© Humensis

Chapitre 16

Panorama des mesures prises contre les manipulations de l'information

Jean-Baptiste Jeangène Vilmer

À l'exception de quelques États d'Europe centrale, nordique et orientale pour lesquels les attaques informationnelles venant de l'Est n'ont pas vraiment cessé avec la fin de la guerre froide, tous ceux qui, à l'« Ouest », avaient mis en place des mesures défensives contre les opérations soviétiques ont « désarmé » dans les années 1990 et se sont donc trouvés dépourvus lorsque, vingt ans plus tard, le besoin s'est fait sentir de se défendre à nouveau contre des attaques informationnelles étatiques de grande ampleur[1]. La prise de conscience a été graduelle – et elle continue de croître partout dans le monde – mais semble s'être accélérée dans les années 2010, en trois étapes.

La première est l'annexion de la Crimée en 2014 et la guerre du Donbass : l'offensive russe en Ukraine est devenue depuis un cas d'école de guerre dite « hybride[2] », dont la « guerre informa-

1. Une étape intermédiaire a été franchie au début des années 2000 lorsque certains États, en premier lieu les États-Unis, ont dû revoir leur appareil de défense informationnelle pour contrer des attaques venant de groupes armés non étatiques, notamment al-Qaida.

2. La notion de « guerre hybride » a été introduite par le lieutenant-général James Mattis et le lieutenant-colonel Frank Hoffman en 2005 (« Future warfare : The rise of hybrid wars », *Proceedings Magazine*, U.S. Naval Institute, novembre 2005, vol. 131, n° 11). Elle peut être définie comme « le mélange d'activités coercitives et subversives, de méthodes conventionnelles et non conventionnelles (c'est-à-dire diplomatiques, militaires, économiques, technologiques), susceptibles d'être utilisées de façon coordonnée

348977AEJ_INFORMATION_cc2019_pc.indd 365 16/09/2020 16:48:45

© Humensis

tionnelle » est une partie, et elle a été le premier accélérateur de la prise de conscience des vulnérabilités étatiques. Cependant, l'Ukraine étant aussi un cas particulier, compte tenu de son histoire avec la Russie et du fait que les populations visées étaient majoritairement russophones, ce risque a surtout trouvé un écho dans les pays présentant l'une ou l'autre de ces spécificités, notamment les États baltes. L'Ukraine, directement visée, prenait elle-même plusieurs mesures, dont certaines assez drastiques comme l'interdiction des médias russes. Mais, sous la pression d'un certain nombre d'États plus préoccupés que les autres, cette prise de conscience s'est généralisée à l'Organisation du traité de l'Atlantique nord (OTAN) et l'Union européenne (UE).

La deuxième étape qui a internationalisé la perception de la menace est l'ingérence russe dans la campagne présidentielle américaine de 2016. Autant les actions précédentes pouvaient convaincre certains grands États d'Europe occidentale ou d'Amérique du Nord qu'ils étaient en quelque sorte « hors d'atteinte » à la fois des capacités et des ambitions russes en la matière, autant le cas américain a démontré à la face du monde que personne, pas même la première puissance mondiale, n'était à l'abri. Cette affaire a eu l'effet immédiat de mettre en alerte tous les autres États. Une autre ingérence électorale dans une grande puissance l'année suivante, la France, avec l'opération dite des « Macron Leaks », a confirmé cette vulnérabilité partagée et donc la nécessité de mieux se protéger. L'accumulation des mesures – organisationnelles, législatives ou éducationnelles – prises par les États est exponentielle à partir de 2017.

La troisième étape dans cette prise de conscience en escalier a consisté à globaliser la perception de la menace, qui n'est ni seulement russe, ni seulement étatique. Cela s'est notamment traduit par un « pivot asiatique » plaçant la Chine au centre des préoccupations

---

par des acteurs étatiques ou non étatiques en vue d'atteindre certains objectifs, sans que le seuil d'une guerre déclarée officiellement ne soit dépassé » (Commission européenne, *Cadre commun en matière de lutte contre les menaces hybrides*, Bruxelles, 6 avril 2016).

348977AEJ_INFORMATION_cc2019_pc.indd 366 16/09/2020 16:48:45

© Humensis

– ce qui a toujours été le cas pour quelques pays, dont Taïwan, l'Australie et Singapour notamment, la nouveauté étant que la question de l'influence chinoise et, plus précisément, de ses manœuvres informationnelles, est désormais posée avec autant d'inquiétude à Washington, Bruxelles ou Addis-Abeba. Il en va de même pour les acteurs non étatiques : la prise de conscience avait déjà eu lieu depuis le début des années 2000 concernant le cas particulier des groupes armés djihadistes, d'abord al-Qaida puis Daech (et avait amorcé des tentatives de réponses coordonnées), mais elle s'étend désormais aux mouvements populistes, nationalistes et aux extrêmes de toute sorte, ainsi qu'aux entreprises qui font de la désinformation un business. En d'autres termes, il est clair désormais que la menace est globale, protéiforme et multiscalaire. Rares sont ceux qui ne s'estiment pas concernés. Des îles Féroé aux îles Fidji en passant par le Mali, les Philippines et le Brésil, la prise de conscience est quasi universelle, à des degrés divers bien sûr, certains s'estimant (à tort ou à raison) plus ou moins menacés que d'autres.

Dans ce contexte, la question que pose ce chapitre est celle de savoir quelles sont les réponses : quelles mesures les États et les sociétés civiles ont-ils prises pour se défendre contre les manipulations de l'information ? Ce que l'on peut appeler la « défense informationnelle » (*information defense*)[1] est autant la défense *de* que la défense *par* l'information. On distinguera les mesures prises par les États, la coopération internationale et la société civile, avant d'en pointer les limites[2].

1. « *Information Defense* » est le terme revendiqué par Ben Nimmo, comme l'indiquait son titre lorsqu'il était au Digital Forensic Research Lab (DFRLab) de l'Atlantic Council (« Senior Fellow for Information Defense »). Depuis 2019, il est « Director of Investigations » chez Graphika.

2. Ce chapitre s'appuie notamment sur Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera, *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, Paris, août 2018 ; et sur Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, Paris/Washington DC, IRSEM/Atlantic Council, 2019.

