. CCDCOE, 2024 [Consulté le 24/03/2024]. Disponible sur : https://ccdcoe.org/about-us/.

[20] Hybrid CoE. *What are hybrid threats ?* [En ligne]. Hybrid CoE, 2024 [Consulté le 24/03/2024]. Disponible sur : https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/

[21] Commission européenne. *Code of Practice on Disinformation* [En ligne]. Commission européenne, 2022 [Consulté le 24/03/2024]. Disponible sur : https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

[22] Bulnois, Olivier. *La souveraineté numérique face aux manipulations de l'information en France de 2011 à 2021*. Université Jean Moulin Lyon III, mémoire de master, 2021.

[23] Commission européenne. *Législation sur les marchés numériques: garantir des marchés numériques équitables et ouverts* [En ligne]. Commission européenne, 2024 [Consulté le 24/03/2024]. Disponible sur : https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_fr.

[24] Commission européenne. *Législation sur les marchés numériques: garantir un environnement en ligne sûr et responsable* [En ligne]. Commission européenne, 2024 [Consulté le 24/03/2024]. Disponible sur : https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_fr.

[25] Junius, Lie « Plus de moyens pour trouver des informations de qualité en Europe ». *Google Actualité* [En ligne], 24 avril 2019 2024 [Consulté le 24/03/2024]. Disponible sur : https://france.googleblog.com/2019/04/plus-de-moyens-pour-trouver-des.html.

[26] Meta. « Facebook poursuit sa démarche de transparence en matière de publicité et de gestion des pages ». *Facebook News* [En ligne], 28 juin 2018 [Consulté le 24/03/2024]. Disponible sur : https://about.fb.com/fr/news/2018/06/facebook-poursuit-sa-demarche-de-transparence-en-matiere-de-publicite-et-de-gestion-des-pages/.

[27] Les Jeunes IHEDN. *Présentation de l'association* [En ligne]. Les Jeunes IHEDN, 2024 [Consulté le 24/03/2024]. Disponible sur : https://www.jeunes-ihedn.org/presentation/.

Ressources utilisées

Jeangene Vilmer, Jean-Baptiste et al. *Les Manipulations de l'information : un défi pour nos démocraties*. Rapport du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, août 2018, p. 148.

Giry, Julien. « Les fake news comme concept de sciences sociales. Essai de cadrage à partir de notions connexes : rumeurs, théories du complot, propagande et désinformation ». *Questions de communication* [En ligne], 2020/2 (n° 38) [Consulté le 20/03/2024]. Disponible sur : https://www.cairn.info/revue-questions-de-communication-2020-2-page-371.htm.

Ianni, Pascal. « Gagner la guerre de l'Influence ». *Servir* [En ligne], 2024/1 (n° 525) [Consulté le 20/03/2024]. Disponible sur : https://www.cairn.info/revue-servir-2024-1-page-13.htm.

Klen, Michel. « La nouvelle guerre de l'information ». *Revue Défense Nationale* [En ligne], 2024/1 (n° 866) [Consulté le 20/03/2024]. Disponible sur : https://www.cairn.info/revue-defense-nationale-2024-1-page-94.htm.

Villani, Cédric. « Les enjeux de l'IA pour la Défense de demain ». *Revue Défense Nationale* [En ligne], 2019/5 (n° 820) [Consulté le 20/03/2024]. Disponible sur : https://www.cairn.info/revue-defense-nationale-2019-5-page-23.htm.

Foucart, Stéphane ; Horel, Stéphane et Laurens, Sylvain. *Les gardiens de la raison. Enquête sur la désinformation scientifique* [En ligne]. La Découverte, Coll. « Cahiers libres », 2020 [Consulté le 20/03/2024]. Disponible sur : https://www.cairn.info/les-gardiens-de-la-raison--9782348046155.htm.

Béasse, Muriel. « Véridicité de l'information : un concept opérationnel pour l'éducation critique aux médias ». *Les Enjeux de l'information et de la communication* [En ligne], 2023/S1 (n° 23/1A) [Consulté le 20/03/2024]. Disponible sur : https://www.cairn.info/revue-les-enjeux-de-l-information-et-de-la-communication-2023-S1-page-135.htm.

Bronner, Gérald. *Les lumières à l'ère numérique. Rapport sur la désinformation* [En ligne]. Présidence de la République, 11 Janvier 2022 [Consulté le 20/03/2024]. Disponible sur : https://www.vie-publique.fr/rapport/283201-lumieres-l-ere-numerique-commission-bronner-disinformation.

