LES MANIPULATIONS DE L'INFORMATION

Un défi pour nos démocraties

Un rapport du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées)

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

MINISTÈRE
DES ARMÉES

AUTEURS

Jean-Baptiste Jeangène Vilmer, Alexandre Escorcia, Marine Guillaume, Janaina Herrera.

À PROPOS DU CAPS ET DE L'IRSEM

Le Centre d'analyse, de prévision et de stratégie (CAPS), créé en 1973, est rattaché au ministre de l'Europe et des Affaires étrangères. Composé d'une vingtaine d'experts, diplomates ou universitaires, il produit, pour le ministre et pour les autorités françaises, des analyses transdisciplinaires et prospectives des évolutions de moyen et long termes de l'environnement international et présente des recommandations politiques et des options stratégiques sur la politique étrangère, sur la base de sa propre réflexion et de son interaction avec le monde des think tanks et de la recherche universitaire en relations internationales.

L'Institut de recherche stratégique de l'École militaire (IRSEM), créé en 2009, est un institut de recherche du ministère des Armées. Composé d'une quarantaine de personnes, civiles et militaires, dont la plupart sont titulaires d'un doctorat, il est le premier centre de recherche en études sur la guerre (*War Studies*) dans le monde francophone. En plus de conduire de la recherche interne (au profit du ministère) et externe (à destination de la communauté scientifique) sur les questions de défense et de sécurité, l'IRSEM apporte un soutien aux jeunes chercheurs (la « relève stratégique ») et contribue à l'enseignement militaire supérieur et au débat public.

Pour citer ce rapport
J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. 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.

Ce rapport est publié en français et en anglais (original en français et traduction en anglais).

Imprimé à Paris en août 2018.

ISBN : 978-2-11-152606-8

Couverture © Antonio/Getty Images.

LES MANIPULATIONS DE L'INFORMATION

Un défi pour nos démocraties

Un rapport du Centre d'analyse, de prévision et de stratégie (CAPS, ministère de l'Europe et des Affaires étrangères) et de l'Institut de recherche stratégique de l'École militaire (IRSEM, ministère des Armées)

SOMMAIRE

AVANT-PROPOS

Notre enquête

Notre enquête est le produit d'une prise de conscience en deux temps du danger – existentiel – que les manipulations de l'information font peser sur nos démocraties. D'abord, les ingérences répétées qui se sont produites depuis 2014 (Ukraine, Bundestag, référendum néerlandais, Brexit, élection américaine) ont prouvé que les démocraties occidentales, même les plus grandes, n'étaient pas immunes. Ensuite, la tentative d'ingérence dans l'élection présidentielle française de 2017, avec l'affaire dite des « Macron Leaks », a achevé d'intéresser la France et nous a convaincus de l'importance d'étudier le sujet.

En septembre 2017, nous avons donc décidé, de notre propre initiative, de constituer un groupe de travail réunissant quelques membres 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, initialement pour envisager l'opportunité d'une cellule interministérielle de lutte contre les manipulations de l'information, mais plus fondamentalement pour étudier le problème, ses causes, ses conséquences et ses solutions.

Ce groupe de travail devait être interministériel pour répondre à la nature intrinsèquement interdisciplinaire des manipulations de l'information, à l'intersection des relations internationales, des études sur la guerre, sur le renseignement, sur les médias, de la sociologie et de la psychologie

sociale ; et au fait que, par voie de conséquence, le sujet concerne plusieurs administrations.

Ce groupe de travail devait être focalisé sur l'international, compte tenu non seulement de nos intérêts propres mais aussi de la nature transnationale d'un phénomène qui se joue des cadres de la souveraineté et de la territorialité des systèmes juridiques. Si certains cas sont plus connus que d'autres, les manipulations de l'information sont universelles. Elles préoccupent les sociétés civiles et les gouvernements d'un grand nombre d'États, non seulement en Europe et en Amérique du Nord, mais aussi en Asie, au Moyen-Orient, en Afrique et en Amérique latine. Mais les manipulations de l'information sont aussi multiformes, et chaque cas est différent, car taillé sur mesure pour la communauté ciblée.

Il faut notamment distinguer, d'une part, entre les manipulations exogènes, provenant de l'extérieur de l'État visé, et les manipulations endogènes, provenant de l'intérieur et, d'autre part, entre celles causées par des acteurs étatiques et celles causées par des acteurs non étatiques. Comme il était impossible de tout couvrir, et que notre angle est à l'intersection des affaires étrangères et de la défense, nous avons choisi de nous limiter, dans ce rapport, à l'étude des manipulations de l'information d'origine étatique et étrangère, c'est-à-dire aux ingérences.

Au cours des derniers mois, nous avons donc visité vingt pays (Allemagne, Autriche, Belgique, Canada, Danemark, Espagne, Estonie, États-Unis, Finlande, Italie, Japon, Lettonie, Pays-Bas, Pologne, République tchèque, Royaume-Uni, Russie, Singapour, Suède, Ukraine) et trois organisations (UE, OTAN, OSCE). Nous y avons conduit une centaine d'entretiens avec les autorités (ministères des Affaires étrangères, de la Défense et services de renseignement) et des représentants de la société civile (universitaires, think tanks, ONG, journalistes), pour savoir quelles étaient leur perception de la menace et les contre-mesures mises en place. Nous avons aussi mené des entretiens en France, avec les autorités, la société civile et des acteurs privés, et travaillé à partir de la littérature scientifique disponible, dont un aperçu se trouve en bibliographie.

Nous avons produit une quinzaine de notes internes pour les ministères et services concernés, une note publique[1] et plusieurs événements dont un cycle de séminaires à l'IRSEM sur les « guerres de l'information » et un colloque international organisé par le CAPS, ouvert par la ministre de la Culture et clos par un discours du ministre de l'Europe et

1. Maud Quessard, *La Diplomatie publique américaine et la désinformation russe : un retour des guerres de l'information ?*, Note de recherche de l'IRSEM, n° 54, 30 avril 2018.

des Affaires étrangères qui reste à ce jour l'expression officielle la plus précise sur le sujet.

Dans son discours, le ministre mentionnait le présent rapport, alors en préparation, qui est le principal résultat de nos recherches. Il souhaitait pouvoir en « tirer les enseignements[2] ». C'est aussi ce que nous espérons. Pour autant, ce rapport n'est pas et ne doit pas être considéré comme une position officielle du gouvernement français. Le CAPS et l'IRSEM jouissent d'une certaine liberté de ton au sein de leurs ministères respectifs. Notre groupe, composé de chercheurs et de diplomates, a travaillé en toute indépendance.

Ce rapport n'est pas non plus une position définitive : nous continuerons à l'avenir d'explorer le sujet, dans les limites de nos compétences, notamment pour tenter de mettre au jour les mutations de ce phénomène qui continuera de marquer la vie de nos démocraties sous des formes toujours renouvelées.

2. « Le centre d'analyse, de prévision et de stratégie de mon ministère, avec l'Institut de recherche stratégique de l'École militaire, finalise en ce moment un rapport recueillant les analyses et les meilleures pratiques de nos partenaires, des chercheurs, des médias et des organisations des sociétés civiles à l'échelle internationale. Je souhaite que nous puissions en tirer les enseignements » (Jean-Yves Le Drian, *Discours de clôture de la conférence internationale « Sociétés civiles, médias et pouvoirs publics : les démocraties face aux manipulations de l'information »,* Paris, 4 avril 2018).

RÉSUMÉ

Les manipulations de l'information ne sont pas un phénomène nouveau. Leur actualité récente est liée à la combinaison de deux facteurs : d'une part, les capacités inédites de diffusion rapide et de viralité offertes par internet et les réseaux sociaux, couplées, d'autre part, à la crise de confiance que vivent nos démocraties et qui dévalue la parole publique allant jusqu'à relativiser la notion même de vérité.

Les élections américaine de 2016 et française de 2017 ont jeté une lumière crue sur ce phénomène, ses ressorts et ses conséquences. Pour autant, l'impact des manipulations de l'information, dans certains cas leur existence même, sont parfois remis en cause. Ne sommes-nous pas dans le cadre du débat démocratique, dont les excès peuvent être corrigés par la législation en vigueur ? L'accent mis par un certain nombre de gouvernements sur les « fausses nouvelles » n'est-il pas un moyen commode de se dédouaner ou de pointer du doigt de prétendus ennemis de la démocratie, y compris extérieurs, afin de consolider sa propre position politique ? Voire un prétexte insidieux pour remettre en cause les libertés publiques, et avant tout la liberté d'expression ?

Ces objections sont sérieuses. Elles exigent un examen approfondi, afin de cerner autant que possible ce que sont et ce que ne sont pas les manipulations de l'information. Le présent rapport propose ainsi une définition du problème en substituant à la notion trop vague et polémique de

fake news celle, plus précise, de manipulation de l'information, entendue comme la diffusion intentionnelle et massive de nouvelles fausses ou biaisées à des fins politiques hostiles. Ce rapport s'intéresse avant tout aux manipulations de l'information d'origine étatique et visant à fragiliser ou à déstabiliser le débat démocratique dans d'autres États.

À partir de cette définition, de nos entretiens dans une vingtaine de pays et d'une revue aussi complète que possible de l'abondante littérature sur le sujet, ce rapport procède de la façon suivante. D'abord, il s'intéresse au « pourquoi ? », aux causes des manipulations de l'information, qui sont à la fois individuelles, liées à la nature humaine, relevant donc de la psychologie et de l'épistémologie (des failles cognitives et une crise de la connaissance) et collectives, liées à la vie en société (une crise de confiance dans les institutions, une crise de la presse et une désillusion à l'égard du numérique). Après avoir analysé chacune de ces causes, nous voyons qui en profite, c'est-à-dire qui sont les acteurs des manipulations de l'information, en nous focalisant sur les États qui manipulent à l'extérieur, c'est-à-dire qui s'ingèrent.

Ensuite, ce rapport s'intéresse au « comment ? » : il met en avant des traits distinctifs des récentes campagnes de manipulation de l'information, afin d'en dégager quelques caractéristiques communes, en termes de facteurs de vulnérabilité (la présence de minorités, des divisons internes, des divisions externes, un écosystème médiatique vulnérable, des institutions contestées) et de moyens (des leviers et des vecteurs multiformes, des narratifs calibrés, des lieux et des mécanismes privilégiés, la fuite massive de documents, la falsification de documents, les ingérences électorales). Nous explorons d'autres terrains des manipulations de l'information – autres par rapport à l'espace post-soviétique, l'Europe et l'Amérique du Nord qui sont les plus connus – et notamment le Moyen-Orient, l'Afrique et l'Amérique latine.

Dans une troisième partie consacrée aux réponses, nous faisons la synthèse des contre-mesures adoptées par tous les acteurs : États, organisations internationales, société civile et acteurs privés, en commençant par une étude sur les « Macron Leaks », qui reste un cas à part dans l'histoire récente des tentatives d'ingérence dans les campagnes électorales puisque celle-ci a échoué. Il convient donc de comprendre pourquoi, et d'en tirer des leçons.

Pour finir, nous tentons de dessiner quels seront les défis futurs – défis technologiques, futures tendances de la « guerre de l'information » russe, scénarios possibles – avant de formuler 50 recommandations, partant du

principe que les manipulations de l'information continueront de constituer un défi de longue haleine pour nos démocraties, auquel elles devront apporter une réponse participative, libérale et respectueuse des droits fondamentaux. En guise de post-scriptum, nous proposons enfin quelques réponses aux objections, afin d'anticiper les critiques les plus communes.

L'information est de plus en plus considérée comme un bien commun, dont la protection échoit à tous les citoyens préoccupés par la qualité du débat public. C'est avant tout à la société civile de développer sa propre résilience. Les gouvernements ne peuvent et ne doivent venir qu'en appui de cet effort, mais ils ont un rôle clé, tant ils ne peuvent se désintéresser d'une menace qui vise à miner les fondements de notre démocratie et donc, *in fine*, de notre sécurité nationale.

INTRODUCTION

La manipulation – par production, rétention ou déformation – est aussi vieille que l'information, c'est-à-dire que la vie en société, puisqu'elle lui est consubstantielle. Elle est partie prenante des ruses de guerre, qui ont toujours existé. Avant la bataille de Qadesh en 1274 avant notre ère, par exemple, les Hittites auraient utilisé de fausses informations transmises aux Égyptiens, pour influer sur le sort du conflit. La manipulation de l'information est théorisée depuis l'Antiquité, au travers d'ouvrages comme l'*Arthashâstra* indien du IVe siècle avant notre ère, les *Dialogues* de Platon et la *Rhétorique* d'Aristote[1] ou encore, plus récemment, *L'Art de persuader* de Pascal (1660) ou *L'Art d'avoir toujours raison* d'Arthur Schopenhauer (1830). L'historien Robert Darnton montre comment ces fausses nouvelles ont bénéficié du développement de la presse écrite, notamment les brochures sensationnalistes françaises (« canards » parisiens) et anglaises aux XVIIe et XVIIIe siècles[2].

Ne serait-ce qu'au XXe siècle, la désinformation a une longue histoire[3], dont les *Protocoles des Sages de Sion* (1901) constituent un premier exemple fameux. Le totalitarisme a joué un rôle de catalyseur et la guerre froide a

1. Alexandre Koyré, *Réflexions sur le mensonge*, Allia, 2004.

2. Robert Darnton, « On retrouve tout au long de l'histoire l'équivalent de l'épidémie actuelle de "fake news" », *Le Monde*, 20 février 2017. Voir son article « The True History of Fake News », *The New York Review of Books*, 13 février 2017.

3. Vladimir Volkoff, *Petite Histoire de la désinformation*, Éd. du Rocher, 1999.

eu aussi son lot d'épisodes célèbres, avec les campagnes soviétiques voulant attribuer à un complot de la CIA l'assassinat de Kennedy (1963) ou l'épidémie du sida (opération Infektion, 1983-1987[4]). En 1962, le juriste et sociologue Jacques Ellul estime que la propagande « est devenue un phénomène très général dans le monde moderne[5] ».

En dépit – ou peut-être à cause – de cette longue histoire, le sujet souffre d'une confusion terminologique évidente : il existe une profusion de termes utilisés comme synonymes, ou sans être préalablement définis, dont les principaux sont « propagande », « désinformation », *fake news* et « post-vérité » mais aussi tous types de « guerre » (de l'information, psychologique, politique, idéologique, subversive, hybride, etc.). C'est grâce à cette confusion que certains peuvent comparer RT avec la BBC ou France 24, par exemple, ou minorer le problème en expliquant que « tout est propagande ». Une clarification terminologique s'impose donc comme un préalable indispensable. Dans cette introduction, nous allons passer en revue différents vocables pour finalement défendre la terminologie qui nous semble le mieux adaptée à la situation, celle de « manipulation de l'information ». Il s'agit d'en cerner précisément les contours et de démontrer que la question n'est pas un faux débat, compte tenu de la grande capacité de nuisance et de l'efficacité de ces manipulations.

I. De quoi parle-t-on ?

Le sujet est traversé par une terminologie abondante et imprécise, mêlant des notions classiques (influence, propagande, désinformation) avec des néologismes (*fake news*, post-vérité, *fact-checking*) dont la multiplication « signale l'incapacité du vocabulaire existant à décrire un monde social en pleine transformation[6] ». Partir sur de bonnes bases implique donc de commencer par faire le tri dans cette profusion de termes, pour écarter les plus vagues et proposer une définition précise du phénomène concerné.

– *Fake news* est l'expression la plus communément employée, y compris en français, où elle est parfois traduite par « fausses informations » alors qu'il faudrait plutôt parler d'informations falsifiées, contrefaites ou

4. Thomas Boghardt, « Operation Infektion: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign », *Studies in Intelligence*, 53:4, 2009, p. 1-24.

5. Jacques Ellul, *Propagandes*, Armand Colin, 1962, p. 5.

6. Jayson Harsin, « Un guide critique des *Fake News* : de la comédie à la tragédie », *Pouvoirs*, n° 164, janvier 2018, p. 99.

forgées. Le terme a été popularisé par l'émission satirique américaine *The Daily Show* depuis 1999, qui assumait de truquer l'information pour faire rire, comme le journal *The Onion*. Cette première génération, humoristique, a duré une quinzaine d'années. Depuis la campagne présidentielle américaine de 2016, l'usage du terme a littéralement explosé (+ 365 % en 2017 selon le dictionnaire Collins qui l'a alors nommé « mot de l'année ») mais son acception a changé, dans un tournant « de la comédie à la tragédie[7] ». Comme le groupe d'experts européen de haut niveau sur les fausses informations et la désinformation en ligne[8], nous le rejetons pour au moins deux raisons : d'une part, parce qu'il est trop vague et ne permet pas de rendre compte du fait qu'une partie du problème vient aussi d'informations qui ne sont pas « fausses » à strictement parler. D'autre part, parce que le terme est devenu tellement galvaudé qu'il en vient parfois, et même chez certains chefs d'État, à désigner l'ensemble des nouvelles qu'ils n'aiment pas, et finalement à incarner une forme de populisme hostile à la liberté de la presse.

– La notion de « guerre politique » (*political warfare*), qui couvre l'ensemble des moyens non militaires et non létaux, ou même celle de son sous-domaine « guerre de l'information » (*information warfare*), sont trop larges et présentent la spécificité de militariser le champ informationnel et donc les études qui lui sont consacrées. C'est aussi le cas de « guerre hybride », notion répandue mais néanmoins confuse, qui désigne en réalité une guerre menée sur l'ensemble du spectre, du conventionnel à l'informationnel en passant par le cyber, les opérations clandestines et l'intimidation nucléaire[9]. Elle est donc encore plus large que les catégories précédentes, puisqu'elle articule le non-cinétique, dont l'informationnel relève, avec le cinétique.

– La « propagande », définie comme « une tentative d'influencer l'opinion et la conduite de la société de telle sorte que les personnes adoptent une opinion et une conduite déterminée[10] », est également trop vague et, surtout, elle s'applique mal à notre objet, car elle implique la défense d'une vision du monde alternative, élément qui fait précisément défaut aux phénomènes actuels, essentiellement centrés sur le dénigrement des autres.

7. *Ibid.*

8. European Commission, *A Multi-Dimensional Approach to Disinformation, Report of the Independent High Level Group on Fake News and Online Disinformation*, mars 2018, p. 10.

9. Pour une critique du vocable de la guerre hybride et de sa prétendue nouveauté, voir Joseph Henrotin, *Techno-guérilla et guerre hybride : le pire des deux mondes*, Nuvis, 2014 et Élie Tenenbaum, *Le Piège de la guerre hybride*, Focus stratégique n° 63, IFRI, octobre 2015.

10. Jean-Marie Domenach, *La Propagande politique,* PUF, 1965, p. 8.

– L'« influence » et la « diplomatie publique » sont également très larges et, surtout, elles ne sont pas en soi problématiques – tous les États qui en ont les moyens ont des stratégies d'influence servies notamment par une diplomatie publique. Cela permet de répondre à l'argument commun selon lequel RT et Sputnik, par exemple, ne sont que les équivalents russes des grands médias occidentaux. La rédactrice en chef de RT répète que « Nous ne donnons pas le point de vue du Kremlin mais celui de la Russie, comme France 24 ou la BBC, qui montrent les valeurs de la France et de la Grande-Bretagne, ou Al-Jazeera pour le monde arabe[11] ». Or, ce qui est reproché à RT et à Sputnik n'est pas de faire de la diplomatie publique, mais de manipuler l'information, ce qui n'est pas la même chose.