348977AEJ_INFORMATION_cc2019_pc.indd 367 16/09/2020 16:48:45

© Humensis

La mobilisation des États

Face aux manipulations de l'information dont les conséquences, pendant les élections ou en dehors, sont désormais prises au sérieux, les États ont pris depuis le milieu des années 2010 un certain nombre de mesures allant du design organisationnel, c'est-à-dire de la manière la plus optimale d'organiser l'administration[1], à la régulation des médias, en passant par le rôle des parlements, qui enquêtent et légifèrent, et la sensibilisation du public.

Le design organisationnel

Le premier réflexe des États – en tout cas des démocraties libérales – a été de modifier leur organisation interne. Ils l'ont fait différemment, car les cultures stratégiques et administratives ne sont pas les mêmes. Tous ont fait le constat que face à une menace « hybride » en ce qu'elle mêle et parfois confond le civil et le militaire, l'étatique et le non-étatique, et plusieurs domaines (non seulement la défense et la diplomatie mais aussi la culture, la justice, etc.), la priorité était d'adopter une approche globale et donc de transversaliser, décloisonner des services qui travaillent généralement en silos. *A minima*, il s'agit donc de connecter des compétences éparpillées, en créant des « comités » ou des « réseaux », comme le Réseau sur l'influence informationnelle finlandais, créé dès 2014 et regroupant une trentaine d'experts gouvernementaux pour identifier, analyser et répondre aux tentatives hostiles d'ingérence étrangère. La plupart des pays européens ont aujourd'hui un dispositif similaire. Il peut

1. Le design organisationnel est traditionnellement défini comme le « processus de décision visant à assurer une cohérence entre les buts ou objectifs pour lesquels l'organisation existe, les schémas de division du travail et de coordination entre unités et les personnes qui effectueront le travail » (Jay R. Galbraith, *Organization Design*, Reading (MA), Addison-Wesley Pub. Co., 1977, p. 5).

348977AEJ_INFORMATION_cc2019_pc.indd 368 16/09/2020 16:48:45

© Humensis

s'agir d'un groupe de travail temporaire ou d'un comité permanent : dans tous les cas, il ne fait que réunir des personnes déjà en poste. Certains vont plus loin en allouant un budget spécifique et en créant des postes pour constituer une structure dédiée à plein temps à la lutte contre les manipulations de l'information, soit au sein d'un service existant, soit en la créant *ex nihilo*.

Qu'il s'agisse d'une mise en réseau de l'existant ou de la création d'une nouvelle structure, se pose la question épineuse du rattachement institutionnel, qui se règle relativement facilement dans les États ayant déjà une culture transversale et horizontale, notamment les États scandinaves, ou les petits États, comme les pays Baltes, dans lesquels les équipes, plus réduites, ont davantage de chance de se connaître et de travailler ensemble. En général, le réseau ou la structure est piloté par les services du Premier ministre, une agence interministérielle ou encore un ministère donné (la Justice au Danemark et aux Pays-Bas, la Culture en Lettonie, le ministère des Communications et de l'Information à Singapour, etc.). Le ministère des Affaires étrangères britannique (FCO) accueille une cellule interministérielle d'une vingtaine de personnes ; le ministère de l'Intérieur en République tchèque héberge un centre de lutte contre le terrorisme et les menaces hybrides (CTHT) d'une vingtaine de personnes également ; et le ministère de l'Intérieur (Home Affairs) en Australie accueille l'équipe du coordinateur national en charge de la contre-ingérence.

Ces exemples témoignent d'ailleurs de la grande variété de focales retenues : les manipulations de l'information au sens strict, l'influence et/ou l'ingérence (une difficulté étant de savoir où finit l'une et où commence l'autre), ou encore les menaces « hybrides », qui sont même parfois, comme en République tchèque, associées aux menaces terroristes[1].

1. Cette association fréquente ne doit pas conduire à confondre les deux dans la mesure où l'objectif d'une attaque dite « hybride » est de générer de l'ambiguïté (si elle est bien conduite, la cible met du temps à comprendre qu'elle est attaquée et par qui), tandis que l'attaque terroriste est le plus souvent revendiquée : son objectif n'est pas d'entraver l'attribution, mais au contraire de la permettre et de l'assumer. Cela ne veut

348977AEJ_INFORMATION_cc2019_pc.indd 369 16/09/2020 16:48:45

© Humensis

Le cas américain est particulier en ce qu'il n'y a pas *une* mais *des* structures dédiées (le Global Engagement Center créé en 2016 au sein du département d'État, mais aussi de nombreuses *task forces* dédiées à la lutte contre la désinformation et/ou l'influence étrangère, dans d'autres administrations, dont le département de la Justice et le département de la Sécurité intérieure). Leur problème est donc moins un manque de ressources qu'un manque de coordination car, sur ce sujet hautement politique, aucune direction claire ne vient du Conseil de sécurité nationale et de la Maison Blanche.

Parmi les États qui ont mis en réseau leurs compétences existantes sans pour autant créer des structures dédiées permanentes et, donc, des postes supplémentaires, certains sont paralysés par des considérations bureaucratiques et budgétaires mais pour d'autres, comme Singapour, c'est un choix assumé, pour montrer que la lutte contre les manipulations de l'information est « l'affaire de tous » et ne pas risquer que la concentration des moyens dans une structure unique fasse que les autres services ne se sentent plus concernés[1].

Le rôle des parlements

Les parlements contribuent à la lutte contre les manipulations de l'information en enquêtant et en légiférant. Les principales enquêtes, aux États-Unis, au Royaume-Uni et en Australie, étant publiques et très suivies par les médias, elles permettent aussi d'informer et sensibiliser la population et, en exposant les responsables présumés, d'avoir peut-être un effet dissuasif. Elles sont le fait des services de police judiciaire (aux États-Unis, le FBI a commencé à enquêter sur « l'affaire russe » en juillet 2016) et des parlements, qui produisent en général des rapports très détaillés et très utiles, comme celui des

pas dire qu'en pratique un service associant les deux fera la confusion, puisqu'il peut réunir des équipes travaillant en parallèle. Dans le cas tchèque, le fait de préciser que le centre lutte contre « le terrorisme *et* les menaces hybrides » implique bien une différenciation, même si, par commodité organisationnelle sans doute, les deux sont réunis.