Franceinfo et AFP. « Paris 2024 : une campagne de désinformation liée à l'Azerbaïdjan a cible les Jeux olympiques, selon un rapport». *Franceinfo Sport* [En ligne], 13 novembre 2023 [Consulté le 20/03/2024]. Disponible sur : https://www.francetvinfo.fr/les-jeux-olympiques/les-francais/jo-de-paris-2024-une-campagne-de-desinformation-liee-a-l-azerbaidjan-a-cible-la-competition-selon-un-rapport_6181863.html.

ANSSI. *Panorama de la cybermenace 2023* [En ligne]. ANSSI, 27 février 2024 [Consulté le 20/03/2024]. Disponible sur : https://www.cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/.

Charon, Paul et. Jeangène Vilmer, Jean-Baptiste. *Les Opérations d'influence chinoises. Un moment machiavélien*. Rapport de l'Institut de recherche stratégique de l'École militaire (IRSEM), Paris, ministère des Armées, 2e édition, octobre 2021.

Polewka, Anna. « Outiller les élèves pour combattre la désinformation ». *Revue internationale d'éducation de Sèvres* [En ligne], n°93, septembre 2023 [Consulté le 06/03/2024]. Disponible sur : https://doi.org/10.4000/ries.14003.

Baur, Monica. « La lutte contre la désinformation sur YouTube ». *Communication* [En ligne], vol. 38/2, 1er novembre 2021 [Consulté le 06/03/2024]. Disponible sur : http://journals.openedition.org/communication/14314.

Dauphin, Florian. « Succès et limites du debunking pour lutter contre la désinformation. Le cas des vidéastes sceptiques sur YouTube ». *Questions de communication* [En ligne] 2022, n°42 [Consulté le 06/03/2024]. Disponible sur : https://www.cairn.info/revue-questions-de-communication-2022-2-page-315.htm.

Jeangène Vilmer, Jean-Baptiste. « Chapitre 16. Panorama des mesures prises contre les manipulations de l'information », *in :* Marangé, Céline et Quessard, Maud. *Les guerres de l'information à l'ère numérique* [En ligne]. Presses Universitaires de France, 2021, pp. 365-388 [Consulté le 06/03/2024]. Disponible sur : https://doi.org/10.3917/puf.maran.2021.01.0365.

Marangé, Céline et Quessard, Maud. *Les guerres de l'information à l'ère numérique* [En ligne]. Presses Universitaires de France, 2021 [Consulté le 06/03/2024]. Disponible sur : https://doi.org/10.3917/puf.maran.2021.01.0365.

Pariser, Eli. *The filter bubble: What the Internet is hiding from you*. Penguin, 2011.

Lassalle, Bruno et De Gliame, Brice. « Sensibiliser et armer les citoyens face à la guerre cognitive ». *Revue Défense Nationale* [En ligne], 2022, n°3 [Consulté le 06/03/2024]. Disponible sur : https://doi.org/10.25965/interfaces-numeriques.4830.

Boyadjian, Julien. « Désinformation, non-information ou sur-information? ». *Réseaux* [En ligne], 2020, vol. 222, n° 4 [Consulté le 06/03/2024]. Disponible sur : https://doi.org/10.3917/res.222.0021.

Dubet, François. *Trois jeunesses: la révolte, la galère, l'émeute*. Le Bord de l'eau, 2018.

U.S. Department of Justice. *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* [En ligne]. DoJ, Vol. I à III, mars 2019 [Consulté le 23/03/24]. Disponible sur : https://www.justice.gov/archives/sco/file/1373816/download.

Vincent Bernard. « Éduquer au numérique au-delà des risques ». *Nouvelle Revue de l'Enfance et de l'Adolescence* [En ligne], 2021, n°2 [Consulté le 23/03/24]. Disponible sur : https://doi.org/10.3917/nrea.005.0021.

Cycle Défense & Cyber. *Tactiques, techniques et procedures (TTPs) de la matrice DISARM sur la désinformation* [En ligne]. Viginum, février 2024 [Consulté le 23/03/24]. Disponible sur : https://defense-cyber.fr/actus-defense-cyber/matrice-disarm-viginum-fevrier-2024/.

Les Jeunes IHEDN. *Devant nous. 32 ambitions pour le future* [En ligne]. Les Jeunes IHEDN, 2020 [Consulté le 23/03/24]. Disponible sur : https://jeunes-ihedn.org/wp-content/uploads/2020/05/Devant_Nous_FR.pdf.

contact@jeunes-ihedn.org