– La « désinformation » est généralement définie comme la diffusion d'informations délibérément fausses ou trompeuses. Elle se distingue de la « mésinformation » (*misinformation*), qui n'est pas intentionnelle. Le problème bien entendu est que l'intention est rarement claire[12] et ne peut être que supposée. La désinformation reste le moins mauvais des vocables courants, mais il est à la fois trop large et trop étroit. Trop large car il inclut la désinformation bénigne, sans intention hostile, même si ses conséquences peuvent être réelles, comme en 1938 lorsqu'Orson Welles sema la panique aux États-Unis avec son adaptation radiophonique de *La Guerre des mondes*, qui amena la population à croire à une attaque extraterrestre. Diffuser intentionnellement de fausses informations n'est pas en soi problématique : nous devons nous concentrer sur celles qui ont un effet négatif ou au moins une intention hostile. En même temps, le concept est aussi trop étroit car tous les problèmes que nous rencontrons ne sont pas de la désinformation *stricto sensu*. Parfois, l'information n'est pas fausse mais simplement exagérée, ou biaisée, ou présentée de façon très émotionnelle comme peuvent le faire les tabloïds. L'information peut être manipulée de nombreuses manières, par la production, la diffusion et même la rétention d'informations. Tous les procédés n'impliquent pas une dichotomie entre le vrai et le faux. La plupart du temps, le manipulateur ne se positionne pas par rapport à la vérité : il cherche simplement à produire un effet. Pour cette raison, réduire le problème à de la désinformation est trompeur.

Pour rendre compte de cette complexité, certains, dont le groupe d'experts européen, définissent la désinformation comme désignant des

11. Margarita Simonian, alors rédactrice en chef de Russia Today et Sputnik, citée par Isabelle Mandraud, « Les médias, machine de guerre du Kremlin », *Le Monde*, 25 novembre 2015, p. 2.

12. Caroline Jack, *Lexicon of Lies: Terms for Problematic Information*, Data & Society Research Institute, 2017, p. 4.

« informations dont on peut vérifier qu'elles sont fausses ou trompeuses, qui sont créées, présentées et diffusées dans un but lucratif ou dans l'intention délibérée de tromper le public et qui sont susceptibles de causer un préjudice public » – une définition reprise dans différentes publications, dont un rapport gouvernemental irlandais et un rapport d'un groupe d'experts belge[13].

Il nous semble préférable, car plus inclusif, d'utiliser le terme générique de « manipulation ». La manipulation est délibérée (elle suppose l'intention de nuire) et clandestine (ses victimes en sont inconscientes). Nous nous intéressons aux manipulations de l'information cumulant trois critères : une campagne coordonnée, de diffusion de nouvelles fausses ou sciemment déformées, avec l'intention politique de nuire.

La notion de campagne coordonnée renvoie moins à l'idée d'une opération orchestrée avec donneurs d'ordre et exécutants qu'à un faisceau d'indices indiquant qu'à travers plusieurs médias, se déroule simultanément un ensemble d'actions provenant de différentes sources humaines et non humaines tendant toutes à la diffusion d'un certain contenu problématique (Twitter, Facebook, blogueurs, repris par des institutionnels type ambassades, puis par des émetteurs type RT, Sputnik, WikiLeaks, etc.).

Nous avons donc fait le choix de mettre en avant l'intentionnalité politique de la campagne de manipulation de l'information comme critère déterminant. L'intention politique de nuire est entendue au sens large, et ne signifie pas que le champ soit limité aux affaires politiques ou nationales : la campagne peut vouloir saper la légitimité d'un processus électoral, ruiner la réputation d'une grande entreprise à l'international, ou encore vouloir susciter un environnement hostile pour une opération militaire extérieure.

Nous excluons de fait du champ d'étude de ce rapport les nombreuses manipulations de l'information dont l'intention n'est ni politique ni hostile.

En revanche, il ne faut pas distinguer trop nettement, comme on le fait parfois, les manipulations commerciales, dont l'intention serait de faire de l'argent, et qui pour cette raison sont souvent dépolitisées par ceux qui les analysent, des manipulations politiques, qui nous intéressent ici. Car non seulement les premières peuvent avoir, qu'elles le veuillent ou non, des effets politiques bien réels, mais les secondes peuvent aussi faire gagner

13. Government of Ireland, *First Report of the Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation*, prepared by the Department of the Taoiseach, juin 2018 et Alexandre Alaphilippe *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, juillet 2018.

de l'argent aux médias, aux plateformes numériques, voire à des adolescents macédoniens[14]. Autrement dit, les intérêts politiques et économiques s'entremêlent.

Nous défendons l'expression « manipulations de l'information » dans des notes internes depuis début 2018. Le ministre de l'Europe et des Affaires étrangères Jean-Yves Le Drian l'a fait publiquement dans son discours du 4 avril et, en mai, un amendement à la proposition de loi actuellement à l'étude au Parlement a également permis de le renommer, passant d'une loi « contre les fausses informations » à une loi « relative à la lutte contre la manipulation de l'information ». La communication française est donc cohérente sur ce point.

II. Les manipulations de l'information, un enjeu mineur ?

En 2013, le Forum économique mondial avait identifié la « mésinformation » en ligne comme l'une des dix tendances à suivre en 2014[15] – de façon prémonitoire puisque la désinformation a joué un rôle non négligeable dans la crise ukrainienne. Depuis, le sujet n'a cessé de croître. Tous les sondages confirment qu'il est une préoccupation majeure pour les populations, les journalistes, les ONG et les gouvernements dans le monde entier, qui reconnaissent les dommages que ces manipulations peuvent causer à la société[16]. Et cette prise de conscience ne fait que s'accroître, en étendue (davantage de pays s'y intéressent) comme en profondeur (les analyses sont toujours plus fouillées).

Cependant, il existe aussi une tendance répandue à minorer l'efficacité de ces manipulations, et donc l'importance du sujet. Cette tendance est moins visible dans les pays qui sont traditionnellement sensibilisés (Europe

14. Une enquête a révélé comment la ville de Veles, en Macédoine, était devenue une pépinière de fausses nouvelles et comment des jeunes, parfois adolescents, avaient de fait, sans aucune motivation politique, soutenu les pro-Trump dans la campagne américaine, tout simplement après avoir constaté que c'était la cause la plus profitable (les contenus pro-Trump étaient plus partagés, donc généraient plus de revenus publicitaires). Certains d'entre eux gagnaient ainsi près de 5 000 dollars par mois, dans un pays où le salaire moyen était à moins de 400 euros (Craig Silverman et Lawrence Alexander, « How Teens in the Balkans are Duping Trump Suppporters with Fake News », *BuzzFeed News*, 4 novembre 2016). Aujourd'hui, certains d'entre eux produisent toujours des fausses nouvelles à la chaîne mais ils gagnent beaucoup moins d'argent car depuis la révélation de l'affaire ils ne peuvent plus vendre à Google.

15. World Economic Forum, *Outlook on the Global Agenda 2014*, 2013, p. 28-29.

16. Voir par exemple la dernière consultation publique conduite par la commission européenne sur les fausses nouvelles et la désinformation en ligne entre novembre 2017 et février 2018 (*Synopsis report* du 26 avril 2018) et le *Reuters Institute Digital News Report 2018*, qui a sondé plus de 74 000 personnes dans 37 États.

centrale de l'Est et du Nord), ou ceux qui ont été les plus évidemment frappés et dont les enquêtes parlementaires en cours entretiennent ce sujet dans les discussions quotidiennes (États-Unis et Royaume-Uni). En revanche, ceux qui s'estiment à l'abri, ou qui se savent visés mais qui peuvent se prévaloir d'un succès – comme la France dans l'affaire dite des « Macron Leaks » (voir *infra*) –, sont plus susceptibles de minorer la menace. Il faut alors se battre, parfois au sein même du gouvernement, et dans le débat public, pour faire comprendre qu'il ne s'agit pas d'un enjeu mineur.

Pour ce faire, il peut être utile de rappeler que les manipulations de l'information, toutes virtuelles qu'elles peuvent paraître, ont de nombreux effets bien réels, et parfois physiques. Ne serait-ce que ces dernières années, elles ont interféré dans plusieurs processus démocratiques majeurs, dont les élections présidentielles des plus grandes puissances mondiales, et ont déstabilisé de grandes entreprises du numérique. Elles ont divisé les opinions publiques, semé le doute quant à la véracité des informations délivrées par les médias de référence, renforçant le rejet dont ces derniers peuvent faire l'objet. Elles ont joué un rôle dans des crises diplomatiques majeures (Ukraine, Syrie, Golfe). Elles ont favorisé la saturation des espaces numériques par des communautés de trolls pratiquant le harcèlement et l'intimidation. Avec parfois des conséquences funestes : les manipulations sur Facebook, à coups de fausses rumeurs et de photos retouchées, ont joué un rôle non négligeable dans la persécution des Rohingya en Birmanie, que les Nations unies ont qualifiée de nettoyage ethnique[17], voire de génocide[18]. À une échelle moindre, en seulement deux mois en Inde, en mai-juin 2018, une quinzaine de personnes ont été lynchées, dans tout le pays, suite à la diffusion de fausses rumeurs à leur endroit, ce qui a poussé les autorités à réagir en coupant temporairement l'accès à certaines plateformes numériques[19]. Le fait que de nombreux États se mobilisent et que la société civile multiplie les initiatives pour s'en prémunir, et que parallèlement se développe une véritable économie de la désinformation, avec ses usines à trolls, ses fermes à clics et ses entrepreneurs millionnaires[20],

17. Annie Gowen et Max Bearak, « Fake News on Facebook Fans the Flames of Hate Against the Rohingya in Burma », *The Washington Post*, 8 décembre 2017.

18. UN Doc. A/HCR/39/64 (24 août 2018).

19. Shweta Ganjoo, « Hindustan or lynchistan? May be Indians should not be allowed to use WhatsApp », *India Today*, 2 juillet 2018.

20. Voir notamment le cas du Mexicain Carlos Merlo, qui dit contrôler des millions de bots et des douzaines de sites. Son entreprise Victory Lab offre des services de « gestion de bots, *containment*, cyberattaques, et création de sites de *fake news* » pour des tarifs allant de 49 000 pesos (2 256 € au moment d'écrire ces lignes) pour un contrat de six mois à un million de pesos (46 000 €) par

est une preuve supplémentaire de la réalité et de l'efficacité – en tout cas économique et politique – de ces manipulations.

Pourtant, l'évaluation de l'efficacité des manipulations de l'information demeure une gageure, et aucune méthode n'est entièrement satisfaisante. Pendant et après la guerre froide, le renseignement américain commandait des sondages minutieux visant à mesurer précisément la perméabilité de groupes cibles aux campagnes de désinformation de Moscou[21]. Aujourd'hui, l'analyse des réseaux sociaux fournit des informations précieuses : elle permet de détecter des mouvements artificiels et coordonnés, de mesurer le nombre de personnes atteintes, c'est-à-dire le « tissu infecté », y compris en filtrant les comptes automatisés (bots). Mais le nombre de personnes atteintes ne dit pas si elles sont ou ont été convaincues et si la fausse information reçue va les faire passer à l'acte (donner ses coordonnées ou de l'argent, manifester, etc.). En outre, le nombre compte moins que la nature de la communauté touchée : un message qui ne toucherait que 2 % de la population pourrait avoir un effet important si ces 2 % sont violents et prêts à agir.

Une autre limite des méthodes utilisées est qu'elles font de l'analyse de texte, alors que les manipulations de l'information passent aussi par les images, qui sont beaucoup plus difficiles à analyser automatiquement. Dès lors, s'il apparaît crucial d'attirer l'attention sur le rôle d'une plateforme comme Facebook, d'autres réseaux (Instagram, WhatsApp) doivent aussi être remis en question. La désinformation par les images pose aussi la question de la manipulation visant les enfants.

Mesurer l'efficacité des manipulations de l'information est quasi impossible, car le lien entre un message diffusé et un comportement implique trop de facteurs. On peut toutefois distinguer *l'impact* dans l'environnement numérique, relativement mesurable car quantifiable (si l'on parvient à départager les vrais comptes des bots de plus en plus sophistiqués), de *l'effet* plus général qui ne peut être que supposé. On peut distinguer plusieurs effets.

---

mois. Voir Ben Nimmo *et al.*, « #ElectionWatch: Trending Beyond Borders in Mexico », Atlantic Council's Digital Forensic Research Lab, Medium.com, 28 juin 2018.

21. Les rapports spéciaux S réalisés par la communauté du renseignement pour l'Agence d'information des États-Unis. Le département de la Défense (via la Defense Intelligence Agency, DIA), le département d'État, la CIA comme l'USIA auparavant considèrent en effet les études en sciences sociales comme des outils incontournables pour la mise en œuvre de leurs stratégies respectives. L'Office of Research and Intelligence (INR) produit des dizaines de « Special S reports » (sondages, études de cas et d'impact), et collabore avec de nombreux départements et laboratoires de recherche universitaires. Ces rapports une fois déclassifiés sont consultables aux archives nationales des États-Unis : « Special "S" Reports », Entry 1009, Record Group 306, Box 17, Archives Nationales II, College Park, MD.

« Ne croyons pas que cela ne fonctionne pas. Nous savons que cela fonctionne, nous l'avons vu à l'œuvre à l'étranger mais aussi en France. Le processus démocratique s'en trouve profondément altéré parce que l'indignation que suscitent ces fausses nouvelles est éruptive et prend le dessus sur la réflexion. Et c'est d'ailleurs le pari en quelque sorte anthropologique qui est fait par ceux qui manipulent ces canaux. […] Des barrières ont été érigées mais les campagnes présidentielles d'à peu près toutes les démocraties contemporaines ont montré la faiblesse de celles-ci et notre incapacité collective à apporter des réponses qui sont à la hauteur aujourd'hui des menaces. »

(Emmanuel Macron, président de la République, discours à l'occasion des vœux à la presse, 4 janvier 2018.)

D'une part, un effet direct. La question est de savoir si les manipulations peuvent convaincre de nouvelles opinions ou si elles ne font que conforter des opinions existantes. De notre enquête, il ressort que l'effet de ces manipulations ne serait pas de changer les opinions mais de semer le doute et la confusion et, parfois, d'encourager le passage à l'acte, c'est-à-dire de transformer une conviction passive en une conviction active, et donc un agissement – de manière similaire au processus de radicalisation. L'acte en question peut être un vote.

D'autre part, un effet indirect qui est de générer chez les gouvernants une tentation liberticide. Cela pourrait être le véritable effet final recherché par les puissances étrangères à l'origine des manipulations de l'information : non pas tant de convaincre la population de tel ou tel récit que d'inciter les gouvernements à prendre des mesures contraires à leurs valeurs démocratiques et libérales, ce qui suscitera des réactions (d'une autre partie de la classe politique et de la société civile) et *in fine* contribuera à approfondir les divisions de la société. D'où l'importance pour l'État de bien doser ses efforts de contre-désinformation, dans le respect des libertés publiques.

Il apparaît donc essentiel de se doter des moyens d'une recherche indépendante, en sciences de l'information et de la communication, pour évaluer la réception de ces campagnes, mais les effets bien réels de ces phénomènes nous interdisent d'attendre les résultats de cette recherche pour agir.

Première partie

POURQUOI ?

Lutter efficacement contre les manipulations de l'information implique d'abord d'identifier les racines du problème. Elles sont multiples et c'est précisément l'une des difficultés : il y a des causes individuelles, liées à la nature humaine, relevant donc de la psychologie et de l'épistémologie, des failles cognitives et une crise de la connaissance qui nous rendent particulièrement vulnérables aux manipulations de l'information. Il y a aussi des causes collectives, liées à la vie en société, une crise de confiance dans les institutions, une crise de la presse et une désillusion à l'égard du numérique : internet devait nous libérer, et il nous enferme. Après avoir analysé chacune de ces causes, nous verrons qui en profite, c'est-à-dire qui sont les acteurs des manipulations de l'information, en nous focalisant sur les États.

Les manipulations de l'information prolifèrent d'autant plus en temps de guerre – donc bénéficient d'autant plus de la « déspécification » de la guerre, de l'ambiguïté croissante entre temps de guerre et temps de paix – que, comme l'avait bien relevé Marc Bloch en 1921 dans un article analysant la prolifération des fausses nouvelles durant la Première Guerre mondiale, « l'émotion et la fatigue détruisent le sens critique[1] ». La censure joue également un rôle, puisqu'elle est plus forte dans ces moments de crise et qu'elle suscite toutes sortes de fantasmes.

1. Marc Bloch, « Réflexions d'un historien sur les fausses nouvelles de la guerre », *Revue de synthèse historique*, n° 33, 1921, p. 32.

Marc Bloch sur les causes des fausses nouvelles (1921)

« De faux récits ont soulevé les foules. Les fausses nouvelles, dans toute la multiplicité de leurs formes, – simples racontars, impostures, légendes, – ont rempli la vie de l'humanité. Comment naissent-elles ? De quels éléments tirent-elles leur substance ? Comment se propagent-elles, gagnant en ampleur à mesure qu'elles passent de bouche en bouche ou d'écrit en écrit ? […] L'historien qui cherche à comprendre la genèse et le développement des fausses nouvelles, déçu par la lecture des documents, songera naturellement à se tourner vers les laboratoires des psychologues. […]
L'erreur ne se propage, ne s'amplifie, ne vit enfin qu'à une condition : trouver dans la société où elle se répand un bouillon de culture favorable. En elle, inconsciemment, les hommes expriment leurs préjugés, leurs haines, leurs craintes, toutes leurs émotions fortes. Seuls – j'aurai l'occasion d'y revenir plus loin – de grands états d'âme collectifs ont le pouvoir de transformer une mauvaise perception en une légende.
[…] parmi toutes les questions de psychologie sociale que les événements de ces derniers temps peuvent aider à élucider, celles qui se rattachent à la fausse nouvelle sont au premier plan. Les fausses nouvelles ! Pendant quatre ans et plus, partout, dans tous les pays, au front comme à l'arrière, on les vit naître et pulluler ; elles troublaient les esprits, tantôt surexcitant et tantôt abattant les courages : leur variété, leur bizarrerie, leur force étonnent encore quiconque sait se souvenir et se souvient d'avoir cru.
[…] le plus souvent la fausse nouvelle de presse est simplement un objet fabriqué ; elle est forgée de main d'ouvrier dans un dessein déterminé, – pour agir sur l'opinion, – pour obéir à un mot d'ordre, – ou simplement pour orner la narration, conformément à ces curieux préceptes littéraires qui s'imposent si fortement aux plus modestes publicistes et où traînent tant de souvenirs des vieilles rhétoriques ; Cicéron et Quintilien ont dans les bureaux de rédaction plus de disciples qu'on ne le croit communément. […]
Une fausse nouvelle naît toujours de représentations collectives qui préexistent à sa naissance ; elle n'est fortuite qu'en apparence, ou, plus précisément, tout ce qu'il y a de fortuit en elle c'est l'incident initial, absolument quelconque, qui déclenche le travail des imaginations ; mais cette mise en branle n'a lieu que parce que les imaginations sont déjà préparées et fermentent sourdement. Un événement, une mauvaise perception par exemple qui n'irait pas dans le sens où penchent déjà les esprits de tous, pourrait tout au plus former l'origine d'une erreur individuelle, mais non pas d'une fausse nouvelle populaire et largement répandue. Si j'ose me servir d'un terme auquel les sociologues ont donné souvent une valeur à mon gré trop métaphysique, mais qui est commode et après tout riche de sens, la fausse nouvelle est le miroir où la « conscience collective » contemple ses propres traits.