1. Entretien avec un responsable singapourien, Singapour, 5 novembre 2019.

348977AEJ_INFORMATION_cc2019_pc.indd 370 16/09/2020 16:48:45

© Humensis

sénateurs démocrates américains de janvier 2018[1] ou du comité pour le numérique, la culture, les médias et le sport de la Chambre des communes britannique en février 2019[2]. En décembre 2019, le parlement australien a à son tour établi un Comité restreint sur l'ingérence étrangère par les médias sociaux qui devrait remettre un rapport d'ici 2022[3]. Il est à noter que les rapports parlementaires ne s'inscrivent pas nécessairement dans une enquête visant un cas d'ingérence suspecté ou avéré. À Singapour, c'est pour préparer sa loi contre la désinformation que le parlement a créé en janvier 2018 un Comité restreint sur les mensonges délibérés en ligne qui, après de nombreuses auditions, y compris d'experts étrangers, a rendu son rapport en septembre 2019[4]. Au Royaume-Uni, le comité susnommé de la Chambre des communes a également publié un rapport sur *Misinformation in the COVID-19 Infodemic* en juillet 2020.

D'autre part, les parlements légifèrent. Certains États disposaient déjà, depuis parfois très longtemps, d'une législation dans ce domaine. En France par exemple, la loi sur la liberté de la presse de 1881 punissait déjà « la publication, la diffusion ou la reproduction, par quelque moyen que ce soit, de nouvelles fausses, de pièces fabriquées, falsifiées ou mensongèrement attribuées à des tiers lorsque, faite de mauvaise foi, elle aura troublé la paix publique, ou aura été susceptible de la troubler ». Mais ces anciennes dispositions étaient parfois incomplètes, ou inadaptées à l'ère numérique dans

1. US Senate, *Putin's Asymmetric Assault on Democracy in Russia and Europe : Implications for U.S. National Security*, A Minority Staff Report Prepared for the Use of the Committee on Foreign Relations, 10 janvier 2018, 115th Congress, Second Session (https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf).

2. UK House of Commons, Digital, Culture, Media and Sport Committee, *Disinformation and « Fake News » : Final Report*, 14 février 2019. PDF téléchargeable à l'adresse suivante : https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

3. Parliament of Australia, « Foreign interference through social media ». Voir en ligne : https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Interference_through_Social_Media/ForeignInterference.

4. Singapore, *Report of the Select Committee on Deliberate Online Falsehoods*. PDF en ligne : https://www.rajahtannasia.com/media/pdf/Exec_Summary_Rpt_on_Deliberate_Online_Falsehoods.pdf.

348977AEJ_INFORMATION_cc2019_pc.indd 371 16/09/2020 16:48:45

© Humensis

laquelle nous vivons désormais et qui a changé non pas la nature des manipulations de l'information (qui ont toujours existé) mais les moyens et la vitesse de leur propagation, puisqu'il est désormais possible de toucher des millions de personnes en quelques minutes. Il est donc apparu nécessaire soit de mettre à jour, soit dans d'autres cas de créer de toutes pièces, une législation adaptée.

Certaines démocraties libérales se sont engagées dans cette voie. L'Allemagne la première avec sa fameuse loi « Netzwerkdurchsetzungsgesetz » (NetzDG), entrée en vigueur au 1er janvier 2018, forçant les plateformes numériques à supprimer les messages « de toute évidence illégaux » dans les 24 heures, au risque d'encourir une amende susceptible d'aller jusqu'à 50 millions d'euros. En France, une loi contre la manipulation de l'information a été adoptée par l'Assemblée nationale en novembre 2018 puis validée par le Conseil constitutionnel le mois suivant. En Israël, un jugement de la Cour suprême interdit, à compter de mars 2019, les publicités anonymes et contraint les faux comptes utilisés pour faire de la propagande et les bots à s'identifier. Taïwan est un autre exemple, avec la loi « anti-infiltration » de décembre 2019 qui contient certaines mesures pour lutter contre la désinformation.

Le fait est cependant que la plupart des législations ont été adoptées dans des pays qui ne peuvent pas être considérés comme des démocraties libérales. La Chine et la Russie passent régulièrement des lois criminalisant le fait de diffuser des rumeurs susceptibles de nuire à l'ordre social. Lorsque la Malaisie (avril 2018), le Cambodge et le Kenya (mai 2018), la Biélorussie (juin 2018), l'Égypte (juillet 2018), l'Algérie (avril 2020), le Kirghizistan (juin 2020) ou encore le Brésil (juillet 2020) ont également adopté des législations dans ce domaine, ils ont été vivement critiqués par les organisations de défense des droits humains. Dans ces contextes où la liberté de la presse est déjà menacée, voire inexistante, ces mesures législatives ne font que la dégrader davantage et renforcer le contrôle de l'exécutif sur sa population. Le cas singapourien est également ambivalent : la loi sur la protection contre les mensonges en ligne et la désinformation (POFMA), adoptée par le parlement en mai 2019, a été

348977AEJ_INFORMATION_cc2019_pc.indd 372 16/09/2020 16:48:45

© Humensis

vivement critiquée dans certains médias occidentaux[1] pour avoir été utilisée contre un parti d'opposition – une affaire qui suscite un débat à Singapour même, où elle a été portée devant la Haute Cour de justice.

La sensibilisation de la population

Les démocraties libérales ont vite compris que les mesures précédentes ne suffiraient pas si la population dans son ensemble n'était pas consciente des dangers des manipulations de l'information. Pour la sensibiliser, les États – certains plus que d'autres naturellement – ont donc mis en place un éventail de mesures parmi lesquelles la formation des fonctionnaires[2] et des partis politiques en période électorale[3], mais aussi la mise en ligne de sites Internet dédiés pour informer le grand public[4] ou la distribution de brochures[5].

Une autre mesure préventive est bien entendu l'ajout ou le développement de l'éducation aux médias dans les programmes scolaires[6].

1. Voir par exemple « Singapore "falsehoods" law shows perils of fake news fight », *Financial Times*, 3 février 2020.

2. En février 2020, l'agence suédoise des contingences civiles (MSB) en avait déjà formé 13 000 (entretien au MSB, le 5 février 2020).

3. En France, le Secrétariat général de la défense et de la sécurité nationale (SGDSN) les avait alertés dès la fin de l'été 2016 et, en octobre, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) – qui dépend du SGDSN – a organisé pour eux un séminaire sur la cybersécurité (Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 31-32).

4. Comme l'a fait la Belgique avec Stopfakenews.be.

5. Le MSB a envoyé par la poste près de 5 millions d'exemplaires d'une brochure expliquant quoi faire en cas de crise, qu'il s'agisse d'une attaque terroriste ou d'une manipulation de l'information. Voir https://www.dinsakerhet.se/siteassets/dinsakerhet.se/broschyren-om-krisen-eller-kriget-kommer/om-krisen-eller-kriget-kommer---engelska.pdf.

6. Dès 2017, l'Italie a ajouté l'objectif de pouvoir « reconnaître les fake news » aux programmes scolaires ; plusieurs États américains, dont la Californie et le Massachusetts, ont adopté des lois en ce sens en 2018 ; tandis que depuis juillet de la même année la Suède développe les « compétences numériques » dans ses écoles, etc.

348977AEJ_INFORMATION_cc2019_pc.indd 373 16/09/2020 16:48:45

© Humensis

Le financement de la société civile est également important[1], comme le soutien à la recherche, qui implique de financer et parfois co-publier des études, comme l'a fait le MSB avec l'université de Lund pour leur *Handbook* sur les opérations d'influence.

La régulation des médias

Parmi les mesures prises par les États, certaines visent spécifiquement les médias qui, avec les plateformes numériques, sont les principaux vecteurs des manipulations de l'information. Ces mesures consistent généralement à renforcer le pouvoir des autorités de régulation des médias comme l'Ofcom britannique ou le Conseil supérieur de l'audiovisuel français ; et contraindre les médias à faire preuve de transparence quant à leurs relations financières avec un État étranger, comme le fait le *Foreign Agent Registration Act* aux États-Unis. À la demande du département de la Justice, RT et Sputnik se sont ainsi enregistrés comme « agents de l'étranger ». La Russie a adopté une loi similaire, dans un contexte où la liberté de la presse est bien moindre que dans les démocraties occidentales[2], de sorte que, dans les faits, ce statut d'agent de l'étranger peut être utilisé pour pousser un certain nombre de médias à la fermeture. Enfin, certains États ont choisi d'interdire purement et simplement certains médias, comme l'Ukraine l'a fait avec les médias russes (73 chaînes de télévision interdites entre 2014 et 2016) et plusieurs sites russes en mai 2017 (VKontakte, Odnoklassniki, Yandex, Mail.ru). De même, l'Indonésie a également choisi de bloquer des sites ou des réseaux sociaux pour lutter contre les manipulations de l'information – un choix généralement critiqué par les démocraties libérales et les organisations de défense des droits humains.

1. Le plan canadien révélé en janvier 2019 prévoit ainsi 7 millions de dollars pour des projets permettant de sensibiliser la population au risque que présente la désinformation en ligne.

2. La Russie est à la 149e place (sur 180) dans le classement de Reporters sans frontières. Voir https://rsf.org/fr/classement.

348977AEJ_INFORMATION_cc2019_pc.indd 374 16/09/2020 16:48:45

© Humensis

La coopération internationale

Les menaces que posent les manipulations de l'information étant par nature transnationales, non seulement parce qu'une attaque peut venir de l'étranger mais aussi et surtout parce qu'Internet n'a pas de frontière, elles posent à la société internationale un défi global qui nécessite des réponses coordonnées. La coopération internationale est donc cruciale. Elle n'a cessé de progresser, en particulier depuis 2014. On peut distinguer plusieurs couches : le partage du renseignement, principalement bilatéral, les formats multilatéraux (UE, OTAN, G7) et le rôle des think tanks.

Le partage du renseignement

La première couche, qui a toujours existé, est le partage du renseignement – qui reste toutefois limité car, dans ce domaine comme dans celui du cyber, partager des informations revient aussi à partager des vulnérabilités ; les États sont donc souvent réticents. À quelques exceptions près dont les Five Eyes[1], ce type de coopération est généralement bilatéral, entre deux États qui se font confiance. Il est difficile de s'ouvrir à un plus grand nombre, et le niveau de l'information partagée (ce qu'on dit) dépend du niveau de confiance du partenaire (à qui on le dit). Il y a par exemple une réticence à trop partager avec des services qu'on estime trop pénétrés par l'adversaire, ou des États dont le leadership politique est considéré comme trop ambivalent à l'égard de cet adversaire.

Néanmoins, entre alliés de longue date, comme la France et les États-Unis par exemple, le partage de renseignement fonctionne bien et c'est d'ailleurs l'une des leçons que l'on peut tirer de la bonne

1. Une alliance des services de renseignement des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande.

348977AEJ_INFORMATION_cc2019_pc.indd 375 16/09/2020 16:48:45

© Humensis

gestion de l'opération dite des « Macron Leaks » en 2017. Si la France a appris des États-Unis, c'est autant en tirant les leçons des erreurs commises par l'administration Obama durant la campagne présidentielle de 2016, qu'en bénéficiant du renseignement américain. À plusieurs reprises durant la campagne française, les services américains ont alerté les services français sur les « activités russes[1] ».

Les formats multilatéraux : UE, OTAN, G7

La deuxième couche est celle des formats multilatéraux, dont les plus actifs dans la lutte contre les manipulations de l'information sont l'UE, l'OTAN et le Groupe des sept (G7).

Premièrement, pour répondre aux conclusions du Conseil européen des 19-20 mars 2015 qui soulignaient « la nécessité de contrer les campagnes de désinformation menées par la Russie » et qui invitaient la haute représentante à élaborer un plan d'action sur la communication stratégique, la division Communication stratégique du Service européen pour l'action extérieure (SEAE) a créé trois équipes : une « *task force* de communication stratégique orientée vers le voisinage oriental » (East StratCom Task Force), active depuis septembre 2015, composée d'une quinzaine de personnes, qui diffuse son travail sur son site Internet « EU vs Disinformation » (euvsdisinfo.eu), dans une *Disinformation Review* hebdomadaire et sur les réseaux sociaux sous le nom de « briseurs de mythes » (*EU Mythbusters*) ; une *task force* « Sud », créée en 2015 et composée de quatre personnes, qui lutte contre le discours djihadiste ; et une *task force* « Balkans occidentaux » créée en 2017, composée de trois agents, qui se concentre sur la défense de l'image de l'UE dans la région.

En 2016, la Commission européenne a adopté un cadre commun en matière de lutte contre les menaces hybrides[2]. À la suite d'une

1. Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 30.