(Marc Bloch, « Réflexions d'un historien sur les fausses nouvelles de la guerre », *Revue de synthèse historique*, n° 33, 1921, p. 13-35.)

Bloch cite un humoriste de l'époque, qui écrivait que « l'opinion prévalait aux tranchées que tout pouvait être vrai à l'exception de ce qu'on laissait imprimer[2] ». C'est aujourd'hui la conviction d'un certain nombre de conspirationnistes. Le texte de Bloch vaut d'être relu car il montre combien les fondamentaux du débat sur les « fausses nouvelles » n'ont pas changé.

I. Des causes individuelles

S'adressant en même temps à l'individu et la masse, « la propagande moderne repose sur les analyses scientifiques de la psychologie et de la sociologie. C'est à partir de la connaissance de l'être humain, de ses tendances, de ses désirs, de ses besoins, de ses mécanismes psychiques, de ses automatismes, et aussi bien de la psychologie sociale que de la psychologie des profondeurs, que la propagande organise peu à peu ses techniques[3] ».

A. Les failles cognitives

La désinformation exploite une paresse intellectuelle naturelle, qui consiste à ne pas exercer son esprit critique de manière systématique, et à relayer des propos naïvement sans chercher à les étayer par des preuves. Les conspirationnistes demandent qu'on leur fournisse la preuve que leurs théories sont inexactes et farfelues, à rebours du travail journalistique. Comme le rappelle Emmanuel Macron, « la charge de la preuve est inversée : là où les journalistes doivent prouver sans cesse ce qu'ils disent – ce qui est l'éthique même de leur métier, ils doivent montrer qu'ils disent ou écrivent le vrai –, les propagateurs de fausses nouvelles crient à la face du monde : "À vous de prouver que nous avons tort !"[4] ».

Nous avons tous tendance à privilégier les informations qui confirment nos hypothèses, nous confortent dans nos positions, et ne heurtent pas nos sensibilités : ce phénomène psychologique est communément appelé « biais de confirmation ». En publicité, cette faille est bien connue et exploitée : le succès d'une campagne publicitaire peut reposer sur l'engagement et la consistance d'un individu, c'est-à-dire sa tendance à rester fidèle à une opinion déjà formée[5].

2. *Ibid.*
3. Jacques Ellul, *Propagandes*, *op. cit.*, p. 15.
4. Emmanuel Macron, discours à l'occasion des vœux à la presse, 4 janvier 2018.
5. Joel J. Davis, *Advertising Research: Theory and Practice*, 2e ed., Pearson, 2011.

Ensuite, les humains ont tendance à croire avec certitude, c'est-à-dire en surestimant « leurs capacités de mémoire et de raisonnement, bref à se croire plus rationnels et plus intelligents qu'ils ne le sont en fait[6] ». Dans ce contexte, « l'idée répandue selon laquelle le raisonnement vise à atteindre la vérité, de bonnes décisions, et doit être impartial et objectif » est fausse[7]. Comme le rappelle Pascal Engel, « le raisonnement n'a pas évolué en vue d'établir la vérité, mais uniquement en vue de l'emporter sur nos adversaires : nous ne raisonnons que pour argumenter dans le cadre d'un jeu social où nous favorisons systématiquement notre propre point de vue et nos intérêts[8] ». Les manipulations de l'information sont aussi naturelles que nos vulnérabilités à leur égard.

Une étude récente montre également que les fausses nouvelles se propagent plus vite que les vraies, pour des raisons psychologiques[9] : d'une part, les vraies nouvelles sont souvent moins nouvelles, elles ne font que confirmer ce que l'on savait déjà, ou que l'on suspectait, elles contribuent à l'accumulation du savoir, elles sédimentent. Tandis que les fausses nouvelles surprennent, elles sont rédigées pour être surprenantes, aller à l'encontre de la *doxa*. La nouveauté de la fausse nouvelle non seulement suscite un plus grand intérêt du plus grand nombre, mais aussi explique leur plus grande diffusion de la part de personnes voulant apprendre quelque chose aux autres (dimension réputationnelle, statut social, etc.). D'autre part, elles sont taillées pour la viralité, elles sont rédigées dans un style spectaculaire, émotionnel, souvent alarmiste, elles jouent sur la peur, les angoisses, alors que ce n'est généralement pas la priorité des vraies nouvelles. Ce sont donc nos biais cognitifs qui contribuent en grande partie à la diffusion des fausses nouvelles.

La recherche en publicité identifie d'ailleurs plusieurs failles cognitives que le bon publicitaire peut exploiter : non seulement la consistance de l'individu (biais de confirmation) mais aussi la preuve sociale (l'individu va faire ce qu'il pense que les autres font), l'autorité (il tend à obéir à des figures d'autorité, même quand elles demandent l'accomplissement d'actes condamnables), l'illusion de corrélation (il établit une relation entre deux

6. Pascal Engel, « Vous pensez être capable de détecter des "fake news"… N'en soyez pas si sûrs » (interview), *Atlantico*, 7 janvier 2017.

7. Hugo Mercier et Dan Sperber, *The Enigma of Reason*, Harvard University Press, 2017, p. 129.

8. Pascal Engel, « Si on ne peut pas prouver que le monstre du Loch Ness n'existe pas, c'est qu'il existe… », *Libération*, 19 février 2018.

9. Soroush Vosoughi, Deb Roy et Sinan Arai, « The spread of true and false news online », *Science*, 359:6380, 9 mars 2018, p. 1146-1151.

événements temporellement proches) ou encore les préférences (il est plus aisément convaincu par les personnes qu'il apprécie).

B. Une crise épistémologique

Les manipulations informationnelles ne sont que l'une des manifestations d'un phénomène plus large qui intègre également les pseudo-sciences – notamment dans les domaines de la médecine et de la biologie –, le révisionnisme historique et les théories conspirationnistes. Dans les milieux universitaires, on assiste également à une recrudescence de contrefaçons : il existe des milliers[10] de fausses revues scientifiques et de fausses maisons d'édition qui publient des articles et des livres à la chaîne sans les évaluer mais en faisant payer les auteurs – les chercheurs reçoivent de plus en plus de spams de ces « éditeurs prédateurs ». Certains pays sont particulièrement touchés, dont le Kazakhstan et l'Indonésie. Le phénomène a été étudié par une coalition de médias internationaux baptisée « Fake Science »[11].

En 2008, l'écrivain et journaliste britannique Damian Thompson alertait déjà sur « une pandémie de crédulité » et le repli des valeurs des Lumières face à la « contre-connaissance[12] ». Le fait est qu'« une grande proportion de la population vit dans un espace épistémique ayant abandonné les critères conventionnels de la preuve, de la cohérence et de la recherche des faits. Il s'ensuit que l'état actuel du débat public ne peut plus être évalué à la lumière d'une désinformation qu'il suffirait de corriger, mais doit l'être à celle d'une réalité alternative partagée par des millions d'entre nous[13] ».

En 2013, le sociologue Gérald Bronner consacrait lui aussi un ouvrage à la crédulité grandissante dans nos démocraties, ce « ventre mou de notre rationalisme contemporain dans lequel l'irrationalisme se taille allègrement un espace très conséquent et paradoxal[14] ». Il l'explique par la combinaison de deux phénomènes principaux : d'une part, la libéralisation du marché

10. Le documentaliste américain Jeffrey Beall en a recensé 11 000 (beallslist.weebly.com).

11. Stéphane Foucart et David Larousserie, « Alerte mondiale à la fausse science », *Le Monde*, 19 juillet 2018.

12. Damian Thompson, *Counter-Knowledge: How we surrendered to conspiracy theories, quack medicine, bogus science and fake history*, Atlantic, 2008.

13. Stephan Lewandowsky, Ullrich Ecker et John Cook, « Beyond Misinformation: Understanding and Coping with the 'Post-Truth' Era », *Journal of Applied Research in Memory and Cognition*, 6:4, 2017, p. 360, traduit et cité par Sebastian Dieguez, *Total Bullshit ! Au cœur de la post-vérité*, PUF, 2018, p. 316.

14. Gérald Bronner, *La Démocratie des crédules*, PUF, 2013, p. 86.

de l'information dans lequel les sources rationnelles doivent affronter la concurrence des sources irrationnelles, et le fait que cette compétition favorise les « croyants » qui sont « généralement plus motivés que les non-croyants pour défendre leur point de vue et y consacrer du temps[15] » ; et, d'autre part, la paresse intellectuelle des usagers des médias, qui tombent facilement dans divers biais cognitifs, dont le biais de confirmation.

Olivier Schmitt explique quant à lui que la crise épistémologique « prend la forme de l'entrelacement dans l'espace public des versions abâtardies de trois approches épistémologiques[16] » : le doute cartésien détourné en doute systématique sur lequel peut proliférer le complotisme ; les relations entre savoir et pouvoir, en caricaturant Foucault pour affirmer que « tout savoir produit est forcément au profit des plus puissants » ; et le déconstructionnisme, qui chez Derrida cherche à révéler les non-dits d'un texte, et qui dans sa version abâtardie vise la déconstruction systématique d'un « discours dominant ». En somme, la crise épistémologique contemporaine repose sur la mauvaise interprétation, le détournement, la simplification d'approches respectables par ailleurs.

Un phénomène de droite ou de gauche ?

Si la plupart des études, aux États-Unis en tout cas, montrent que la droite est plus souvent – mais bien entendu pas exclusivement – à l'origine des nouvelles fausses et biaisées, c'est parce que les citoyens progressistes consomment généralement une plus grande variété de sources d'informations et font davantage confiance au journalisme professionnel, tandis que les conservateurs ont tendance à davantage fréquenter des sources et des réseaux conformes à leurs opinions politiques, et à avoir un biais anti-médias et anti-intellectuels – que l'on observe aussi dans le populisme de droite européen. En raison de ces vulnérabilités, si la droite semble plus susceptible d'être victime d'informations fabriquées, c'est « parce qu'elle semble être plus systématiquement la cible de ceux qui cherchent à les exploiter de façon stratégique[17] ».

15. *Ibid.*, p. 76. Voir aussi Dominique Cardon, *La Démocratie Internet. Promesses et limites*, Éd. du Seuil, 2010.

16. Olivier Schmitt, « "Je ne fais que poser des questions". La Crise épistémologique, le doute systématique et leurs conséquences politiques », *Temps présents,* 15 juin 2018.

17. Jayson Harsin, « Un guide critique des *Fake News* : de la comédie à la tragédie », *op. cit.*, p. 116.

Le complotisme avait été bien décrit par le philosophe Karl Popper au début des années 1960 : « Il existe une thèse, que j'appellerai la thèse du complot, selon laquelle il suffirait, pour expliquer un phénomène social, de découvrir ceux qui ont intérêt à ce qu'il se produise. Elle part de l'idée erronée que tout ce qui se passe dans une société, guerre, chômage, pénurie, pauvreté, etc., résulte directement des desseins d'individus ou de groupes puissants[18]. »

Le complotisme (ou conspirationnisme) est l'exagération d'une tendance naturelle à croire que tout effet est causé par une action intentionnelle, en particulier ceux qui bénéficient à certaines personnes. Les théories conspirationnistes sont alors inévitables, et se nourrissent notamment des crises et des événements violents. Heureusement, toutes ne sont pas dangereuses. Certaines sont inoffensives. Mais d'autres peuvent avoir des effets déstabilisateurs, même si elles ne sont partagées que par une ultra-minorité de la population : il suffit que cette minorité soit prête à passer à l'action violente. La radicalité s'accompagne souvent d'une vision conspirationniste de la réalité.

La plupart des conspirationnistes ne sont ni fous ni irrationnels mais souffrent simplement d'un manque de bonnes sources : les théories qu'ils défendent sont injustifiées au regard de l'ensemble des informations disponibles mais pas au regard des sources qui sont les leurs et au regard desquelles ces théories peuvent sembler cohérentes. La cause du problème est donc la pauvreté épistémique de leur environnement. C'est aussi vrai, dans une certaine mesure, de l'extrémisme en général, dont certains auteurs ont dit qu'il souffrait d'une « épistémologie handicapée[19] ». L'une des solutions est alors « l'infiltration cognitive des groupes extrémistes » en trouvant des moyens physiques ou virtuels de semer le doute dans leur esprit, en introduisant de la diversité explicative[20].

Les conspirationnistes posent une difficulté spécifique car ils sont particulièrement résistants aux tentatives de démythification (*debunking*), surtout si elles viennent de l'État : le conspirationnisme consistant à attribuer à certaines personnes le pouvoir démesuré de dissimuler leurs actions, ces tentatives sont d'emblée absorbées comme faisant partie du complot.

18. Karl Popper, *La Société ouverte et ses ennemis*, t. 2 : *Hegel et Marx*, Éd. du Seuil, 1979 [1962-1966], p. 67.

19. Russell Hardin, « The Crippled Epistemology of Extremism » in Albert Breton *et al.* (eds.), *Political Extremism and Rationality*, Cambridge University Press, 2002, p. 3-22.

20. Cass R. Sunstein et Adrian Vermeule, « Conspiracy Theories: Causes and Cures », *The Journal of Political Philosophy*, 17:2, 2009, p. 219.

Nous vivons donc une crise de la connaissance, une crise épistémologique – qui n'est pas nouvelle puisque c'était déjà le combat de Platon contre les sophistes, leur reprochant de ne pas s'intéresser à la vérité, seulement à la conviction, de ne pas viser la connaissance (*episteme*), seulement l'opinion (*doxa*). Jamais davantage qu'aujourd'hui la distinction entre *episteme* et *doxa*, et à travers elle la possibilité même de la connaissance, n'aura été autant menacée. Avec une différence majeure par rapport aux époques précédentes : nous ne sommes pas dans une ère idéologique du remplacement d'une vérité par une autre, mais dans une ère sceptique ou relativiste de remise en cause de la possibilité même de la vérité.

Le 16 novembre 2016, les dictionnaires Oxford ont décerné au terme de *post-truth* le titre de mot de l'année. Entre 2015 et 2016, son usage aurait augmenté de 2 000 %[21]. « Au lieu de saper la vérité par la base, en tentant laborieusement d'en imposer une autre par un travail monumental de manipulation et de surveillance, [la post-vérité] la disqualifie d'emblée et en amont. La post-vérité n'impose aucune vérité particulière, et c'est précisément ainsi qu'elle sème la confusion et le doute, s'accommodant parfaitement des dissensions et critiques, laissant les "faits alternatifs" se multiplier à l'infini, aussi contradictoires soient-ils[22]. »

II. Des causes collectives

A. La crise de confiance dans les institutions

Une enquête menée auprès de plus de 33 000 personnes dans 28 pays en novembre 2017 a montré que la méfiance à l'égard des institutions s'accroît, que les médias sont désormais l'institution en laquelle la confiance est la moindre, que la confiance dans les plateformes (médias sociaux) décroît mais que celle dans le journalisme s'accroît, et que quasiment 70 % de la population s'inquiète de l'usage de fausses nouvelles comme arme, ce pourcentage étant le plus élevé au Mexique, en Argentine, Espagne et Indonésie (76-80 %) et le moins élevé – quoique toujours majoritaire – en France, Suède et Pays-Bas (55-60 %)[23]. Or, « de quoi les fausses nouvelles

21. Sabrina Tanquerel, « Quand l'exigence de vérité devient secondaire », *The Conversation*, 12 février 2017.

22. Sebastian Dieguez, *Total Bullshit ! Au cœur de la post-vérité*, *op. cit.*, p. 307. Voir aussi Julien Nocetti, « La guerre de l'information. Comment l'information recompose les relations internationales. La faute à Internet ? » *in* IFRI (dir.), *RAMSES 2018. La guerre de l'information aura-t-elle lieu ?,* Dunod, 2018.

23. 2018 Edelman Trust Barometer, Global Report.

en circulation nous parlent-elles ? Elles traitent de la trahison des élus, de la confiscation de la parole par les médias, d'un certain nombre d'angoisses liées à la mondialisation. En ce sens, les *fake news* sont également l'expression d'une défiance virulente à l'égard des élites politiques et intellectuelles[24] ».

Les manipulations de l'information sont à la fois une cause et un symptôme de la crise de la démocratie, incarnée par une abstention croissante aux élections et une défiance de l'opinion à l'égard des élus, voire une remise en cause des valeurs démocratiques et libérales. La dépréciation de la vérité est l'une des manifestations de cette crise de confiance, en même temps qu'elle l'entretient. Cette crise est due à des facteurs circonstanciels, dont la crise financière de 2008-2009, mais aussi à des causes profondes :

1. Le rejet des élites. Des États-Unis aux Philippines en passant par la Hongrie, la haine de l'*establishment* semble être une passion partagée des opinions dont s'emparent efficacement tous les *outsiders* populistes, vrais ou prétendus.

2. La polarisation identitaire. En réaction à la porosité des frontières et aux formes hybrides de métissage culturel qu'engendre la globalisation, les opinions sont en demande d'une réaffirmation claire de la clôture du « nous » contre « eux ». Y participent des phénomènes tels que l'érection de murs (Israël, États-Unis, Hongrie), l'expansion de *gated communities* urbaines, l'imposition de quotas de réfugiés, etc.

3. La subversion et le détournement des institutions démocratiques. Les pouvoirs en place tendent à transformer de l'intérieur la nature de l'État de droit dont ils héritent (asservissement du judiciaire en Pologne, renforcement des pouvoirs de police grâce aux lois d'exception en Turquie, criminalisation des oppositions et des ONG en Russie et en Israël). Le recours aux plébiscites permet de légitimer la perpétuation de l'exécutif au-delà des délais prévus par les constitutions (3e mandats au Venezuela, au Burundi et au Congo).

4. La « barbarisation des bourgeois » en temps de crise[25]. Les leaders populistes ou « nouveaux démagogues » se posent le plus souvent en champions d'une classe moyenne dopée à la croissance (pays émergents) ou terrorisée à l'idée d'un déclassement (zone OCDE).

5. Une crise globale de la communication politique. Cette crise du *logos* profondément destructrice pour l'espace public trouve sa source dans un

24. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, FYP éditions, 2017, p. 44.

25. Pierre Hassner, « Le Barbare et le Bourgeois », *Politique internationale*, n° 84, été 1999, p. 90-91.

double phénomène : le développement, d'une part, d'une blogosphère conspirationniste et transnationale qui fait le jeu de la propagande et celui, d'autre part, de la désinformation de certains régimes et mouvements anti-libéraux.

B. La crise de la presse

Ce qu'il est convenu d'appeler la crise de la presse s'exprime généralement d'au moins deux manières : une crise du modèle économique et une crise des normes[26]. La crise du modèle économique est ancienne et principalement due à la baisse des revenus publicitaires de la presse concurrencée d'abord par la télévision, puis par internet. Le passage au numérique ne compense pas automatiquement dans la mesure où la publicité numérique est moins rémunératrice que l'imprimée et la télévisuelle. Beaucoup d'agences et d'organes de presse ont donc dû licencier un certain nombre de journalistes, les plans sociaux s'enchaînent et certains titres ferment. Cette précarité les rend plus vulnérables aux manipulations de l'information, puisqu'il y a moins de personnes et de temps pour les détecter, et un primat de la quantité sur la qualité.