2. Cité *supra*, p. 365.

348977AEJ_INFORMATION_cc2019_pc.indd 376 16/09/2020 16:48:45

© Humensis

résolution du parlement européen de juin 2017 qui lui demande d'étudier l'éventualité « d'une intervention législative afin de limiter la publication et la diffusion de faux contenus[1] », la Commission européenne se saisit du sujet. La Commissaire pour l'économie et la société numériques constitue un groupe d'experts qui rend un rapport en mars 2018 faisant un certain nombre de recommandations. Complété par une consultation publique, il sert de base à la communication sur la lutte contre la désinformation que la Commission publie le mois suivant. Celle-ci propose l'élaboration d'un « code de bonnes pratiques contre la désinformation », qui est publié en juillet 2018. En octobre, le code est signé par Facebook, Twitter, Google, Mozilla et plusieurs associations professionnelles, s'engageant à faire des progrès pour lutter contre la désinformation en ligne, notamment en supprimant davantage de faux comptes et en limitant la visibilité des sites favorisant la désinformation. En mai 2019, Microsoft signe à son tour. En octobre de la même année, les signataires publient les premiers rapports d'autoévaluation sur la mise en œuvre de leurs engagements. Cette procédure a la vertu de pousser les plateformes à davantage de transparence quant aux mesures prises, à la fois quantitativement et qualitativement, et met en évidence un réel effort de leur part mais aussi quelques manques, notamment en matière de mesures à prendre pour « donner aux consommateurs et à la communauté des chercheurs les moyens d'agir[2] ».

En amont des élections européennes de 2019, l'UE a pris des mesures additionnelles pour lutter contre le risque de manipulations de l'information à des fins d'ingérence, incluant notamment le « paquet électoral » annoncé par le président Juncker dans son discours de 2018 sur l'état de l'Union. Pendant la campagne, ont été relevées « des preuves de comportements non authentiques

1. 2016/2276(INI) – 15/06/2017. *Text adopted by Parliament, single reading.*

2. Représentation en France de la Commission européenne, « Code de bonnes pratiques contre la désinformation, un an après : les plateformes en ligne soumettent leurs rapports d'autoévaluation », 29 octobre 2019 (https://ec.europa.eu/france/news/20101029/rapport_code_bonne_conduite_desinformation_fr).

348977AEJ_INFORMATION_cc2019_pc.indd 377 16/09/2020 16:48:45

© Humensis

coordonnés visant à diffuser sur les plateformes en ligne, y compris au moyen de logiciels robots et de faux comptes, du contenu de nature à semer la division[1] ». Cependant, les mesures prises par la société civile, notamment les journalistes et vérificateurs de fait, les plateformes numériques, les autorités nationales et enfin les institutions européennes, ont maintenu ces tentatives en deçà d'un seuil de nuisance et, globalement, les élections européennes se sont bien passées. Au début de l'année 2020, la Commission envisage une réglementation contre la désinformation, « particulièrement quand de la désinformation coordonnée sur des plateformes tech peut poser des problèmes de sécurité[2] ».

Enfin, dans le cadre européen il faut aussi souligner l'importance du centre européen d'excellence contre les menaces hybrides de Helsinki (Hybrid CoE), créé en 2017, et qui constitue un hub de ressources sur le sujet, entretenant des réseaux de chercheurs, organisant des séminaires, et produisant régulièrement des publications.

Deuxièmement, un autre acteur multilatéral majeur est l'OTAN. Confrontée aux opérations informationnelles soviétiques durant la guerre froide, l'Alliance reste aujourd'hui principalement préoccupée par les menaces provenant de Russie, même si, plus récemment, elle s'est intéressée aussi et de manière croissante à la Chine. De fait, l'OTAN est l'une des principales cibles de la désinformation et doit faire face chaque jour à un grand nombre de nouvelles fausses ou biaisées la concernant. Elles visent principalement ses intentions, présentées comme hégémoniques et agressives, son expansion et le volume de ses troupes, notamment celles déployées dans les États baltes et la Pologne, ou encore les crimes que commettraient ses soldats.

1. « Une Europe qui protège : l'UE fait rapport sur les progrès réalisés dans la lutte contre la désinformation en vue du Conseil européen », communiqué de presse du 14 juin 2019. Voir en ligne https://ec.europa.eu/commission/presscorner/detail/fr/IP_19_2914.

2. Élodie Lamer, « Vera Jourova, vice-présidente de la Commission européenne : "Le temps des accords avec les géants du Net est révolu" » (interview de Vera Jourova, vice-présidente de la Commission européenne pour les valeurs et la transparence), *Le Soir*, 10 février 2020.

348977AEJ_INFORMATION_cc2019_pc.indd 378 16/09/2020 16:48:45

© Humensis

Deux acteurs majeurs en son sein sont chargés de répondre à ces attaques et plus largement d'étudier les manipulations de l'information. D'une part, la Division Diplomatie publique (PDD) du secrétariat international, à Bruxelles, qui produit régulièrement des réfutations des accusations russes, notamment sur une page dédiée du site Internet répondant aux principaux « mythes ». La PDD joue également un rôle de coordination entre les différentes structures de l'organisation et entre les Alliés. D'autre part, le centre d'excellence de l'OTAN sur la communication stratégique de Riga (NATO StratCom COE), créé en 2014, publie un grand nombre d'analyses et organise chaque année un « StratCom Summit » sur ces questions, qui est l'un des moments importants de partage et d'échange d'informations entre acteurs étatiques et non étatiques du monde entier. Certains pays asiatiques, notamment Singapour, sont de plus en plus investis dans ces événements traditionnellement « euratlantiques », car il y a en Asie une inquiétude croissante que la Chine prenne progressivement le chemin de la Russie, c'est-à-dire adopte des tactiques plus agressives[1].

Troisièmement, depuis 2018, le G7 dispose d'un « mécanisme de réaction rapide », coordonné par le Canada, qui permet de faire circuler l'information rapidement entre les pays du G7. Les personnes ressources de chaque État se connaissent et se voient régulièrement, et l'unité de coordination du ministère canadien des Affaires globales collecte et partage un grand nombre d'informations pertinentes, notamment des publications et des événements. En termes d'accès à l'information, c'est un progrès important.

Les think tanks, passeurs d'idées

La troisième couche de la coopération internationale est celle des think tanks, acteurs non étatiques mais souvent au moins en partie

1. Ce que les opérations chinoises à Taïwan et Hong Kong semblent confirmer : sur cette réduction de l'écart Russie-Chine, voir Jean-Baptiste Jeangène Vilmer et Paul Charon, « Russia as a hurricane, China as climate change : Different ways of information warfare », *War on the Rocks*, 21 janvier 2020.