De nouveaux modèles économiques s'inventent toutefois, dont le payant, sur abonnement, et la diversification des sources de revenus (en investissant aussi l'événementiel, par exemple) – avec parfois des succès qui convainquent que la presse est peut-être davantage « dans une situation de réinvention qu'en crise[27] ». Le cas du *New York Times* est exemplaire, avec plus d'un milliard de dollars de recettes en 2017 grâce à ses abonnements[28].

Quant à la crise des normes, elle est principalement due à l'essor des médias sociaux (voir *infra*), dont le pouvoir égalisateur permet à n'importe qui de diffuser des informations qui ne respectent pas les standards journalistiques, et de propager des discours parfois extrêmes et haineux, comme le font les trolls (voir *infra*). Là aussi, toutefois, il y a des raisons d'espérer, car ces excès créent une fatigue de la population et poussent les médias sérieux désireux de montrer leur valeur ajoutée à développer davantage de normes (voir *infra*) et à valoriser l'investigation, des enquêtes longues, poussées, parfois collaboratives.

---

26. Heidi Tworek, « Responsible Reporting in an Age of Irresponsible Information », Alliance for Securing Democracy (GMF) Brief 2018, n° 009, mars 2018, p. 2.

27. Entretien avec Jean-Marie Charon, *Télérama*, 18 mars 2017.

28. Sydney Ember, « New York Times Co. Subscription Revenue Surpassed $1 Billion in 2017 », *The New York Times*, 8 février 2018.

C. La désillusion numérique

Les manipulations de l'information ont toujours existé mais ont connu trois accélérations dues à des innovations techniques : l'imprimerie, les médias de masse et internet. Cette dernière phase a elle-même connu une accélération encore plus spectaculaire depuis un peu plus d'une décennie, avec les médias sociaux.

La révolution numérique – surtout depuis la généralisation du haut débit, c'est-à-dire une quinzaine d'années – et le développement conséquent des réseaux sociaux numériques (MySpace 2003, Facebook 2004, Twitter 2006) ont changé la donne. Omniprésents dans la vie de milliards d'individus (Facebook a plus de 2 milliards d'utilisateurs actifs depuis juin 2017, YouTube 1,5 milliard, Instagram 700 millions et Twitter 328 millions), les réseaux sociaux sont utilisés comme source d'information pour 62 % des adultes américains et 48 % des Européens[29]. Google et Facebook concentrent désormais plus de 70 % du trafic web, ce qui signifie que les autres sites, dont des entreprises de presse, tirent l'essentiel de leur audience de ces plateformes, devenues des portiers du web. Elles génèrent du même coup des revenus publicitaires colossaux.

Dans un premier temps, cette croissance des réseaux sociaux et plus généralement du web 2.0, des blogs, du journalisme citoyen, a pu faire croire à un moment d'émancipation du peuple face aux États[30] – comme l'ont incarné les « printemps arabes », au risque de certaines caricatures (on parlait alors de « révolution Facebook » ou « révolution Twitter »). La désillusion est venue quelques années plus tard, d'abord avec l'affaire Snowden (2013) qui a révélé (ou confirmé) que les États n'avaient pas perdu la main, puis avec une série d'interférences dans des processus démocratiques à partir de 2016 (référendum néerlandais sur l'accord d'association entre l'Ukraine et l'UE, Brexit, élection présidentielle américaine, élection présidentielle française).

Le développement exponentiel des plateformes numériques a considérablement accru le risque de manipulations de l'information de plusieurs manières :

• par la surabondance d'informations, « infosaturation » ou « infobésité ». « L'Américain moyen est désormais exposé à cinq fois plus

29. *Reuters Insititute Digital News Report 2016*.

30. François-Bernard Huyghe, « Que changent les *fake news* ? », *La Revue internationale et stratégique*, n° 110, février 2018, p. 79.

d'informations qu'en 1986[31]. » Or, la surcharge d'information contribue à la désinformation via la déconcentration, qui affaiblit notre vigilance et notre capacité d'envisager des réfutations[32]. Ce n'est au fond que l'application aux réseaux sociaux d'une thèse bien connue des psychologues dans le monde physique : trop d'informations nuit à la prise de décision ;

• par le nombre de vecteurs disponibles pour diffuser la fausseté (potentiellement autant qu'il y a d'utilisateurs de ces réseaux, c'est-à-dire plusieurs milliards) ;

• la plus grande précision de la segmentation et du ciblage de la population (*micro-targeting*) – les cibles les plus vulnérables étant les jeunes (17-25 ans) – ;

• le faible coût de cette diffusion (quelques clics, quelques minutes) et la démocratisation de l'apparence journalistique (facile de faire un blog, une page, un site, d'allure professionnelle) ;

• l'horizontalité des médias sociaux permettant à chacun de diffuser des contenus à tout le monde sans passer par des instances de contrôle éditorial ;

• le fait qu'internet n'ait pas de frontière, et donc que des puissances étrangères puissent facilement y infiltrer des communautés et y répandre de fausses nouvelles ;

• le progrès technique dans l'édition de contenus photo, vidéo, audio qui sont de plus en plus proches de la réalité, donc moins détectables.

Comme le résume Ben Nimmo, « la diffusion des technologies de publication numérique a rendu plus facile de créer de fausses histoires ; internet a rendu plus facile de les publier ; et les réseaux sociaux de les diffuser[33] ». Déjà en 2005, avant l'essor des principaux réseaux sociaux numériques, on pouvait écrire que « chacun est un reporter[34] ». Cette tendance n'a fait que s'accentuer.

---

31. Daniel Levitin, auteur de *Weaponized Lies: How to Think Critically in the Post-Truth Era*, cité dans Eoin O'Carroll, « How information overload helps spread fake news », *The Christian Science Monitor*, 27 juin 2017.

32. Xiaoyan Qiu *et al.*, « Limited individual attention and online virality of low-quality information », *Nature Human Behaviour*, 1, article number 0132, 2017.

33. Ben Nimmo, pour son audition devant le parlement singapourien (Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures, written representation 36, 22 février 2018).

34. Lucas Grave, « Everyone's a reporter », *Wired Magazine*, 9 janvier 2005.

La vitesse de propagation s'est ainsi considérablement accrue. Il a fallu quasiment quatre ans au KGB pour diffuser globalement la rumeur selon laquelle le virus du sida était une création du Pentagone (la fausse nouvelle est plantée dans un journal indien en 1983 mais n'atteint la presse soviétique qu'en 1985 puis les médias occidentaux en 1987). Aujourd'hui, les réseaux sociaux réduisent ce temps à quelques minutes ou quelques heures, comme le montre l'exemple des « Macron Leaks » (voir *infra*). On pourrait croire qu'il ne s'agit que d'un changement d'échelle. Mais, comme l'a déclaré le ministre de l'Europe et des Affaires étrangères Jean-Yves Le Drian, « il est des domaines, comme celui de l'information, où le changement d'échelle constitue en réalité un changement de nature[35] ».

Pour augmenter le temps de présence en ligne des internautes, ces plateformes développent des dispositifs techniques comme le *matching* avec des contenus sponsorisés, notamment ceux qui sont les plus susceptibles de nous faire réagir, donc de cliquer et de poursuivre la navigation. Cela pose plusieurs problèmes[36] :

1. Cela enferme les internautes dans des « bulles filtrantes ». Les moteurs de recherche et les réseaux sociaux ont des algorithmes de personnalisation : depuis 2010, les résultats de recherche dans Google ne sont pas les mêmes pour tout le monde, ils dépendent des préférences de l'internaute, d'après l'historique de ses recherches et de sa géolocalisation. Partant d'une logique commerciale – proposer à l'utilisateur les résultats les plus proches (dans tous les sens du terme) de ses attentes – cette pratique a l'effet pervers d'enfermer les internautes « dans des espaces cognitifs clos où ne seraient portés à leur connaissance que des contenus qui les conforteraient dans leurs positions. Le moteur deviendrait ainsi un outil de confirmation plutôt que d'information[37] ». C'est pour dénoncer cet enfermement qu'Eli Pariser a, en 2011, introduit l'expression de « bulle de filtrage[38] ». Facebook et d'autres réseaux sociaux font de même. Or, ces plateformes étant pour la plupart des utilisateurs les « portiers » du web, des voies d'accès au reste, leurs algorithmes de personnalisation enferment les individus dans des cocons, des espaces cognitifs confortables mais qui ne font

35. Jean-Yves Le Drian, *Discours de clôture* du 4 avril 2018, *op. cit.*

36. Nous remercions le secrétariat général du Conseil national du numérique pour sa contribution à l'analyse suivante.

37. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 33.

38. Eli Pariser, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, 2011.

que confirmer leurs préjugés plutôt que les confronter à ceux d'autrui. Ce problème de « bulles filtrantes » amplifie nos biais sociologiques et cognitifs, en particulier notre « biais de confirmation » : nous n'aimons pas être contredits, et les algorithmes de création de contenus des plateformes s'assurent que nous ne le soyons pas, en nous fournissant des informations qui nous confortent dans nos opinions. La révolution numérique contribuerait ainsi, paradoxalement, à nous refermer sur nous-mêmes.

Ce phénomène a contribué aux « surprises » politiques de l'année 2016, le fait que personne ou presque ne semble avoir anticipé le Brexit ni l'élection de Trump. Dans un article célèbre intitulé « How technology disrupted the truth », Katharine Viner, la rédactrice en chef du *Guardian*, en fait la démonstration dans le cas du Brexit[39]. Quelques mois plus tard, dans un article au titre évocateur – « Il y a 58 millions d'électeurs pro-Trump et je n'en ai vu aucun » – Julien Cadot fait de même pour l'élection de Trump[40].

2. Cela crée aussi un phénomène d'« information en cascade » : les utilisateurs relaient les informations postées par leurs proches sans nécessairement les vérifier ou même questionner leur validité. Plus l'information sera partagée, plus on tendra à lui faire confiance et moins on exercera son esprit critique.

3. Cela favorise les contenus les plus divertissants ou scandaleux car ils sont les plus susceptibles de nous faire réagir, indépendamment de leur véracité. Ce modèle participe ainsi à la polarisation de l'opinion en réduisant la visibilité des contenus nuancés car jugés moins engageants. Ce modèle d'affaire est optimisé pour le profit plus que la vérité : il valorise les fausses nouvelles.

4. Cela déclenche une course à la capture de l'attention. Les plateformes investissent des sommes colossales pour étudier nos mécanismes attentionnels et les failles de notre volonté.

Pour l'ensemble de ces raisons, l'éthique journalistique, la traçabilité des sources, la vérification des faits sont sacrifiées sur l'autel de la viralité. Cette course au nombre de pages vues, pour augmenter à la fois les revenus publicitaires et l'attractivité du point de vue des investisseurs, gangrène les entreprises de presse, aux dépens du journalisme sérieux. Elle favorise

39. Katharine Viner, « How technology disrupted the truth », *The Guardian*, 12 juillet 2016.

40. Julien Cadot, « Bulles de filtrage : il y a 58 millions d'électeurs pro-Trump et je n'en ai vu aucun », numerama.com, 9 novembre 2016. Voir aussi Matthew Hughes, « How the Internet tricked you into thinking Trump wouldn't win », *The Next Web*, 9 novembre 2016.

les titres racoleurs, le sensationnalisme, même des pièges à clics (*clickbait*), au détriment de la vérité.

III. Qui manipule l'information et pourquoi ?

Les vulnérabilités identifiées dans les pages précédentes constituent un terreau favorable aux manipulations de l'information. À elles seules, cependant, elles n'expliquent pas la situation actuelle : ce terreau est utilisé par des acteurs qui perçoivent ces vulnérabilités comme des opportunités pour défendre leurs intérêts stratégiques. Qui sont-ils ? Ils sont extrêmement divers, de l'individu plus ou moins isolé à l'État en passant par des groupes non étatiques et des entreprises. Tous les types d'acteurs manipulent l'information. Le présent rapport se concentre sur un certain type de manipulation par un certain type d'acteur : les manipulations de l'information d'origine étatique et ciblant la population d'un autre État, c'est-à-dire les ingérences. Nous commencerons toutefois par évoquer les autres situations.

A. Des acteurs non étatiques

Ce rapport s'intéresse aux acteurs non étatiques avant tout en tant qu'ils servent de relais, ou parfois d'aiguillon, aux manipulations de l'information d'origine étatique. Pour autant, les techniques de manipulations de l'information sont aussi utilisées par des acteurs non étatiques agissant pour leur propre compte et pour promouvoir leur propre agenda. Parmi ceux-ci, deux cas d'étude peuvent apporter des indications intéressantes : les groupes djihadistes, qui témoignent du rôle des manipulations de l'information dans les entreprises terroristes ; les communautés ethniques et/ou religieuses qui, lorsqu'elles manipulent et/ou sont manipulées, fragilisent certains États, surtout en Asie et en Afrique. Le cas des mouvements nationalistes et/ou populistes au sein même de nos démocraties occidentales, qui ont joué un rôle dans le Brexit et l'élection de Donald Trump, et ont tenté d'influer sur la dernière élection présidentielle française, relève d'une logique un peu différente, dans la mesure où l'on observe une confluence de leur agenda avec celui d'acteurs étatiques. L'affaire dite des « Macron Leaks » faisant l'objet d'un chapitre distinct (voir *infra*), nous ne donnerons ici que des exemples des deux premières catégories.

1. Des groupes djihadistes : le cas de Daech

Les opportunités offertes par la sphère virtuelle pour mener des opérations terroristes avaient déjà été reconnues par Al-Qaïda. En 2005, Ayman al-Zawahiri déclarait : « Nous sommes dans une bataille, et plus de la moitié de cette bataille s'effectue dans les médias. Dans la bataille médiatique, nous luttons pour conquérir les cœurs et les esprits de notre Oumma [la communauté musulmane][41]. » Dix ans plus tard, le Geneva Centre for Security Policy estimait que la campagne de Daech sur les médias sociaux lui avait permis d'attirer plus de 18 000 soldats étrangers, venant de plus de 90 pays[42]. L'appareil propagandiste djihadiste constitue l'une des forces majeures du groupe à l'heure où ses forces armées sont battues en Syrie et en Irak.

La propagande mise en place par Daech est multidimensionnelle, multivectorielle et ciblée. Elle est multidimensionnelle tout d'abord car elle s'appuie sur une vision du monde manichéenne, simple et complotiste, visant à expliquer l'ensemble de la vie sociale. Les contenus médiatiques comprennent ainsi des cours d'histoire (réécrivant les accords Sykes-Picot[43], la colonisation, l'intervention en Irak de 2003), des articles d'actualité (sur les actions de la coalition, l'Iran), des reportages type BBC présentés par John Cantlie, otage-reporter montrant par exemple les bonnes conditions de vie à Mossoul[44], mais aussi des cours de théologie, fondés sur une lecture extrémiste du texte religieux. Les thèses complotistes diffusées contribuent à l'établissement d'une grille de lecture séduisante pour les jeunes en crise d'identité, principales cibles du groupe[45]. Multidimensionnelle, la propagande de l'État islamique convoque à la fois des discours prétendument de vérité et des éléments émotionnels – combinaison qui permet

41. Christina Schori Liang, *Cyber Jihad: Understanding and Countering Islamic State Propaganda,* The Geneva Centre for Security Policy, Policy Paper, février 2015, p. 2.

42. *Ibid.*

43. James Renton, « Décrypter Daech : le califat et le spectre des accords Sykes-Picot », *The Conversation*, 4 mars 2016.

44. Dans une vidéo publiée par l'État islamique en janvier 2015, le reporter propose une visite touristique de la ville. La vidéo apparaît comme une réponse directe à un article de *The Guardian* racontant que les habitants de Mossoul manquent d'eau, de nourriture et d'électricité. John Cantlie présente une ville agréable en dépit des conflits, répétant à de nombreuses reprises qu'il n'y a pas de coupures électriques sur place.

45. Xavier Crettiez et Romain Sèze, *Saisir les mécanismes de la radicalisation violente : pour une analyse processuelle et biographique des engagements violents,* Rapport de recherche pour la Mission de recherche Droit et Justice, avril 2017.

l'acquisition d'une crédibilité discursive et la conquête « des cœurs et des esprits[46] ».

La propagande de Daech est aussi multivectorielle. L'agence de communication de Daech, AMAQ, est très active. Mais le groupe communique également via son centre médiatique Al-Hayat[47] et la « djihadosphère » a connu un développement notable depuis la proclamation officielle du califat en 2014. Désormais, l'État islamique possède non seulement des sites internet, forums de chat et revues en ligne, mais fait aussi une utilisation intensive des réseaux sociaux, blogs, messageries instantanées, sites de partage vidéo, Twitter, Facebook, Instagram, WhatsApp, Tumblr, etc. Il est aussi actif sur Telegram et sur des forums spécialisés (*terror forums*), ainsi que sur le web profond (Darknet) où les opérations terroristes peuvent être préparées. Cette diversité des moyens de diffusion traduit également une diversité de formats : vidéos, articles, chansons, reportages, mèmes, etc. Les attentats de novembre 2015 à Paris ont ainsi été revendiqués via un communiqué officiel écrit, qui a également été repris en chanson, pour atteindre un public plus jeune. Ce faisant, l'État islamique bâtit un appareil propagandiste capable d'attirer des publics variés.

Ces publics font l'objet d'un ciblage méticuleux qui cherche avant tout à exploiter les vulnérabilités sociales, économiques, politiques et culturelles des sociétés visées. La multiplication des mèmes et vidéos terroristes le montre, les jeunes constituent la principale cible des thèses complotistes de l'État islamique, qui leur offre des réponses à des crises d'identité vécues localement, à l'heure d'entrer dans le monde du travail ou de se bâtir une identité d'adulte[48]. Daech pratique le ciblage et l'individualisation à un niveau sans équivalent.

2. Des communautés ethniques et/ou religieuses : le cas indonésien

Le cas indonésien paraît assez représentatif de la manière dont s'opèrent les manipulations de l'information qui touchent aux communautés ethniques et/ou religieuses. En Indonésie, la désinformation porte généralement sur des sujets tels que l'augmentation du nombre de travailleurs chinois (qui a effectivement augmenté mais pas autant que ces fausses informations le prétendent) ou l'origine ethnique ou religieuse des

46. Kierat Ranautta-Sambhi, in NATO StratCom COE et The King's College London, *Fake News. A Roadmap,* janvier 2018, p. 51.

47. Christina Schori Liang, *Cyber Jihad*, *op. cit.*, p. 2.

48. Xavier Crettiez et Romain Sèze, *Saisir les mécanismes de la radicalisation violente*, *op. cit.*

leaders (durant l'élection présidentielle de 2014, Jokowi était accusé de dissimuler ses origines chinoises et d'être chrétien). Le problème est apparu lors de l'élection du gouverneur de Jakarta en 2012, et plus récemment lors de celle de 2017 qui a suscité de nombreuses campagnes de désinformation tentant de monter les musulmans contre les Indonésiens d'origine chinoise – ce qui n'est pas nouveau dans le pays. Une des cibles principales était le gouverneur d'alors, Basuki Tjahaja Purnama (premier chrétien d'origine chinoise à ce poste), accusé de blasphème. Cette campagne a eu de réelles conséquences : des centaines de milliers de musulmans sont allés manifester et Basuki Tjahaja Purnama a été condamné à deux ans de prison.

La désinformation pollue aussi la vie quotidienne, avec des effets bien réels : plusieurs temples et pagodes ont été détruits en 2016 dans le nord de Sumatra suite à la propagation d'une fausse rumeur sur les réseaux sociaux selon laquelle une femme chinoise se plaignait de l'appel à la prière du matin. L'année suivante, dans l'ouest du Kalimantan, un homme innocent a été battu à mort par une foule suite à une fausse rumeur (plus sophistiquée, avec le logo de la police) selon laquelle une opération d'enlèvement d'enfants avait lieu. Un groupe nommé Saracen (sarrasin en français) vendait ses services pour mener des campagnes en ligne contre tel ou tel groupe ethnique ou religieux. Avant d'être arrêtés en août 2017, ses membres ont notamment contribué à exacerber les sentiments anti-chinois. Le groupe contrôlait 800 000 comptes sur les réseaux sociaux.

Les raisons de la vulnérabilité indonésienne sont une population peu éduquée et très polarisée (tensions ethniques et religieuses). La désinformation indonésienne reste toutefois indigène : l'écosystème est en grande partie isolé du reste du monde par sa langue, le bahasa, et demeure donc relativement protégé de tentatives d'ingérences étrangères.

Le président a depuis déclaré la « guerre » aux *fake news* et la société civile a lancé un certain nombre d'initiatives pour les détecter, comme TurnBackHoax. Le gouvernement a aussi créé une National Cyber Encryption Agency pour contrer l'extrémisme religieux et les fausses nouvelles en ligne.

B. Des États

Face aux mouvements sociaux lancés par ou avec l'aide des plateformes numériques, en particulier Twitter et Facebook, les gouvernements autoritaires ont eu successivement deux réactions. La première a été une stratégie de la rareté informationnelle en censurant les contenus et en bloquant les

accès, comme en témoignent de nombreux exemples au début des années 2000, de la Chine à l'Afrique du Nord en passant par le Moyen-Orient. Ils ont toutefois rapidement pris conscience du potentiel qu'offraient ces technologies en termes de surveillance et d'influence de leurs citoyens. La deuxième génération du contrôle de la population par internet a donc au contraire consisté à tirer profit de la surabondance informationnelle. Les États se retrouvent dans la position paradoxale d'utiliser aujourd'hui « les mêmes outils qu'ils considéraient auparavant comme une menace, pour déployer les technologies de l'information comme moyen de consolidation du pouvoir et de contrôle social, alimentant des opérations de désinformation et diffusant la propagande gouvernementale à une échelle sans précédent[49] ».

Le dernier rapport annuel de l'ONG Freedom House sur la liberté en ligne[50] montre que de plus en plus d'États manipulent l'information sur les médias sociaux, à l'aide de trolls, de bots ou de faux sites : l'ONG dénonce les actions de 30 gouvernements, contre 23 l'année précédente, et rappelle qu'en 2016 la manipulation en ligne et la désinformation ont joué un rôle important dans les élections d'au moins 18 États. Le cas des États-Unis était particulier en ce qu'il a révélé la manipulation d'un autre État, la Russie, pour défendre ses intérêts et son influence à l'étranger. Il existe en effet deux sortes de manipulations d'origine étatique : celles, les plus courantes, que l'État met en œuvre contre sa propre population, pour la contrôler ; et celles, qui nous intéressent plus spécifiquement ici, qu'il mobilise contre une population d'un autre État, et qui constituent donc des ingérences.

1. Les manipulations visant la population intérieure

Dans la plupart des cas, les gouvernements manipulent l'information donnée à leur propre population pour renforcer leur pouvoir, utilisant des techniques de contrôle surtout développées par la Chine et la Russie mais qui sont désormais devenues « un phénomène mondial » selon le président de Freedom House[51].

49. Carly Nyst et Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, Institute for the Future, 2018, p. 8.

50. Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, novembre 2017.

51. « De plus en plus de gouvernements manipulent les réseaux sociaux », AFP, 14 novembre 2017.

Le *trolling* est l'une de ces techniques, dont l'usage va croissant. On parle d'un « nouveau phénomène », défini comme « l'usage par les États de campagnes ciblées de haine et de harcèlement en ligne pour intimider et réduire au silence des individus critiquant l'État[52] ». Les études de cas sont légion – non seulement en Russie et en Chine (la fameuse « armée des 50 cents », composée de plus de deux millions de personnes, poste près de 450 millions de commentaires par an[53]) mais aussi en Iran (où les services de renseignement et les Gardiens de la révolution peuvent s'appuyer sur un réseau de 18 000 « volontaires » pour surveiller les réseaux sociaux[54]), au Mexique (où l'on a parlé de *Peñabots* pour désigner les bots au service du président Enrique Peña Nieto[55]), en Inde (le BJP, parti au pouvoir, aurait une « IT Cell »[56]), au Vietnam (où le gouvernement a lancé en décembre 2017 une brigade connue sous le nom de « Force 47 » et composée de 10 000 cyberinspecteurs[57]), en Argentine (le président Mauricio Macri est également soupçonné d'avoir recours à une « armée de trolls »[58]), en Corée du Sud (une unité de guerre psychologique du Service national de renseignement aurait payé des millions de citoyens pour dénigrer le candidat libéral et soutenir la candidate conservatrice dans la campagne présidentielle 2012[59]), en Turquie (où une armée de 6 000 « AK Trolls » – du nom du parti – aurait été formée par le régime en réaction aux manifestations de 2013[60]) ou encore aux Philippines, où la campagne ayant conduit à l'élection de Rodrigo Duterte a été décrite comme un cas exemplaire de « trollage patriotique », une pratique définie comme « l'utilisation de campagnes de harcèlement et de propagande haineuse en ligne, ciblées et parrainées par un État dans le but précis de réduire au silence et d'intimider

52. Carly Nyst et Nick Monaco, *State-Sponsored Trolling, op. cit.*, p. 1. Voir aussi Michael Riley, Lauren Etter et Bibhudatta Pradhan, *A Global Guide to State-Sponsored Trolling*, Bloomberg, 19 juillet 2018.

53. Gary King, Jennifer Pan, Margaret E. Roberts, « How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument », *American Political Science Review*, 111:3, 2017, p. 484-501.

54. RSF, *Online Harassment of Journalists: Attack of the trolls*, 2018, p. 27.

55. Erin Gallagher, « Mexican Botnet Dirt Wars: Bots are waging a dirty war in Mexican Social media », media.ccc.de, août 2015.

56. Swati Chaturvedi, *I am a Troll: Inside the Secret World of the BJP's Digital Army*, Juggernaut Publication, 2016.

57. RSF, *Online Harassment of Journalists: Attack of the trolls*, *op. cit.*, p. 28.

58. « Trolls: cómo funciona el ejército de perfiles macristas truchos que denuncian Tinelli y la oposición », politicaargentina.com, 15 juillet 2016.

59. « Ex-intelligence official arrested for 2012 election-meddling », *Korea Herald*, 19 septembre 2017.

60. RSF, *Online Harassment of Journalists: Attack of the trolls*, *op. cit.*, p. 25.

des personnes[61] ». L'équipe de Duterte s'en prenait à toute personne les critiquant : « Les attaques brutales dirigées en ligne contre l'un ou l'autre citoyen, politicien ou journaliste, en vue d'en faire des exemples, ont eu un effet paralysant » – selon ce que la théorie de la communication appelle une « spirale du silence[62] ».

Le *trolling* plus ou moins étatique (dépendamment du degré de contrôle de l'État sur les trolls) n'est que l'une des actions que peuvent mener les « cybertroupes », définies comme « des équipes du gouvernement, des armées ou des partis politiques dont la mission est de manipuler l'opinion publique via les médias sociaux[63] ». Beaucoup d'États s'en sont dotés, y compris des États démocratiques, mais toutes ces structures ne sont évidemment pas comparables dans leurs activités.

L'objet du présent rapport n'est pas le recensement de l'ensemble des manipulations informationnelles mises en œuvre par des États contre leur propre population – c'est le rôle des ONG de défense des droits humains – mais d'analyser celles qui visent des populations étrangères et constituent donc des ingérences, en premier lieu contre nos démocraties.

2. Les manipulations visant une population extérieure

Cette catégorie concerne beaucoup moins d'États. Nous ne développerons dans les pages suivantes que les principaux d'entre eux : en premier lieu la Russie, et dans une moindre mesure la Chine. Cela ne signifie pas, naturellement, que seuls ces deux États manipulent l'information en dehors de leurs frontières : d'autres le font ou tentent de le faire, mais avec des moyens et une incidence tellement moindres sur la politique internationale qu'il est justifié de s'arrêter prioritairement sur ces deux cas.

a. La Russie

Ce n'est pas faire preuve de « russophobie » que de constater que toutes les ingérences récentes dans des référendums (Pays-Bas, Brexit, Catalogne) et des élections (États-Unis, France, Allemagne) sont liées, de près ou de loin, à la Russie. Nos interlocuteurs dans les instances européennes

61. Carly Nyst, « Patriotic Trolling: How governments endorse hate campaigns against critics », *The Guardian*, 12 juillet 2017.

62. SCRS, *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui : points saillants de l'atelier*, Ottawa, février 2018, p. 88.

63. Samantha Bradshaw et Philip N. Howard, *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Working paper n° 2017.12, University of Oxford, juillet 2017, p. 3.

attribuent 80 % des efforts d'influence en Europe à la Russie, le reste provenant d'autres États (principalement la Chine et l'Iran) et d'acteurs non étatiques (groupes djihadistes, en particulier Daech)[64]. Pour ne prendre que l'exemple de l'élection présidentielle française de 2017, une analyse indépendante des 800 sites les plus visités durant la campagne et de près de 8 millions de liens partagés entre novembre 2016 et avril 2017 « n'a identifié d'influence étrangère qu'en provenance de Russie. Aucune autre source étrangère d'influence n'a été détectée[65] ». De nombreux théoriciens ou officiels russes ont d'ailleurs mis en avant l'utilisation de l'information à des fins d'intimidation et de déstabilisation politiques, avec une recherche d'objectifs stratégiques (voir *infra*).

Pour un certain nombre de pays particulièrement exposés – les pays baltes et scandinaves, les pays d'Europe centrale et orientale –, il n'y a là rien de nouveau. Ils sont depuis longtemps la cible de campagnes de manipulation de l'information et, jusqu'en 2014, prêchaient dans le désert : leurs tentatives d'attirer l'attention sur ce phénomène ont longtemps suscité chez les « grands » pays d'Europe de l'Ouest de l'indifférence voire de l'énervement pour ce qui était parfois décrit comme de « l'hystérie » anti-russe. Tout cela a changé.

Les responsables politiques occidentaux n'hésitent plus à accuser nommément la Russie. Dans son discours annuel devant le Lord Maire de Londres en novembre 2017, Theresa May s'est ainsi adressée directement à Moscou : « J'ai un message très simple pour la Russie. Nous savons ce que vous faites. Vous n'y arriverez pas parce que vous sous-estimez la résistance de nos démocraties, la capacité d'attraction des sociétés libres et ouvertes, ainsi que l'engagement durable des nations occidentales envers les alliances qui les unissent[66]. » Elle accuse notamment la Russie de l'annexion de la Crimée, du conflit du Donbass, des violations de l'espace aérien de pays européens, des cyberattaques et des ingérences dans les processus électoraux. La *National Security Strategy* suédoise de 2017 accuse tout aussi explicitement la Russie de mener en Suède et dans d'autres États occidentaux des opérations d'influence visant à « semer la discorde, créer de l'incertitude et influencer les processus de prise de décision et les choix politiques ». Peter Hultqvist, le ministre de la Défense, a aussi dénoncé « l'agression inacceptable de la Russie en Ukraine », et le recours

64. Entretien à Bruxelles, le 26 septembre 2017.

65. Bakamo, *2017 French Election Social Media Landscape: The Role and Impact of Non-Traditional Publishers in the French Elections 2017*, 19 avril 2017, p. 18.

66. PM speech to the Lord Mayor's Banquet, 13 novembre 2017.

« systématique à la désinformation » et aux cyberattaques par Moscou pour « diviser l'Ouest »[67].

Ayant constaté d'autres attaques à l'approche des élections fédérales allemandes de 2017, le directeur de l'agence de renseignement intérieur (Bundesamt für Verfassungsschutz) a directement accusé le Kremlin : « Nous reconnaissons là une campagne dirigée par la Russie. Nos homologues tentent d'obtenir des informations pouvant être utilisées pour des opérations de désinformation ou d'influence[68]. » Dans son rapport sur la désinformation, le service canadien du renseignement de sécurité (SCRS) estime qu'elle est « le plus habile pourvoyeur étatique de mensonges[69] ». Le ministre français de l'Europe et des Affaires étrangères a également évoqué « les campagnes orchestrées depuis la Russie contre le candidat Emmanuel Macron[70] ».

Moscou n'est certes pas le seul acteur étatique qui utilise ces tactiques, mais c'est le seul qui les utilise aussi bien, depuis aussi longtemps, qui les a érigées en doctrine officielle et dont la stratégie assumée est d'affaiblir l'Occident, comme le montreront les pages suivantes.

Pour être exact, il faudrait comme le recommande le SCRS parler du Kremlin plutôt que de « la Russie », pour ne pas faire l'amalgame entre le pouvoir et le peuple. Les Russes sont les premières victimes des manipulations de l'information : « Pratiquement toutes les mesures prises par le Kremlin contre l'Occident ont d'abord été mises en œuvre en Russie, contre le peuple russe et contre de nombreuses minorités ethniques, nationales et religieuses[71]. » Il faut d'ailleurs ajouter que « beaucoup de Russes sont parfaitement conscients que les nouvelles sont truquées : le pouvoir du Kremlin ne réside pas dans une tentative de persuader les gens qu'il dit la vérité mais en leur faisant clairement comprendre qu'il peut dicter les termes de "la vérité"[72] ».

Nous nous limitons ici à l'influence *par l'information*, qui n'est qu'une partie des moyens d'influence du Kremlin, les autres étant de nature politique, diplomatique, militaire, économique, culturelle. Il a « arsenalisé »

67. Discours du 20 mai 2017 à l'université Johns Hopkins.

68. Andrea Shalal, « Germany Challenges Russia over alleged cyberattacks », Reuters, 4 mai 2017.

69. SCRS, *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui : points saillants de l'atelier*, *op. cit.*, p. 6.

70. Jean-Yves Le Drian, *Discours de clôture* du 4 avril 2018, *op. cit.*

71. SCRS, *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui : points saillants de l'atelier*, *op. cit.*, p. 25.

72. Peter Pomerantsev et Michael Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Interpreter, a project of the Institute of Modern Russia, 2014, p. 10.

quatre sphères d'activités en particulier : « les médias traditionnels et sociaux, l'idéologie et la culture, le crime et la corruption, et l'énergie[73] ». L'influence russe, notamment en France, est déjà bien étudiée[74]. Les pages suivantes se concentrent sur son volet informationnel.

Une tradition soviétique

La désinformation russe – impliquant notamment des interviews de faux experts, des documents contrefaits, et des photos et vidéos retouchées – a une longue tradition remontant à la période soviétique. Le mot lui-même vient du russe (*dezinformatzia*)[75]. La désinformation comme arme de guerre a commencé à être systématisée en 1923 avec la création d'une unité spéciale au sein du Guépéou, et la première opération importante était l'opération Trust (1923-1927) visant les Russes blancs en exil. L'usage de la désinformation s'est sophistiqué à la fin des années 1960 sous l'impulsion du directeur du KGB Iouri Andropov[76]. La tentative soviétique de désinformation la plus célèbre de cette période est certainement la théorie selon laquelle JFK a été assassiné par la CIA. Cette rumeur soviétique est toujours populaire, et utilisée par le Kremlin pour se défendre de certaines accusations en les faisant passer pour des opérations sous fausse bannière (*false flag*). Parmi les autres fausses nouvelles fameuses de l'époque soviétique, se trouvaient des histoires affirmant notamment la responsabilité américaine dans le putsch des généraux en 1961 en France, dans la tentative d'assassinat du pape Jean-Paul II en 1981 ou encore dans la « création » du virus du sida. L'interférence dans les processus démocratiques n'est pas non plus nouvelle.

73. Bob Corker *et al.*, *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, United States Senate, 10 janvier 2018, p. 37. Cette expression a été popularisée par Pomerantsev et Weiss qui, dans un rapport de 2014, estimaient que le Kremlin « arsenalisait » l'information, l'argent et la culture (*The Menace of Unreality*, *op. cit.*).

74. Voir notamment Cécile Vaissié, *Les Réseaux du Kremlin en France*, Les petits matins, 2016 ; Nicolas Hénin, *La France russe*, Fayard, 2016 ; Olivier Schmitt, *Pourquoi Poutine est notre allié ? Anatomie d'une passion française*, Hikari, 2016 ; Céline Marangé, *Les Stratégies et les pratiques d'influence de la Russie*, Étude de l'IRSEM, n° 49, mars 2017.

75. Sur l'histoire des opérations soviétiques de désinformation, voir les notes de Vasili Mitrokhin, qui a été archiviste du KGB pendant trente ans avant de passer à l'Ouest en 1992, et dont Christopher Andrew notamment a tiré deux livres (*The Mitrokhin Archive: The KGB in Europe and the West*, Allen Lane, 1999 et *The Sword and the Shield: the Mitrokhin Archive and the Secret History of the KGB*, Basic Books, 1999). Voir aussi général Ion Mihai Pacepa, *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, 2013.

76. Cité dans SCRS, *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui : points saillants de l'atelier*, *op. cit.*, p. 26-27.

Les « mesures actives » désignent l'ensemble des stratégies et techniques, « ouvertes » ou secrètes, mises en œuvre par le Kremlin pour influencer les opinions et les agissements des opinions publiques étrangères. Parmi celles-ci, la désinformation, mais également les infiltrations ou manipulations d'organisations de jeunesse ou de syndicats, le recours à des agents d'influence, l'utilisation de médias étrangers pro-russes ou *mainstream* pour disséminer l'information. Or, la Maison-Blanche refusa d'y répondre directement. C'est seulement en 1981 que l'administration Reagan créa un groupe interagences (réunissant la CIA, l'USIA, le FBI et le département d'État) pour analyser et organiser les moyens de la riposte sous la forme de rapports communs présentés au Congrès et de briefings destinés aux principaux organes de presse. Ce précédent représente l'unique occurrence d'une réponse coordonnée et efficace de l'appareil institutionnel américain à la menace de l'influence soviétique.

Le 12 avril 1982, Iouri Andropov, toujours directeur du KGB, ordonne à tous les agents de prendre des « mesures actives » pour que Ronald Reagan ne soit pas réélu[77]. Moscou a également lancé « une campagne de propagande massive » pour faire battre Helmut Kohl lors des élections fédérales allemandes de 1983, en vain[78].

In fine, et même si la Russie d'aujourd'hui n'est plus l'URSS, la continuité est frappante : les moyens ont parfois changé mais la doctrine reste la même, comme le recours aux « vieilles méthodes (sabotage, tactique de diversion, désinformation, terreur d'État, manipulation, propagande agressive, exploitation du potentiel de protestation de la population locale)[79] ».

Les opérations informationnelles russes sont aujourd'hui un habile mélange de propagande de tradition soviétique et de divertissement à l'américaine. Il y a une part mimétique dans l'approche russe, qui s'inspire des dernières techniques occidentales de communication et de relations publiques. Le Kremlin bénéficie d'ailleurs de l'aide de certaines sociétés, comme Ketchum, une entreprise américaine de relations publiques, dont le plus beau « coup » a été de placer une tribune de Poutine dans le *New York Times* le 11 septembre 2013, date symbolique[80].