348977AEJ_INFORMATION_cc2019_pc.indd 379 16/09/2020 16:48:45

© Humensis

financés par des États et ayant dans leurs équipes du personnel passé par des ministères, des agences ou services de l'État dans les domaines de la défense et de la sécurité, ou qui y sont encore tout en étant détachés à « l'extérieur ». Dans la zone grise entre deux mondes, ils ont à la fois l'accès à des ressources et à des informations et la capacité de les diffuser plus librement. Ils organisent régulièrement des séminaires plus ou moins fermés, dont des « tracks 1.5 », c'est-à-dire des rencontres associant officiels et société civile. Ce mélange des genres, cette fécondation croisée, permet aux officiels de « s'aérer », de récolter des idées « en dehors de la boîte », et aux membres de la société civile de mieux comprendre comment les États travaillent et d'espérer pouvoir peut-être les influencer. Parmi les rencontres connues de ce genre, on peut citer celles qu'organise le DFRLab d'Atlantic Council à Washington et à Bruxelles et celles du Centre d'excellence pour la sécurité nationale (CENS) de la S. Rajaratnam School of International Studies (RSIS) à Singapour – qui présente l'avantage de croiser les perspectives géographiques, notamment euratlantique et asiatique.

Les think tanks américains, en particulier Graphika (Camille François, Ben Nimmo), l'Atlantic Council (DFRLab), la Brookings (Alina Polyakova, désormais présidente de CEPA) et le GMF (Laura Rosenberger), produisent une part substantielle de la recherche « opérationnalisable » sur les manipulations de l'information, en lien avec les décideurs politiques mais aussi les plateformes numériques, notamment Twitter, Facebook et Google qui, de façon croissante, participent à ces activités.

L'implication de la société civile

Quelles que soient les mesures décrites dans les pages précédentes, mises en place par les États, le degré de résilience d'une société, sa capacité de résistance aux manipulations de l'information, dépend

348977AEJ_INFORMATION_cc2019_pc.indd 380 16/09/2020 16:48:45

© Humensis

d'abord et avant tout de la mobilisation de ses citoyens. Ce sont eux qui sont en première ligne et notamment les journalistes : outre qu'ils ont tous la responsabilité de fournir des informations fiables et sincères, certains se sont spécialisés dans la chasse aux trolls et autres réseaux d'influence, et d'autres travaillent à améliorer les standards journalistiques. Sont également importants les vérificateurs de faits, qui sont souvent mais pas nécessairement des journalistes. Tous ne sont pas récents (l'américain Snopes qui est l'un des plus connus existe depuis 1994) mais ils se sont multipliés dans les années 2010, partout dans le monde, comme un indicateur supplémentaire de la prise de conscience à l'œuvre. Certains d'entre eux sont opérés par des médias connus, qui en plus de produire des informations s'occupent de plus en plus de les vérifier (AFP Fact Check, Reality Check de la BBC, Decodex du *Monde*, CheckNews de *Libération*, etc.). Mais il n'y a pas que les médias reconnus : de nombreux sites diffusant des nouvelles fausses ou biaisées prétendent eux-mêmes faire du *fact-checking*. L'Institut Poynter a donc créé en 2015 un International Fact-Checking Network et a adopté un « code » de principes communs pour garantir une vérification transparente et non partisane. Les vérificateurs « approuvés » par Poynter sont censés satisfaire ces critères méthodologiques.

Il y a également des initiatives normatives – labels, index et autres classements – permettant de distinguer les sources d'information fiables des autres. Certains ont défendu des classements « négatifs » (un classement international de la désinformation sur le modèle de ceux de Freedom House sur la liberté de la presse et de Transparency International pour la corruption)[1] ou au contraire des classements « positifs » ou une forme de certification, comme l'initiative pour la confiance dans le journalisme (*Journalism Trust Initiative*) de Reporters sans frontières (RSF) qui entend « renverser la logique en donnant un avantage réel à tous ceux qui produisent des

1. Peter Pomerantsev et Michael Weiss, *The Menace of Unreality : How the Kremlin Weaponizes Information, Culture and Money*, New York, The Interpreter/Institute of Modern Russia, 2014.

348977AEJ_INFORMATION_cc2019_pc.indd 381 16/09/2020 16:48:46

© Humensis

informations fiables, quel que soit leur statut[1] », avec l'objectif que les plateformes numériques attribuent une « prime » à la qualité dans leurs algorithmes et leur accordent donc une visibilité accrue.

Il faut aussi mentionner des initiatives citoyennes comme le phénomène dit des « elfes » (qui chassent, identifient et exposent les « trolls »), originaire de Lituanie et dont se revendiquent des milliers d'internautes essentiellement mais pas seulement en Europe centrale, orientale et nordique.

Enfin, les plateformes numériques elles-mêmes, qui ont été longtemps réticentes à reconnaître le problème, ont été contraintes à réagir. Le tournant de la coopération date de 2018, année durant laquelle elles ont commencé à partager des informations (Reddit en avril sur 944 comptes liés à l'Internet Research Agency [IRA] russe, Facebook en juillet au sujet d'une autre opération de l'IRA, Twitter en octobre sur 9 millions de tweets également attribués à l'IRA, etc.)[2]. Elles publient depuis des documents pédagogiques, comme par exemple *How Google Fights Disinformation* en février 2019, et rendent des comptes à la commission européenne dans le cadre du Code des bonnes pratiques contre la désinformation. Ces plateformes – certaines plus que d'autres – ont aussi pris l'habitude de partager des informations (pages, comptes concernés) avec certains chercheurs et analystes avec lesquels ils ont développé une relation de confiance, avant des *takedowns*, c'est-à-dire des suppressions massives de comptes[3]. Ces informations ont notamment alimenté les études de DFRLab et Graphika ces dernières années. Les plateformes consacrent désormais des moyens importants à la détection et à la suppression des manipulations de l'information sur

1. Christophe Deloire, cité dans François Bougon, « Un label pour redonner confiance dans le journalisme », *Le Monde*, 3 avril 2018.

2. Ben Nimmo, « Investigative standards for analyzing information operations », à paraître.

3. Le *takedown* est une procédure par laquelle les plateformes suppriment des contenus illicites ou contrevenant à leurs règles (dans le cas de Facebook, par exemple, cette procédure vise des pages ou des comptes ayant un « comportement inauthentique coordonné »).

348977AEJ_INFORMATION_cc2019_pc.indd 382 16/09/2020 16:48:46

© Humensis

leurs sites. À la conférence de sécurité de Munich en février 2020, Marc Zuckerberg a ainsi rappelé qu'à Facebook 35 000 personnes scrutaient la plateforme pour détecter des contenus problématiques et que, avec l'aide de l'intelligence artificielle, plus d'un million de faux comptes étaient supprimés chaque jour.

Les limites des mesures prises

L'ensemble des mesures présentées dans les pages précédentes peut sembler impressionnant. Il est indéniable qu'en l'espace de quelques années, la prise de conscience a été réelle et que les États, les organisations internationales, la société civile et même les plateformes numériques ont fait d'importants progrès dans la lutte contre les manipulations de l'information. Les défis restent toutefois considérables pour les raisons suivantes.

Premièrement, la vérification des faits est nécessaire mais insuffisante, pour au moins deux raisons. La première est que son efficacité est discutée. De nature corrective, elle est par définition *post facto*, elle arrive quand le mal est fait sans pouvoir effacer l'impact psychologique de l'information fausse ou biaisée. En outre, les études montrent que le cerveau humain est résistant à la correction et que la plupart des gens continuent de diffuser une information dont ils reconnaissent la fausseté. Et la correction peine à atteindre sa cible à cause d'une sorte de parallélisme des audiences, les personnes étant les plus susceptibles de lire des fausses nouvelles sur des sites douteux et d'être convaincues par elles n'étant en général pas les mêmes qui fréquentent les sites sérieux vérifiant les faits[1].

La deuxième raison est que ce qui compte n'est pas tant les faits que les histoires. Peu importe au fond que nous ayons raison : tant que nos adversaires auront de meilleures histoires, ils gagneront.

1. Voir dans ce volume le chapitre de Divina Frau-Meigs.

348977AEJ_INFORMATION_cc2019_pc.indd 383 16/09/2020 16:48:46

© Humensis

Corriger de fausses informations n'empêchera pas qu'elles soient propagées, parce que ce qu'une certaine frange de la population recherche ce sont de « bonnes histoires », qu'elles soient vraies ou pas. Comme l'explique bien Ben Nimmo, nous ne sommes pas tant dans une « guerre de l'information » (*information warfare*) que dans une « guerre de récit » (*narrative warfare*). De ce point de vue, corriger une fausse information ne suffit pas, il faut réussir à imposer un autre récit, à raconter une bonne histoire. Laquelle ? Celle de l'attaque, répond Nimmo. C'est ce qui a fonctionné dans le cas des « Macron Leaks » : quelques analyses en temps réel ont permis de réorienter l'attention de l'opinion publique qui s'intéressait moins au contenu des « leaks » qu'à l'origine de l'attaque et aux liens que ces mystérieux acteurs pouvaient entretenir avec un parti politique français ou des puissances étrangères. Et cela était déjà une victoire[1].

Deuxièmement, il est indéniable que la lutte contre les manipulations de l'information peut constituer une menace pour les valeurs démocratiques et libérales, en particulier la liberté d'expression. Le fait que des mesures apparemment similaires soient prises dans des démocraties libérales et des autocraties en est la preuve. Pour que les premières maintiennent un équilibre sain entre sécurité et liberté, qui est au cœur du contrat social, et se préservent de la comparaison avec les régimes autoritaires, elles doivent adopter un principe directeur selon lequel l'État n'est pas et ne doit pas être la première ligne de défense contre les manipulations de l'information : ce sont les citoyens, la société civile, en particulier les journalistes, les vérificateurs de faits et les chercheurs, qui le sont. C'est pourquoi la première des recommandations aux États dans notre rapport de 2018 était d'« avoir une empreinte légère[2] » – approche notamment adoptée dans le plan canadien présenté en janvier 2019, qui ne présume pas que l'État doit protéger des citoyens passifs, mais veut

1. Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 39-40.

2. Jean-Baptiste Jeangène Vilmer *et al.*, *Les Manipulations de l'information…*, *op. cit.*, p. 173.

348977AEJ_INFORMATION_cc2019_pc.indd 384 16/09/2020 16:48:46

© Humensis

les former pour leur donner les moyens de détecter eux-mêmes les manipulations.

Troisièmement, les vertus de la transversalité sont désormais reconnues – il est évident pour tout le monde que, pour se défendre contre les manipulations de l'information, il faut faire travailler ensemble des services voire des ministères différents –, mais toutes les cultures administratives n'y sont pas aussi réceptives. Certains pays (scandinaves, baltes, Canada) y parviennent mieux que d'autres dont la bureaucratie est plus lourde et encore très « ensilotée », avec parfois des rivalités interservices qui paralysent l'action. Tous n'ont pas la souplesse de pouvoir créer un Centre pour la politique numérique internationale comme celui du ministère canadien des Affaires mondiales, une équipe unique mêlant analystes politiques et « geeks » spécialistes des réseaux sociaux, un modèle du genre.

Quatrièmement, beaucoup d'États se focalisent sur les élections et on peut le comprendre, non seulement parce qu'elles sont l'une des incarnations de la démocratie (on doit donc les protéger au même titre que les « infrastructures critiques » qui permettent à nos sociétés de fonctionner : électricité, ponts, réseau ferré, télécommunications, hôpitaux, etc.) mais aussi parce qu'il est consensuel et bipartisan de vouloir les protéger. Néanmoins, on ne doit pas perdre de vue que les attaques – qu'elles soient cyber ou informationnelles – sont quotidiennes. Les mesures prises ne peuvent donc pas être limitées aux périodes électorales.

Cinquièmement et de la même manière, beaucoup d'États se focalisent sur l'ingérence, c'est-à-dire l'intervention étrangère, les menaces « exogènes ». Or, tous les praticiens de la lutte contre les manipulations de l'information le constatent : il n'est pas toujours facile – il est même souvent difficile et parfois impossible – de distinguer entre une manipulation d'origine « étrangère » (qu'on peut donc appeler une ingérence) et une manipulation d'origine intérieure. C'est d'autant plus difficile que nos adversaires jouent sur l'ambiguïté, en ayant recours à des proxies non étatiques, en s'appuyant sur des opérateurs nationaux. Les États sont assez démunis car ce ne sont généralement pas les mêmes services qui luttent contre les menaces extérieures et

348977AEJ_INFORMATION_cc2019_pc.indd 385 16/09/2020 16:48:46

© Humensis

contre les menaces intérieures : l'ambiguïté de la menace implique donc la transversalité de la défense. Elle nous force à faire tomber les barrières entre services, à faire davantage circuler l'information, ce qui n'est pas dans les habitudes de toutes les bureaucraties.