77. Christopher M. Andrew, *The Sword and the Shield*, *op. cit.*, p. 242.

78. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, *op. cit.*, p. 37.

79. Jolanta Darczewska, « The Devil is in the details: Information warfare in the light of Russia's Military Doctrine », *Point of View,* n° 50, Varsovie, mai 2015, p. 7.

80. Peter Pomerantsev et Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 18.

L'évolution de l'approche russe

Une différence majeure avec la période soviétique est la renonciation idéologique : l'objectif des manipulations de l'information n'est plus de convaincre d'une idéologie alternative – ce que les autorités russes reconnaissent volontiers (« à la différence de l'URSS, la Russie a renoncé à l'exportation d'une quelconque idéologie[81] »). Cela ne signifie pas, naturellement, qu'elle a renoncé à produire un effet – simplement l'effet recherché n'est plus le même. Il s'agit moins de convaincre que d'affaiblir en divisant. Et, de ce point de vue, les techniques soviétiques restent utiles.

La continuation et l'adaptation des techniques soviétiques se sont faites en plusieurs étapes. Moscou n'a pu que constater que son narratif de la guerre de Tchétchénie, à partir de 1999, n'était pas adopté par l'opinion publique internationale, alors même que la population russe s'est dans sa majorité ralliée au nouveau président Poutine et autour de sa volonté affichée de lutter contre le terrorisme tchétchène.

Suite aux « révolutions de couleur » en Géorgie (2003) et en Ukraine (2004), le Kremlin a pu mesurer l'attrait sur son « étranger proche » d'un narratif démocratique largement diffusé à l'époque par des médias soutenus par l'Occident. Il va donc travailler à renforcer et redéfinir ses outils d'influence internationale. D'abord en tentant une approche classique du *soft power*, fondée sur l'attraction, en créant le club de Valdai ou en recrutant des communicants[82]. C'est dans ce contexte que la chaîne de télévision Russia Today est créée, en décembre 2005, avec l'objectif d'améliorer l'image de la Russie à l'étranger.

Mais les résultats tardent à venir et la guerre de Géorgie de 2008 confirme les faiblesses du dispositif informationnel russe : en dépit de ses efforts, Russia Today échoue à influer sur la perception internationale du conflit. Elle change donc de stratégie : renommée « RT » l'année suivante, un nom plus neutre qui n'affiche pas immédiatement son origine russe, elle va passer d'une démarche positive (promouvoir la Russie), qui visiblement ne fonctionnait pas, à une démarche négative visant à discréditer l'adversaire, y compris en recrutant des voix occidentales (journalistes, experts, militants, personnalités)[83].

81. Commission chargée de la défense de la souveraineté et de la protection contre l'ingérence dans les affaires intérieures du Conseil de la Fédération (chambre haute), rapport du 5 mars 2018 (http://council.gov.ru/media/files/BX3FqMRAl7ykAmPLRl4cR1ju4RaswiKN.pdf).

82. Peter Pomerantsev et Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 12.

83. *Ibid.*, p. 15.

Un tournant important intervient en 2011 avec, d'une part, les printemps arabes, perçus à Moscou comme inspirés et soutenus par l'Occident et, d'autre part, la contestation des élections législatives russes de décembre 2011, qui mobilise des dizaines de milliers de personnes dans plusieurs villes de Russie. Poutine croit à des manipulations occidentales pour le renverser. C'est suite à cet épisode que le Kremlin fait inscrire dans la doctrine militaire « le potentiel de protestation de la population » comme l'une des variables les plus importantes des conflits armés. Il cible d'abord les Russes afin d'étouffer la protestation (répression des ONG avec la loi sur les agents de l'étranger et purges dans les médias ; en septembre 2012, le Kremlin ferme USAID, présentée comme un agent d'influence). Au même moment est mise sur pied l'usine à trolls de Saint-Pétersbourg, devenue fameuse par la suite (voir *infra*) – qui a donc d'abord été créée à des fins de contrôle de la population russe.

Le mouvement Maïdan et la chute du régime Ianoukovitch en Ukraine ont ensuite été perçus comme un revers par le Kremlin, qui voyait arriver à proximité immédiate de ses frontières, qui plus est en Ukraine, le phénomène de *regime change*, nécessairement inspiré, selon Moscou, par les Occidentaux. Ce traumatisme explique pour partie l'intervention militaire en Ukraine, d'abord en Crimée puis dans le Donbass. Il explique également l'intensité de la guerre informationnelle menée par la Russie dès le début de la crise ukrainienne.

Après avoir mis en œuvre un ensemble de mesures visant à juguler le potentiel de protestation de la population russe, le Kremlin a renforcé, depuis la crise ukrainienne particulièrement, son offensive informationnelle à la fois vis-à-vis des pays de l'« étranger proche » et des pays occidentaux. Depuis 2016, la sophistication se poursuit avec l'adoption d'une nouvelle doctrine de l'information et, en 2017, d'une stratégie de développement de la société de l'information, ainsi que la création de « cyber-brigades », l'élargissement de la compétence de la Garde nationale aux champs informationnel et cyber, etc.[84].

Moscou considère que ses actions sont défensives, s'estimant victime d'une guerre de l'information menée par l'Occident, en particulier les États-Unis. La défense des valeurs démocratiques et libérales et le soutien à la société civile sont considérés comme des actions subversives visant un changement de régime. La perception d'une domination occidentale dans le champ informationnel (fondée sur le constat que

84. SCRS, *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui : points saillants de l'atelier*, *op. cit.*, p. 35.

les grands médias américains et britanniques sont beaucoup plus suivis que RT, par exemple) met la Russie sur la défensive. Dans la doctrine de l'État, il est écrit que « les États-Unis et leurs alliés […] cherchent à conserver leur domination dans les affaires internationales » en « contenant » la Russie par une « pression politique, économique, militaire et informationnelle »[85].

Moscou a d'ailleurs fait une réponse symétrique aux accusations occidentales d'ingérences dans les processus démocratiques : le 30 mai 2018, la commission chargée de la défense de la souveraineté et de la protection contre l'ingérence dans les affaires intérieures du Conseil de la Fédération de Russie (chambre haute du parlement) a publié un *Rapport spécial sur les atteintes à la souveraineté électorale lors des élections présidentielles en Fédération de Russie* qui accuse les États-Unis, l'OTAN, l'UE, l'Australie et plusieurs États post-soviétiques dont l'Ukraine d'avoir lancé des « attaques massives » contre les élections présidentielles de 2018, à la fois des cyberattaques et des opérations d'influence via la société civile. Le rapport conclut à l'échec de cette tentative. On notera qu'aucune preuve n'est avancée à l'appui de cette thèse et que, si la Commission électorale centrale a bien constaté des cyberattaques le jour du vote, celles-ci n'ont pas été attribuées.

La « guerre de nouvelle génération »

La communauté stratégique russe parle de « guerre de nouvelle génération » pour désigner l'usage croissant de moyens non militaires et non létaux (ce que les Américains appellent le *political warfare*). Côté occidental, on parle volontiers de la « doctrine » Guérassimov, du nom du général chef d'état-major des armées russes, comme l'une des manifestations de la « guerre hybride ». Il ne s'agit en réalité que d'extraits de l'un de ses articles, publié en 2013 dans un hebdomadaire militaire, dans lesquels il affirme notamment :

> On observe au XXIe siècle une tendance à l'effacement des distinctions entre l'état de guerre et l'état de paix. […] Les moyens non militaires ont vu leur rôle s'accroître pour atteindre des objectifs stratégiques et politiques, et, dans de nombreux cas, dépassent de loin par leur efficacité la force des armes. Les méthodes de lutte utilisées mettent désormais l'accent sur une large [gamme] de moyens politiques, économiques, informationnels, humanitaires, ainsi que d'autres moyens non militaires, réalisés par l'implication du potentiel de protestation de la population. Tout ceci

85. Stratégie de sécurité nationale du 31 décembre 2015.

> est complété par des moyens militaires dissimulés, y compris par la mise en œuvre de manifestations d'opposition [dans la sphère] de l'information et d'actions des forces spéciales d'intervention[86].

Ce n'est ni une doctrine ni nouveau : la même idée avait été formulée à plusieurs reprises dans les revues militaires russes au cours de la décennie précédente. « L'importance et la part proportionnelle des moyens non militaires ont considérablement augmenté », notait déjà Makhmut Gareev, ancien vice-CEMA soviétique et actuel président de l'Académie des sciences militaires russes, en 2003[87]. En 2010, Chekinov et Bogdanov l'ont répété[88], et l'amiral Pirumov écrit que « la guerre de l'information consiste à sécuriser les objectifs de la politique nationale en temps de guerre comme de paix par des moyens et des techniques permettant d'influencer les ressources informationnelles du camp adverse, [dont] la désinformation (tromperie), la manipulation (situationnelle ou sociétale), la propagande (conversion, séparation, démoralisation, désertion, captivité), le lobbying, le contrôle des crises et le chantage[89] ».

Surtout, le discours de Guérassimov est censé décrire la supposée action des Occidentaux dans le cadre des printemps arabes. Finalement, en Ukraine en 2014, la Russie reproduit ce qu'elle pense que les Occidentaux ont fait au cours des révolutions de couleur, des printemps arabes et du Maïdan ukrainien. Guérassimov aime d'ailleurs rappeler que le concept de « guerre hybride » est apparu en 2005 aux États-Unis, sous la plume d'un certain général James Mattis, désormais secrétaire à la Défense[90].

La « guerre de l'information »

Dans cette guerre de nouvelle génération, la part informationnelle occupe une place centrale « puisque […] le principal champ de bataille est

86. Valery Guérassimov, « La valeur de la science de la prédiction », *Voenno-promyshlennyj kur'er* (*Le Courrier militaro-industriel*), 8:476, 27 février-5 mars 2013, traduit par Céline Marangé dans Céline Marangé, *Les Stratégies et les pratiques d'influence de la Russie*, *op. cit.*, p. 21.

87. Makhmut Gareev, « If There Were War Tomorrow », *Armeyskiy Sbornik*, 1er avril 2003, cité dans Linda Robinson *et al.*, *Modern Political Warfare. Current Practices and Possible Responses,* Rand Corporation, 2018, p. 43.

88. Sergei Chekinov et Sergei Bogdanov, « Asymmetrical Actions to Maintain Russia's Military Security », *Military Thought*, vol. 1, 2010, p. 17-22.

89. V.S. Pirumov, *Informatsionnoe Protivoborstvo*, 3, Moscow, 2010, cité par Peter Pomerantsev et Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 12.

90. James N. Mattis et Frank Hoffman, « Future Warfare: The Rise of Hybrid Wars », *Proceedings Magazine* (U.S. Naval Institute), 131:11, novembre 2005, p. 18-19.

la conscience, la perception et les calculs stratégiques de l'adversaire[91] ». Le but est d'acquérir la « supériorité informationnelle[92] ».

L'élite politique et militaire russe n'hésite donc pas à utiliser le terme de « guerre de l'information » (*informatsionaya voyna*), tout en maintenant sa posture défensive, c'est-à-dire en accusant l'Occident et notamment les États-Unis de mener une guerre de l'information contre Moscou mais aussi ailleurs (les printemps arabes de 2011 sont fréquemment cités en exemple). Ils prennent cette expression dans un sens large : les cyberopérations, par exemple, ne sont qu'un sous-domaine de la guerre de l'information[93]. Et lorsque l'Académie militaire de l'état-major des forces armées lui consacre une entrée dans un glossaire, c'est pour distinguer l'acception russe, applicable en tout temps, non limitée au temps de guerre, de l'acception occidentale qui limite les opérations informationnelles à la période des hostilités[94] – confirmant ainsi le continuum russe entre la guerre et la paix, et la conviction assumée d'une différence (qui est un avantage) par rapport à « l'Occident » de ce point de vue.

En mars 2018, plusieurs membres de la Douma ont évoqué la possibilité d'introduire le concept de « guerre de l'information » dans la législation russe : Mikhail Degtyarev a par exemple déclaré que « c'est la continuation de la guerre de l'information lancée contre la Russie. Nous devrions prendre une position plus ferme et commencer par la consolidation législative de la notion de "guerre de l'information"[95] ».

En dépit du dispositif déployé, dont on exagère souvent les capacités, la « guerre informationnelle » russe se heurte à plusieurs limites structurelles. D'abord, la démocratisation de l'information grâce à internet, surtout dans les pays démocratiques, crée une concurrence féroce pour les grands médias russes : en termes d'audience, à la télévision ou même sur les réseaux sociaux, RT reste bien en-deçà de la BBC, de CNN ou d'Al-Jazeera. Cependant, cette même démocratisation de l'information, qui est ambivalente, crée aussi davantage de relais et de moyens d'atteindre certaines audiences, et rend la désinformation plus facile.

---

91. Dima Adamsky, *Cross-Domain Coercion: The Current Russian Art of Strategy*, IFRI, Proliferation Papers, n° 54, novembre 2015, p. 26.

92. Sergei Chekinov et Sergei Bogdanov, « Asymmetrical Actions to Maintain Russia's Military Security », *op. cit.*

93. Keir Giles, *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, 2016, p. 4.

94. Cité par Keir Giles, *The Next Phase of Russian Information Warfare*, *op. cit.*, p. 2.

95. Dar'ja Rynochnova, « Дегтярев предложил внести в законодательство понятие "информационной Войны" », *Parlamentskaja Gazeta*, 13 mars 2018.

Ensuite, le Kremlin ne crée pas tant des crises qu'il n'exploite les vulnérabilités existantes, les divisions, tensions politiques ou intercommunautaires, et souffle sur les braises. Sa logique est réactive plus qu'active.

Enfin, il faut aussi savoir relativiser les capacités des services russes et explorer d'autres causes, souvent endogènes, des crises qui parcourent en ce moment les démocraties occidentales car « tout ce qui arrive de favorable à la Russie n'est pas nécessairement le fait de la Russie, tout comme les États-Unis ne sont pas responsables de tout ce qui est à leur avantage[96] ». Il faut résister à la tentation d'utiliser la Russie pour expliquer tous nos maux, de l'élection de Trump au Brexit, et donc nous déresponsabiliser. Lorsqu'elle fonctionne, la désinformation est le symptôme d'autre chose, d'une crise de confiance dans laquelle les démocraties libérales doivent assumer leur part de responsabilité.

b. La Chine

La République populaire de Chine (RPC) possède une longue tradition de lutte idéologique et d'utilisation de la propagande. Aujourd'hui, ce savoir-faire est mis au service des intérêts chinois à l'échelle globale. Au-delà de l'entretien et de l'amélioration de son image, Pékin développe des outils d'influence et d'ingérence à vocation spécifiquement offensive.

En Chine, la fabrication de la propagande, l'endoctrinement idéologique et l'ingénierie du consentement, constituent des prérogatives fondamentales du Parti communiste chinois (PCC). Celui-ci possède une très large structure bureaucratique de contrôle de l'information désormais adaptée au statut de la RPC sur la scène internationale. Le travail idéologique au sein du PCC répond à deux objectifs : d'une part, façonner l'espace politique intérieur et entretenir la légitimité du Parti (par la censure et la manipulation de l'information) ; d'autre part, influencer les opinions internationales et mettre en œuvre la « guerre informationnelle » au profit des ambitions chinoises.

Les organes chargés de la stratégie de propagande et d'influence sont très haut placés dans la hiérarchie politique : numéro cinq du régime, Wang Huning dirige la « commission centrale d'orientation pour l'établissement d'une civilisation spirituelle » qui définit les contenus idéologiques et pilote leur diffusion au niveau national et international. Cette commission supervise le département central de la propagande (*zhongxuanbu*), dirigé par Huang Kunming, membre du Bureau politique du PCC, dont les activités

96. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 56.

se concentrent essentiellement (mais non exclusivement) sur les aspects internes au Parti et la mise en œuvre des moyens au niveau national[97].

Le rôle de la propagande chinoise est crucial dans son dispositif de diplomatie publique. Qu'il s'agisse de répercuter les slogans destinés à orienter les débats intellectuels sur la Chine (*peaceful rise*, *harmonious world*), ou de disséminer les représentations positives dans les opinions publiques, comme actuellement au sujet du projet Belt and Road Initiative (BRI), Pékin maîtrise les contenus et déploie un nombre très élevé de vecteurs. Aujourd'hui, la Chine contrôle plus de 3 000 chaînes de télévision publique, plus de 150 chaînes de télévision payantes, autour de 2 500 stations de radio, environ 2 000 journaux et 10 000 magazines, plus de 3 millions de sites internet et a publié près de 250 000 ouvrages[98]. Ces vecteurs se doublent de réseaux de diffusion de contenus culturels à vocation pédagogique ou académique, comme les Instituts Confucius, qui constituent des relais privilégiés d'influence et de propagation des messages officiels.

Dans le domaine audiovisuel, la Chine a créé en 2016 un groupe étatique de diffusion mondiale, China Global Television Network, constitué à partir de la fusion de plusieurs canaux de la China Central Television Network (CCTV). Les programmes reprennent de manière coordonnée des contenus fournis en majorité par l'agence de presse étatique Xinhua. Cette dernière a vocation à concurrencer les agences internationales (AP, UPI, Bloomberg, Reuters) et diffuse sur tous les supports (internet et téléphonie mobile). À la poursuite des mêmes objectifs, le *Quotidien du peuple*, le *China Daily* et le *Global Times* constituent les principaux journaux chinois en langue anglaise distribués aussi sur les supports numériques.

Au cours des dernières années, la nature des contenus diffusés par ces médias a substantiellement évolué. Dans le contexte d'une accession de la Chine au rang de puissance mondiale impliquée dans les questions stratégiques et de sécurité, les messages critiques à l'encontre des puissances occidentales – États-Unis en premier lieu – se sont faits plus réguliers et élaborés. Si de nombreux contenus reprennent sans détour les productions des agences russes (comme RT ou Sputnik) dans le traitement de la crise syrienne, la critique des actions françaises en Afrique, des positions internationales sur la mer de Chine méridionale ou du « bellicisme » du Japon et de l'Inde font l'objet d'une diffusion régulière et programmée. Il

97. À l'international, ces deux organes s'appuient ensuite sur un réseau très dense de diffuseurs et d'opérateurs dont la tutelle est essentiellement répartie entre le bureau de l'information du Conseil d'État et le ministère des Affaires étrangères.

98. David Shambaugh, *China goes Global. The Partial Power,* Oxford University Press, 2013, p. 227-228.

s'agit là d'une tentative de contre-influence qui cible en priorité les pays d'Europe de l'Est et les audiences africaines. Ces actions font partie d'une propagande globale destinée à contrer et à réduire l'influence des messages et des valeurs démocratiques et libérales. En cela, la constitution de la Belt and Road Media Community vise non seulement à promouvoir les ambitions chinoises, mais aussi à contrer, voire éteindre, les influences médiatiques externes[99].

L'influence informationnelle de la RPC possède une portée globale. Les contenus idéologiques ne servent pas qu'à séduire ou à influencer, ils ont pour ambition d'orienter les opinions publiques et d'interférer au besoin. Cette dimension proactive est aujourd'hui moins agressive que celle déployée par la Russie, mais les dispositifs chinois s'affinent et prennent graduellement de l'ampleur.