Sixièmement, à l'échelle européenne, l'organisation de la réponse du SEAE en trois équipes géographiques très déséquilibrées – le front « Est », c'est-à-dire russe, concentrant l'essentiel des moyens – ne convainc pas tous les pays, notamment ceux qui s'estiment à un carrefour entre l'Est et le Sud et/ou défendent une vision à 360°. La focalisation explicite sur la Russie, et demain peut-être aussi sur la Chine, dans tous les cas sur une menace spécifique, peut contribuer à diviser les États européens entre ceux qui assument cette opposition et les autres qui ne veulent pas apparaître « anti-Russes » ou, demain, « anti-Chinois ». En outre, la logique géographique a ses limites : les Russes, par exemple, sont très actifs en Afrique, y compris contre les intérêts européens[1]. L'« Est » est aussi au « Sud » et réciproquement. Plutôt qu'avoir trois équipes géographiques déséquilibrées, on pourrait donc imaginer un seul service luttant non pas contre telle ou telle menace étatique identifiée mais contre les manipulations de l'information d'où qu'elles viennent, y compris d'ailleurs d'acteurs non étatiques[2].

Septièmement, les formats de coopération existants (UE, OTAN, G7) sont utiles mais imparfaits, trop larges ou trop étroits, car créés pour autre chose, et dans tous les cas trop hétérogènes, les positions sur la question de savoir si les manipulations de l'information constituent une menace sérieuse étant perçues en fonction des intérêts de chacun et en particulier des relations que ces États

1. Shelby Grossman, Daniel Bush et Renée DiResta, « Evidence of Russia-linked influence operations in Africa », Working Paper, Freeman Spogli Institute for International Studies, Stanford University, 29 octobre 2019. En octobre 2019, Facebook a également supprimé trois réseaux de comptes ayant un « comportement inauthentique coordonné », attribués à des acteurs russes visant des pays africains. Voir https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-russia.

2. Voir aussi les recommandations de James Pamment, The EU's Role in Fighting Disinformation: Taking Back the Initiative, Carnegie Endowment for International Peace, 15 juillet 2020.

348977AEJ_INFORMATION_cc2019_pc.indd 386 16/09/2020 16:48:46

© Humensis

ont ou souhaitent avoir avec ceux généralement présentés comme les principales menaces en la matière, à savoir la Russie et la Chine. Les divergences sont donc nombreuses, avec parfois des obstructions caractérisées, ce qui non seulement rend les décisions plus lentes et moins efficaces mais peut aussi parfois susciter un climat de méfiance entre les membres. C'est pourquoi se multiplient les appels à la constitution plus ou moins formelle d'une alliance *ad hoc* d'États démocratiques, partageant les mêmes valeurs et les mêmes préoccupations, pour partager de bonnes pratiques et formuler des demandes conjointes, notamment aux plateformes numériques[1].

Huitièmement, les plateformes numériques, très critiquées, ont fait des progrès importants en matière de partage d'information ces dernières années. On ne peut plus leur reprocher de ne rien faire, comme c'était sans doute le cas à une époque. On peut toutefois exiger qu'elles fassent toujours davantage, et surtout qu'elles fassent preuve de davantage de transparence quant aux mesures prises. Lorsque Facebook quelques jours avant un *takedown* en donne la primeur à Graphika, par exemple, il leur communique les pages ou les comptes concernés avant de les supprimer au motif qu'ils sont liés au renseignement militaire russe par exemple[2], mais Facebook ne dit pas comment ils sont arrivés à cette conclusion. La communauté des chercheurs doit donc les croire sur parole, ou développer des moyens propres de confirmer – ou d'infirmer – cette attribution[3]. Bien entendu, le partage d'informations aussi sensibles que

1. Dan Fried et Alina Polyakova, *Democratic Defense Against Disinformation*, Atlantic Council, 5 mars 2018 ; Jean-Baptiste Jeangène Vilmer, *The « Macron Leaks » Operation : A Post-Mortem*, *op. cit.*, p. 46.

2. Ben Nimmo, Camille François, C. Shawn Eib, L. Tamora, « From Russia with blogs », Graphika, 12 février 2020.

3. L'attribution, qui consiste à déterminer qui est à l'origine d'une opération cyber, est notoirement difficile, voire impossible dans de nombreux cas, compte tenu de la complexité d'identifier le système informatique utilisé. Et, quand bien même remonterait-on jusqu'à un ordinateur, cela ne dirait pas qui se trouve derrière et si cette personne agit de sa propre initiative ou sous le contrôle d'un État. Sur la manière dont Facebook traite les difficultés de l'attribution, voir Alex Stamos, « How much can companies know about who's behind cyber threats ? », Fb.com, 31 juillet 2018.

348977AEJ_INFORMATION_cc2019_pc.indd 387 16/09/2020 16:48:46

© Humensis

celles ayant permis l'attribution reviendrait à exposer des méthodes de détection, ce qui profiterait aux attaquants qui trouveraient, la prochaine fois, le moyen de les contourner. La question est donc celle de savoir si les plateformes numériques pourraient développer des moyens de partager des informations confidentielles (et devant le rester) avec des gouvernements mais aussi quelques chercheurs de confiance, en distinguant plusieurs niveaux d'accès.

Pour aller plus loin :

Commission Européenne, Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions, intitulée « Lutter contre la désinformation en ligne : une approche européenne », 26 avril 2018.

Chambre Des Communes Du Royaume-Uni, Comité Pour Les Médias, Le Sport Et La Culture, *Disinformation and « Fake News »*. *Final Report*, 14 février 2019. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf.

Jeangène Vilmer Jean-Baptiste, Escorcia Alexandre, Guillaume Marine, Herrera Janaina, *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, Paris, août 2018.

Jeangène Vilmer Jean-Baptiste, *The Macron Leaks Operation : A Post-Mortem*, Paris/Washington DC, IRSEM/Atlantic Council, 2019.

Jeangène Vilmer Jean-Baptiste, Charon Paul, « Russia as a hurricane, China as climate change : Different ways of information warfare », *War on the Rocks*, 21 janvier 2020.

Pamment James, *The EU's Role in Fighting Disinformation : Taking Back The Initiative*, Carnegie Endowment for International Peace, 15 juillet 2020.

Rapport du comité d'étude singapourien sur les fausses informations délibérées en ligne (*Deliberate Online Falsehoods*). https://www.rajahtannasia.com/media/pdf/Exec_Summary_Rpt_on_Deliberate_Online_Falsehoods.pdf.