La guerre de l'information constitue une dimension à part entière dans la stratégie d'influence et d'intimidation chinoise. Depuis le tournant des années 2000, les stratèges chinois travaillent à la mise en œuvre des « trois guerres » (*sanzhan*) dans le domaine de l'information. Réunissant la guerre de l'opinion publique, la guerre psychologique et la guerre juridique, cette approche combinée est destinée – en temps de paix comme en temps de guerre – à contrôler le discours dominant et à influencer les croyances et perceptions de manière à servir les intérêts de la RPC, tout en réduisant la capacité adverse à y répondre[100]. Visant explicitement les opinions publiques démocratiques, cette stratégie exploite spécifiquement les vulnérabilités des sociétés ouvertes.

Les services de renseignement (ministère de la Sécurité d'État, ministère de la Sécurité publique, le deuxième département de l'armée populaire de libération [APL] et le département des liaisons internationales de l'APL notamment) et certains départements du comité central (Front uni [UFWD]) ont engagé une réflexion similaire ces dernières années. Aux efforts consentis afin de renforcer le narratif chinois (*soft power*) sont ainsi désormais associés des opérations clandestines destinées à décupler les capacités d'influence de la Chine. Cette évolution, liée à la montée en puissance de la Chine sur la scène internationale et à la nouvelle assurance qui en découle, repose également sur une conjoncture singulière : l'exemple russe, dont s'inspire Pékin, et le retrait américain engagé par l'administration Trump.

99. Pékin met ainsi en œuvre de nombreuses conférences visant à façonner les contenus et à influencer les nouvelles générations de journalistes. Voir Lu Anqi, « Chinese and African Media Discuss how to tell good stories », *Chinafrica*, 14 août 2016.

100. Elsa B. Kania, « The PLA's Lateste Strategic Thinking on the Three Warfares », *China Brief*, XVI:13, août 2016, p. 10-14.

Malgré l'ampleur du débat suscité par l'ingérence chinoise en Australie (voir encadré ci-contre) et en Nouvelle-Zélande, l'Europe demeure peu préoccupée par cette menace alors que l'augmentation des opérations chinoises est manifeste.

Les opérations d'ingérence et d'influence chinoises prennent des formes diverses :

- instrumentalisation d'anciens hommes d'État européens de premier plan qui œuvrent à la promotion des intérêts chinois ;
- pénétration des organisations régionales (Interpol, Conseil de l'Europe) afin d'orienter leurs activités dans le sens des intérêts chinois ;
- instrumentalisation des diasporas et de la communauté chinoise vivant à l'étranger, celles-ci pouvant être mobilisées par les agents du Front uni lors de visites diplomatiques par exemple ;
- pressions sur les chercheurs et le dispositif de la recherche académique par le truchement des délivrances de visas et des programmes de financement ;
- distribution dans les principaux quotidiens européens, contre rémunération, d'un supplément de presse (*China Watch*) afin de créer une dépendance financière et d'inciter à une forme d'autocensure dans le traitement de l'actualité liée à la Chine ;
- prise de contrôle de la plupart des médias européens en langue chinoise ;
- mesures de rétorsion contre les gouvernements critiques ou jugés peu « amicaux », à l'instar de la Norvège à l'issue de la décision d'attribuer le prix Nobel de la paix à Liu Xiaobo (abaissement des échanges diplomatiques, sanctions commerciales indirectes, etc.).

La mise en œuvre de cette influence multisectorielle a déjà entraîné des réponses politiques et l'édification de nouveaux dispositifs sécuritaires dans plusieurs démocraties, notamment l'Australie, dont l'Europe pourrait s'inspirer. Pékin bénéficie aujourd'hui de capacités de contre-influence et de lutte informationnelle systématiques et multivectorielles. Les contenus chinois diffusés en Afrique francophone véhiculent souvent des positions et des principes contraires aux intérêts français. Cette dimension dépasse largement le cadre de la relation bilatérale franco-chinoise et s'inscrit dans celui d'une compétition stratégique globale.

L'ingérence chinoise en Australie

L'Australie est une cible privilégiée de l'influence chinoise[101]. Les officiers du département du front uni (UFWD) du PCC et d'autres agences, dont le département de liaison de l'Armée populaire de libération, recrutent de manière ciblée des agents d'influence parmi l'élite australienne (entrepreneurs, politiciens, universitaires, etc.). Les vulnérabilités de Canberra exploitées par Pékin sont la diaspora chinoise (5 % de la population), la dépendance économique et des modèles de financement des universités, des médias et des campagnes électorales qui ont permis d'« acheter » l'accès aux milieux politiques et scientifiques du pays. Certaines personnalités politiques sont corrompues qui, en échange de financements de la part des donateurs chinois, font avancer les positions du PCC sur les questions internationales. Certaines universités australiennes sont également devenues de véritables véhicules de la propagande chinoise. L'autocensure est répandue, y compris chez les chercheurs sur la Chine qui sont de plus en plus nombreux à s'interdire certains sujets, ou d'être trop critiques, par crainte de perdre leur éditeur ou leur accès au terrain. L'Australie a pris conscience de cette évolution inquiétante, en partie due au primat du contre-terrorisme aux dépens du contre-espionnage au sein du service de renseignement intérieur (ASIO) dans les années de l'après-11-Septembre. Un rééquilibrage des priorités est en cours, et Canberra a considérablement rehaussé son arsenal juridique afin de surveiller les investissements étrangers sur son territoire, et notamment dans le domaine médiatique[102]. En juin 2018, le parlement a adopté des lois contre l'espionnage et l'ingérence étrangère.

101. John Garnaut, « How China interferes in Australia. And How Democracies Can Push Back », *Foreign Affairs*, 9 mars 2018 ; Clive Hamilton, *Silent Invasion: China's Influence in Australia*, Hardie Grant, 2018.

102. Joshua Kurlantzick, « For Clues on How to Address China's Growing Political Influence Strategies, Look to Australia », *Council of Foreign Relations*, 18 décembre 2017 et Clive Hamilton, « Australia's Fight Against Chinese Political Interference: What Its New Law Will Do », *Foreign Affairs*, 26 juillet 2018.

Deuxième partie

COMMENT ?

De nos analyses des tentatives de manipulation de l'information dans une vingtaine de pays, se dégagent certains traits communs quant aux facteurs de vulnérabilité et aux moyens employés. Cette partie les expose, avant d'explorer d'autres terrains des manipulations de l'information, par rapport à ceux, bien éprouvés, d'Europe et d'Amérique du Nord.

I. Les facteurs de vulnérabilité

A. La présence de minorités

Les tentatives de manipulation sont facilitées par la présence de minorités dont le sentiment de non-appartenance à une communauté nationale peut être instrumentalisé ou exacerbé. C'est le cas en premier lieu dans les États baltes. L'importante minorité russophone, particulièrement en Lettonie (37 % de la population, un peu moins de 50 % à Riga)[1], n'est pas en soi une menace à la cohésion nationale, d'une part car elle n'est pas uniforme, il n'y a pas une mais plusieurs communautés russophones, de différentes nationalités (lituanienne, lettone ou estonienne, avec ou sans statut de « non-citoyen », russe, biélorusse, ukrainienne), ayant des sentiments

1. La minorité russophone de Lettonie est la plus importante des États baltes, contre 29 % en Estonie et 6 % en Lituanie.

divers à l'égard des autorités locales et russes ; et d'autre part car les personnes venant de Russie jouissent dans les États baltes d'une meilleure qualité de vie et d'une liberté de circulation (vers la Russie comme dans l'espace Schengen si ce sont des résidents permanents lettons) tout à leur avantage. Moscou tente toutefois de les rassembler et de les instrumentaliser dans le cadre de sa politique des « compatriotes », lors d'événements comme la cérémonie du 9 mai, sans y parvenir complètement comme en témoigne la fréquentation en baisse (100 000 personnes en 2017 contre 150 000 en 2016 et 200 000 en 2015). Les médias russes développent également des narratifs ciblant spécifiquement cette minorité (les Lettons russophones seraient discriminés, opprimés, on parle d'« apartheid », parfois de « génocide »).

L'affaire Lisa

L'« affaire Lisa » a agité l'Allemagne en janvier 2016. Après avoir disparu pendant 30 heures, une adolescente de 13 ans, appartenant à la communauté des *Russlanddeutsche*, a prétendu avoir été enlevée, frappée et violée par trois hommes de type « méridional ». La Russie s'est alors immédiatement emparée du sujet, d'abord sur la première chaîne nationale, ensuite dans les médias russes à l'étranger (Sputnik, RT Deutsch) et sur les réseaux sociaux, où l'histoire a été relayée notamment par des groupes d'extrême droite. Via Facebook, des manifestations ont été organisées, impliquant notamment les *Russlanddeutsche* et des groupes néonazis – manifestations couvertes par les médias russes et allemands. Le ministre russe des Affaires étrangères, Sergueï Lavrov, a fait deux déclarations publiques dans lesquelles il accusait les autorités allemandes de dissimuler la réalité derrière du politiquement correct pour des raisons de politique intérieure, mettant en cause la compétence de la police et du système judiciaire allemand. Il estimait que Lisa ne pouvait pas avoir « disparu de son plein gré pendant 30 heures ». Son homologue allemand Frank-Walter Steinmeier a quant à lui accusé la Russie de propagande politique. Finalement, l'enquête a démontré que Lisa avait menti : elle avait disparu volontairement et se trouvait chez un ami.

L'affaire Lisa a montré la puissance que peut avoir une information fausse (déclencher des manifestations, contribuer à la montée des sentiments anti-migrants et frôler une crise diplomatique), la vulnérabilité que constitue pour Berlin la communauté des *Russlanddeutsche* et la nécessité de mettre en place un mécanisme pour réagir au plus vite car, si l'affaire a pu se développer, c'est uniquement parce que le démenti est arrivé trop tard. La principale leçon est donc l'importance de la réactivité.

En Allemagne, l'existence, à côté d'une diaspora russe parfois localement importante, d'une communauté de *Russlanddeutsche* – ces ressortissants de l'espace soviétique de langue allemande, descendants des Allemands de la Volga installés par Catherine II au XVIII[e] siècle, déportés par Staline en Asie centrale, puis rapatriés en Allemagne après la réunification – constitue aussi un terreau propice aux manipulations, qui ont pour premier objectif d'accentuer les divisions entre ces *Russlanddeutsche* et le reste des Allemands, sur fond de suspicion à l'endroit d'autres communautés immigrées.

B. Des divisions internes

Même là où n'existent pas de diaspora significative ou de minorités facilement exploitables, les tentatives de manipulation de l'information peuvent jouer, de façon plus insidieuse, sur les divisions sociales et politiques que connaissent nos démocraties.

La Pologne est à cet égard un cas intéressant. Le pays offre *a priori* peu de prises à des tentatives de manipulation d'origine russe : elle en connaît les méthodes (la guerre soviéto-polonaise de 1919-1921 est rétrospectivement qualifiée de « guerre hybride » – non déclarée, avec de la propagande, de la diversion, des tentatives d'influencer les minorités, etc.) ; 70 ans de communisme ont immunisé la population contre la propagande russe ; le pays n'a ni minorité russophone ni parti politique russophile et le sentiment anti-russe est très répandu. Pour autant, des tentatives d'influence indirecte sur les échéances électorales polonaises ont pu être observées (création de faux comptes sur les réseaux sociaux en vue des élections de 2018 et 2019). Moscou tire avantage des divisions politiques, accrues ces derniers temps.

Les réseaux sociaux polonais ont été étudiés par un chercheur d'Oxford qui montre que, quelques jours seulement après le Maïdan de Kiev, un grand nombre de faux comptes ont fait leur apparition sur Facebook, comme sur différentes plateformes diffusant la propagande russe. Il pointe également la difficulté croissante à les détecter et à les attribuer à la Russie, qui les banalise de mieux en mieux. Il montre aussi que les comptes « de droite » sont deux fois plus nombreux et actifs que ceux « de gauche »[2].

2. Robert Gorwa, *Computational Propaganda in Poland: False Amplifiers and the Digital Public Sphere*, Working Paper, n° 2017.4, University of Oxford, Project on Computational Propaganda, 2017.

C. Des divisions externes

Les tensions entre pays voisins sont également exploitées. Moscou travaille ainsi à semer la discorde entre la Pologne et ses voisins, en premier lieu l'Ukraine – cette relation offrant de nombreux points sensibles, d'abord historiques (les massacres des Polonais en Volhynie) – mais aussi la Biélorussie, la Lituanie et l'Allemagne. L'objectif est que la Pologne soit traitée comme un paria en Europe, s'aliénant non seulement ses voisins immédiats mais aussi l'Union européenne en tant qu'institution. En Lituanie, les autorités ont observé en 2017 une forte recrudescence de messages à l'attention de la communauté polonaise visant non seulement à exacerber les tensions intercommunautaires mais aussi à dégrader les relations diplomatiques entre les deux pays[3]. À l'échelle européenne, Moscou tente d'isoler les États baltes (et la Pologne) en les faisant passer pour des hystériques russophobes paranoïaques auprès des États d'Europe de l'Ouest plus « modérés ». Entretenir les divisions parmi les pays européens sur la question russe, mais aussi les caricaturer, est un enjeu majeur pour le Kremlin.

Dans une autre région, le Golfe, les tensions interétatiques servent aussi à catalyser les manipulations de l'information, comme l'illustre notamment la crise entre le Qatar et ses voisins, déclenchée en mai 2017 par une cyberattaque et l'implantation d'une fausse nouvelle (voir *infra*).

D. Un écosystème médiatique vulnérable

L'une des raisons pour lesquelles les « Macron Leaks » ont échoué à avoir un effet sur l'élection présidentielle française de 2017 (voir *infra*) est que l'écosystème médiatique français est relativement sain. Nous entendons par là le fait que la population s'appuie surtout sur les médias traditionnels respectant des normes journalistiques, et moins qu'ailleurs sur les « tabloïds », beaucoup plus développés outre-Manche, ou les sites conspirationnistes qui prolifèrent dans d'autres pays. Les manipulateurs de l'information utilisent un arsenal diversifié : presse populiste, réseaux sociaux, sites de désinformation mais aussi les médias russes, qui peuvent s'appuyer sur une minorité russophone importante dans le pays visé, ou sur une traduction dans les langues locales. Leurs efforts ont d'autant plus de chances d'aboutir que le paysage médiatique est éclaté, avec des médias traditionnels faibles, suscitant la défiance d'une partie de la population, et une variété de vecteurs populistes et conspirationnistes.

3. State Security Department of the Republic of Lithuania, *National Threat Assessment 2018*, p. 42.

Les médias russophones dans les États baltes

Les médias russophones sont nombreux dans les États baltes (presse, radio, télévision, internet). Depuis 2005, la plateforme russe Baltic Media Alliance (BMA), officiellement enregistrée au Royaume-Uni, permet la retransmission dans toute la région des chaînes russes avec un contenu éditorial adapté (First Baltic Channel a ainsi trois comités éditoriaux, pour chacun des États baltes). Il y a quelques années, la Lettonie (2014) puis la Lituanie (2015) avaient bloqué temporairement la chaîne russe RTR-Planeta, accusée d'inciter à la haine envers les Ukrainiens, mais cette mesure temporaire n'a pas eu d'effets structurants. Disposant d'un budget considérable par rapport aux moyens locaux, et de programmes de divertissement très populaires, les chaînes russes sont difficiles à concurrencer. En Lettonie, les autorités ont renoncé à créer une chaîne russophone, alors que l'Estonie a lancé ETV+ en 2015. Il reste toutefois des programmes russophones sur des chaînes publiques lettones (LT7) et une radio publique russophone particulièrement populaire (Latvijas Radio 4).

En termes d'influence, la télévision russe est considérée comme « la plus grande menace » dans les États baltes car elle permet aux russophones de vivre dans un « cocon informationnel[4] ». Les États baltes n'ont tout simplement pas les moyens d'y opposer une alternative de la même qualité et l'union – l'hypothèse d'une chaîne commune – n'est pas non plus envisageable à cause des rivalités et des différences[5].

Sur internet, les autorités lettones ont refusé d'enregistrer Sputnik sur le domaine .lv – une résistance symbolique puisque le site s'est enregistré en .com (sputniknewslv.com). Les sites les plus efficaces pour diffuser la propagande du Kremlin ne sont pas ceux trop évidemment associés à Moscou, comme Sputnik, mais des sites apparemment locaux, comme Vesti.lv, ou régionaux, comme Baltnews ou Rubaltic. Lancé en 2014 en trois éditions distinctes pour chacun des États baltes, Baltnews appartient à Rossiya Segodnya via des sociétés écrans et le contenu de ses sites est en partie piloté par les diplomates russes à Riga, Vilnius et Tallinn. Quant à Rubaltic, il est enregistré à Kaliningrad. Il y a aussi le Club IMHO, un réseau de blogs russophones appartenant au militant pro-russe letton Yuri Alexeyev qui, après s'être développé avec succès en Lettonie, s'implante en Biélorussie et en Ukraine.

4. Todd C. Helmus *et al.*, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, 2018, p. 66-67.

5. *Ibid.*, p. 69.

E. Des institutions contestées

La première partie a montré comment la défiance à l'égard des institutions était l'une des causes essentielles de l'essor et de l'efficacité des tentatives de manipulation de l'information. Elle fait des institutions démocratiques et des politiques publiques des cibles faciles, en entretenant constamment le doute, soit sur un prétendu « agenda caché » des gouvernements, soit sur l'efficacité réelle de leur action.

Ainsi, l'un des narratifs propagés par les tentatives de manipulation dans les États baltes est celui selon lequel ces États seraient des États faillis, envahis par la corruption et qui ne seraient pas viables sans le soutien occidental. Ce narratif est d'autant plus dangereux que, comme dans toutes les démocraties, une frange de la population est critique et déçue par son gouvernement.

En Ukraine, le Kremlin se livre depuis 2014 à une remise en cause systématique des autorités, accusées d'inefficacité, de corruption, etc. À cet effet, des centaines de groupes thématiques ont été créés sur des réseaux sociaux contrôlés par Moscou (VKontakte était particulièrement actif jusqu'à son interdiction en mai 2017). Ces réseaux sociaux utilisent des symboles pro-ukrainiens et une rhétorique nationaliste appelant à l'organisation d'un troisième Maïdan[6].

II. Les moyens des manipulations informationnelles

A. Des leviers et des vecteurs multiformes

Les moyens à la disposition du Kremlin pour mener sa « guerre de l'information » sont bien résumés par la RAND qui distingue quatre catégories, avec un degré de contrôle variable du Kremlin[7] :

1) les instances gouvernementales (le Kremlin lui-même, les ministères, les ambassades et les agences publiques comme Rossotrudnichestvo, dont la mission est l'influence russe à l'étranger, notamment dans les pays de la CEI) ;

2) les fausses ONG, financées par l'État et/ou qui travaillent étroitement avec lui (Russkiy Mir créé en 2007 pour promouvoir la langue et la culture russe à l'étranger et qui sert de pont entre le gouvernement et

6. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 16.
7. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 56.

des relais d'influence à l'étranger ; RT ou encore l'IDC, le think tank du Kremlin, qui a des bureaux à Paris et New York) ;

3) d'autres organisations présentées comme n'ayant aucun lien avec l'État mais qui en fait agissent comme des proxys (le club de motards *Notchnye Volki*, « les Loups de la nuit », qui sont au nombre de 5 000, proches de Poutine) – sur ce segment la stratégie du Kremlin est d'occuper une niche pour que d'autres groupes qui lui seraient moins favorables ne s'y installent pas[8] – ;

4) des relais religieux, politiques ou économiques, indépendants dans leur prise de décision mais qui, sans être aux ordres du Kremlin, défendent soit ses intérêts soit un rapprochement avec ce dernier (l'Église orthodoxe, certains milieux économiques, des partis politiques défendant un rapprochement avec la Russie comme le Bloc d'opposition en Ukraine, le Parti des socialistes de la République de Moldavie ou encore l'Alliance des patriotes en Géorgie pour ce qui concerne l'« étranger proche »).

On pourrait ajouter une cinquième catégorie d'individus à l'étranger utilisés comme faire-valoir auprès de l'opinion intérieure ou relais locaux de la politique extérieure, des « idiots utiles » selon l'expression (sans doute faussement) attribuée à Lénine : il peut s'agir d'intellectuels, que le Kremlin tente de « capter » via des forums comme le club de Valdaï, de politiciens de l'extrême droite à l'extrême gauche, ou de militants de divers mouvements[9]. Les liens avec l'extérieur sont donc à la fois formels (via le réseau diplomatique) et informels (via des proxys, milieux d'affaires, société civile, etc.).

Aux moyens précédents, qui relèvent de ce que l'on appelle la propagande « blanche » (assumée), s'ajoutent des moyens de propagande « grise » tels que les sites conspirationnistes et diverses ressources du Darknet, ainsi que des moyens de propagande « noire », c'est-à-dire réfutables, tels que les trolls, les bots et les hackers[10]. C'est ainsi que s'organisent les campagnes de manipulation de l'information : l'État attaquant morcelle ses actions pour dissimuler son empreinte et donner l'impression d'un mouvement spontané, qui apparaît sur différentes plateformes, dans différents médias, à différents moments, en utilisant tout le spectre du clandestin

8. Mark Galeotti, « An Unusual Friendship: Bikers and the Kremlin (Op-Ed) », *The Moscow Times*, 19 mai 2015.

9. Voir Orysia Lutsevych, *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood,* Chatham House, avril 2016.

10. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 12.

(trolls) au public (diplomatie) – alors qu'il s'agit en réalité d'une action coordonnée[11].

Le Kremlin dispose d'un « arsenal médiatique[12] » composé d'abord de deux principales agences tournées vers l'étranger, Rossiya Segodnya et RT, présentées comme distinctes mais en réalité dirigées par la même rédactrice en chef, Margarita Simonyan. Rossiya Segodnya est propriétaire de Sputnik (fondé en novembre 2014 pour remplacer la Voix de la Russie) et de RT, créé sous le nom de Russia Today en 2005 et renommé en 2009. L'agence prétend être « complètement indépendante[13] » mais ne cache pourtant pas que son objectif est de « garantir les intérêts nationaux de la Fédération de Russie dans la sphère informationnelle[14] ». L'intention initiale était d'utiliser ces relais pour améliorer l'image de la Russie à l'étranger mais, devant l'inefficacité de la manœuvre, le Kremlin a réorienté ces moyens vers une approche négative : ils servent désormais surtout à dégrader l'image de l'adversaire. Ces médias sont peu suivis à l'échelle internationale, où CNN, la BBC, Al-Jazeera dominent. Ils enregistrent toutefois un important succès auprès d'un auditoire sensible aux formations politiques d'extrême gauche ou d'extrême droite ou perméable aux théories conspirationnistes.

Le Kremlin peut aussi compter sur les chaînes nationales russes (telles que Rossiya 24, NTV, Channel One, RTR), encore très regardées dans les pays de l'étranger proche, souvent parce qu'elles sont de meilleure qualité que les chaînes locales. Dans les États baltes, la plupart des « journalistes » russes qui font des reportages à charge travaillent clandestinement : ils entrent dans le pays avec un visa de tourisme ou d'affaires souvent émis en Europe[15]. Ils interrogent des personnalités marginales, opposées au gouvernement, et filment les mouvements de protestation en exagérant leur ampleur pour donner l'impression d'un pays divisé, au bord de la guerre civile.

11. Voir Ben Nimmo, « Russia's Full Spectrum Propaganda: A case study in how Russia's propaganda machine works », DFRLab Medium.com, 23 janvier 2018.

12. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 61.

13. Tweet de Ben Nimmo présentant le document enregistrant RIA Global aux États-Unis, 21 juin 2018 (https://twitter.com/benimmo/status/1009777111857553409).

14. Tweet de Ben Nimmo relayant un communiqué de l'agence fédérale russe pour la presse et les communications de masse, 21 juin 2018 (https://twitter.com/benimmo/status/1009778691398946816).

15. State Security Department of the Republic of Lithuania, *National Threat Assessment 2018*, p. 41.

Quand les chaînes russes inventent la réalité (Suède, France)

En février 2017, une équipe de la chaîne de télévision russe NTV se rend à Rinkeby, une banlieue de Stockholm, pour couvrir des affrontements avec la police. N'y trouvant pas de quoi dresser le portrait d'un pays au bord de la guerre civile, ils proposent à un groupe d'adolescents 400 couronnes (40 euros) chacun pour jouer les fauteurs de trouble face caméra. Les jeunes refusent et rapportent les faits à un média danois. NTV diffuse son reportage quelques jours plus tard : intitulé « Les migrants ont transformé la banlieue de Stockholm en une zone de danger extrême », il exagère la gravité des affrontements et prétend que les violences ont été déclenchées par une enquête sur un viol, alors que celle-ci portait en réalité sur un crime lié à un trafic de drogue[16]. Le viol et les crimes sexuels en général sont l'une des histoires favorites de la désinformation pro-Kremlin car elles déclenchent davantage les passions tout en témoignant à la fois de l'insécurité, de la décadence morale et de la « barbarisation » de l'Europe.

NTV est coutumière de la mise en scène : dans un reportage de 2016 sur la remilitarisation de l'île de Gotland, la chaîne montrait un fonctionnaire de l'administration territoriale pointant de nombreux endroits sur une carte, pendant que le commentaire affirmait que Gotland avait été au centre de toutes les guerres du XX^e^ siècle. En réalité, l'équipe de tournage avait demandé au fonctionnaire de pointer sur la carte une centaine de réserves naturelles, à aucun moment il n'a été question de questions militaires[17]…

Ces manipulations ne sont pas propres à la Suède. Plusieurs affaires similaires ont été détectées en France : dans un reportage de 2016 sur l'euroscepticisme en France, la chaîne Rossiya 24 interviewe des Français et leur fait tenir en les traduisant en russe un discours qu'ils ne prononcent absolument pas. L'année précédente, la chaîne Rossiya 1 avait également diffusé un reportage en France sur l'islamisation truffé de mensonges – la journaliste parcourant les rues de Paris y affirmait notamment que « pratiquement personne ne parle le français. Au marché, on ne vend que de la viande halal […]. Une femme sur deux porte la burqa ou le niqab. Il ne reste pratiquement pas de non-musulmans dans le quartier ». Elle inventait également des statistiques (« 11 millions de musulmans » en France, près de trois fois plus que le chiffre réel, et affirmait qu'ils sont 40 % dans la capitale et 60 % à Marseille, sans citer ses sources)[18].

16. « Russian TV offers money for staged "action" in Sweden? », EUvsDisinfo, 8 mars 2017.

17. « Naturreservaten blev krigiska när den Gazpromägda ryska TV-kanalen rapporterade om Gotland », helahalsingland.se, 19 juillet 2016.

18. Allyson Jouin-Claude, « Le *Petit Journal* dénonce les manipulations d'une chaîne publique russe », *LeFigaro.fr*, 21 mai 2016.

En avril 2018, l'agence de presse russe RIA FAN a annoncé le lancement prochain d'un nouveau site de « réinformation » à destination du public américain, intitulé « USA Really. Wake Up Americans ». Un communiqué de presse présente le projet de la façon suivante : « En raison de la censure politique croissante imposée par les États-Unis, il reste de moins en moins de sources d'information qui ne sont pas sous le contrôle des autorités américaines. À cet égard, les citoyens américains ne peuvent pas recevoir d'informations objectives et indépendantes sur les événements qui se produisent sur le territoire de l'Amérique et dans le monde[19]. » RIA FAN, qui est basée à Saint-Pétersbourg, est en réalité une émanation de l'usine à trolls bien connue (IRA, voir *infra*) : elles étaient initialement domiciliées à la même adresse, et leur propriétaire reste le même (Evgueni Prigozhine). Le nouveau média est lancé en mai 2018 et produit depuis une quinzaine d'articles par jour. Il est encore trop tôt pour anticiper l'effet qu'aura ce nouveau venu dans l'arsenal informationnel russe.

Même si les mécanismes de diffusion des manipulations de l'information se déploient principalement dans le monde virtuel (voir *infra*), ils ont aussi une dimension bien réelle, s'appuyant, selon les pays, sur des vecteurs d'influence variés, dans la sphère politique, médiatique ou économique, voire culturelle. L'un des tours de force de Moscou est de réussir à faire reprendre ses narratifs par des individus et des groupes qui ne sont pas tous sciemment pro-Kremlin, mais qui ont en commun de professer la méfiance ou le mépris des institutions démocratiques et de défendre des idées qui coïncident avec les intérêts de Moscou, et ce même dans les pays où il n'existe pas de forces politiques conséquentes ouvertement pro-russes.

L'exemple de la Pologne est à cet égard éclairant. Moscou est susceptible d'utiliser indirectement les cercles conservateurs opposés à l'Occident libéral (sur la sexualité, l'avortement, la famille, la religion, etc.) ; ou au contraire les cercles libéraux opposés au PiS (pour cultiver la division interne) ; les panslaves estimant partager une culture régionale dont la Russie serait la championne ; les nationalistes, souvent d'extrême droite et antisémites ; ou tout simplement les eurosceptiques, anti-américains et anti-ukrainiens ; et les conspirationnistes ou amateurs d'idéologies alternatives (parce qu'ils sont plus susceptibles de remettre en cause les vérités établies).

En Suède, des partis aussi divers que les Démocrates suédois et le Mouvement de résistance nordique d'extrême droite ou le Parti de gauche et l'Initiative féministe d'extrême gauche constituent autant de relais

19. « USA Really. Wake Up Americans. The story of Russia's new private propaganda outlet », EUvsDisinfo, 16 avril 2018.

potentiels pour des narratifs anti-OTAN (pour ces deux tendances) ou anti-migrants (pour l'extrême droite). En Finlande, le parti des « Finlandais de base » (ou « Vrais Finlandais »), populiste et eurosceptique, a pris un tournant pro-russe, voyant la Russie comme incarnant désormais les valeurs que le parti défend (nationalisme contre libéralisme/cosmopolitanisme, christianisme, suprématie blanche, etc.).

Le tissu associatif peut également être mis à profit. En Suède, des associations sans lien apparent avec la Russie ont des idées qui coïncident avec les intérêts de Moscou : le Swedish Peace Council, à l'extrême gauche ; ou Swedish Doctors for Human Rights, qui nie la réalité des attaques chimiques en Syrie. On observe par ailleurs que d'autres mouvements alternatifs, par exemple contre la vaccination, sont de plus en plus pro-russes. Enfin, différents centres de recherche et instituts plus ou moins ouvertement liés à la Russie propagent les thèses russes en matière de politique étrangère.

S'agissant de l'économie, dans les États baltes, sont visés les projets d'infrastructures stratégiques susceptibles d'accroître soit l'intégration européenne soit l'indépendance énergétique : le projet de centrale nucléaire à Visaginas en Lituanie (en instrumentalisant l'opposition écologiste), le projet de voie ferroviaire Rail Baltica (présenté comme économiquement non viable et agressif car pouvant servir au transport de troupes de l'OTAN), le projet polonais de canal de la Vistule à la mer Baltique (également critiqué comme écologiquement irresponsable, économiquement non viable et militairement agressif), etc.[20].

B. Des narratifs calibrés

L'objectif du Kremlin n'étant pas de convaincre d'une vérité alternative mais de l'absence de vérité objective, pour semer le doute et la confusion, il n'a pas à défendre une ligne idéologique, et c'est une différence majeure par rapport à l'époque soviétique. Il peut soutenir simultanément des mouvements de droite comme de gauche, pourvu qu'ils s'affrontent, et des narratifs contradictoires, enchaînant les explications les plus farfelues, et mutuellement exclusives, sur le crash du MH17, l'affaire Skripal ou l'attaque chimique de Douma, par exemple.

20. Aleksander Król, « Information Warfare Against Strategic Investments in the Baltic States and Poland », *The Warsaw Institute Review*, mars 2017, p. 62-69.

50 nuances d'affaire Skripal

L'affaire Skripal (du nom de l'ex-espion russe empoisonné au Royaume-Uni en avril 2018) a suscité une intense campagne informationnelle russe. Les autorités britanniques ont identifié environ 2 800 comptes Twitter probablement gérés par des bots, qui auraient atteint 7,5 millions d'utilisateurs[21]. Le site EUvsDinfo (de la *task force* de communication stratégique orientée vers le voisinage oriental de l'Union européenne [voir *infra*]) a fait une chronologie de tous les narratifs diffusés par les médias russes, parmi lesquels : une overdose de Fentanyl, la russophobie, une expérimentation britannique, un coup monté pour justifier les sanctions, une tentative d'influencer les élections russes, un coup monté pour justifier un boycott de la coupe du monde de football en Russie, un coup des Américains, puis de l'Ukraine, puis de la future belle-mère de Yulia Skripal, puis des Britanniques pour détourner l'attention de la pédophilie de masse dans le pays, Skripal trafiquait des armes chimiques, une toxine de l'OTAN, etc. L'Ofcom a annoncé avoir ouvert sept enquêtes concernant RT, soupçonnée d'avoir manqué d'impartialité dans le traitement de l'affaire.

Les narratifs visent prioritairement les États les plus peuplés et les plus influents. Pendant trois ans et demi, l'ONG Ukraine Crisis Media Centre (UCMC) a analysé les journaux télévisés et les émissions les plus populaires de trois chaînes russes (la Première chaîne, NTV et Rossiya 1). Sur les plus de 22 000 mentions négatives des pays européens, la France arrive en tête, concentrant 17 % des attaques, suivie par l'Allemagne et le Royaume-Uni[22].

Les messages sont préparés sur mesure, adaptés à des audiences spécifiques, en fonction non seulement de la région mais aussi du profil socio-professionnel, de l'âge, etc. Les vecteurs sont également adaptés à l'écosystème médiatique de chaque pays. La dimension socio-économique est importante : les études montrent que l'influence russe est facteur de la concentration non seulement de russophones mais aussi de populations paupérisées, car elle se nourrit de la frustration de ces acteurs[23].

Les sujets sont très divers mais des constantes émergent (immigration, islamisation, crime, hégémonie américaine ou otanienne, décadence morale, etc.) et ce n'est pas un hasard : le Kremlin va cibler en priorité les

21. « British officials probe 2 800 Russian bots that "spread confusion" after Salisbury nerve agent attack on former spy », *Daily Mail*, 24 mars 2018.

22. UCMC, *Image of the EU and Eastern Partnership countries on Russian TV*, 2 mars 2018.

23. Aleksander Król, « Russian Information Warfare in the Baltic States – Resources and Aims », *op. cit.*, p. 61.

sujets clivants et qui jouent sur la peur. Une tactique est alors de soutenir, sur ces sujets, les deux camps pour les monter les uns contre les autres : pour et contre les noirs, les gays, les LGBT, les réfugiés, etc.

C'est une tactique pathocentrée qui présume à juste titre que les sujets émotifs rendent beaucoup de personnes moins rationnelles donc plus manipulables. À noter que les sujets ne sortent pas de nulle part, les services russes ne les inventent pas, ils se contentent de souffler sur des braises existantes, et qui contiennent souvent un fond de vérité, ce qui les rend plus crédibles.

Monter les communautés les unes contre les autres : l'exemple des émeutes raciales aux États-Unis (2016)

Au moins 29 comptes Twitter des deux côtés (gauche et droite) de la controverse ont été identifiés comme étant d'origine russe, avec les hashtags #BlackLivesMatter, #BlueLivesMatter, #AllLivesMatter. Le plus connu est sans doute le compte Facebook « Blacktivist », qui avait la photo de Freddie Gray (mort aux mains de la police un an plus tôt), et était « liké » par 360 000 personnes (soit davantage que le compte officiel de Black Lives Matter) : il a largement contribué à mobiliser et exciter le mouvement avec des messages incitant à l'action contre les policiers. Le compte s'est avéré être russe et faire partie du volet racial de l'effort russe visant à diviser les communautés américaines. La leçon qu'en tire la communauté noire en ligne est qu'il faut redoubler de vigilance et vérifier la source, l'identité du titulaire du compte, avant de rediffuser ses messages.

Bien qu'elle soit désormais connue, la technique n'a visiblement pas cessé d'être utilisée : fin juillet 2018, Facebook a démasqué une campagne d'influence impliquant de faux profils dont l'activité consistait à attiser les haines des deux côtés de sujets clivants. En l'occurrence, l'un des comptes avait créé une contre-manifestation à un rassemblement de nationalistes blancs qui devait se tenir à Washington DC en août[24].

Les narratifs soutenus par le Kremlin sont de toutes sortes :

• les complotistes (Douma, Skripal) pour susciter le doute et la défiance ;

• les attaques *ad hominem* pour discréditer une personne ou une fonction (comme la rumeur selon laquelle l'ancien Premier ministre britannique David Cameron aurait fourré son sexe dans une tête de cochon – dont le caractère ridicule n'a pas empêché la propagation, au point que Downing Street a dû publier un communiqué de démenti) ;

24. Nicholas Fandos et Kevin Roose, « Facebook Has Identified Ongoing Political Influence Campaign », *The New York Times*, 31 juillet 2018.

• les « anti » qui s'en prennent à nos institutions (anti-UE, anti-OTAN), nos États (anti-américanisme) et nos valeurs (anti-migrants), avec parfois des synergies (la critique de l'UE est catalysée par celle de la migration dans le concept d'« Eurabia », qui désigne un continent menacé par l'islamisation) ;

• les diviseurs, sur tous les sujets clivants, pour monter des communautés les unes contre les autres, minorités russophones contre majorités locales, progressistes contre conservateurs, gays contre homophobes, etc. ;

• les historiques, qui fouillent les recoins les plus sombres des histoires nationales pour dénicher des vulnérabilités, qui ont souvent un lien, fictif ou avéré, solide ou ténu, avec le nazisme ;

• les moralisateurs, qui entendent montrer la décadence morale de l'Occident (comme l'histoire fausse de l'ouverture à Copenhague en octobre 2017 de « la première maison close zoophile d'Europe »).

L'instrumentalisation de l'histoire : le cas des États baltes

Il y a d'abord une différence d'interprétation fondamentale sur la Seconde Guerre mondiale : la Russie estime avoir libéré les États baltes des nazis (ce que les russophones célèbrent le 9 mai de chaque année), alors que les Baltes estiment avoir été occupés par les Soviétiques (1940-1941), les Allemands (1941-1944) puis à nouveau les Soviétiques (1944-1991) – les musées historiques locaux mettent d'ailleurs les occupations nazie et soviétique sur le même plan, ce que les Russes ont du mal à accepter. Ce différend historique reste très vif : en 2014, la Lettonie a unilatéralement suspendu la commission bilatérale d'historiens (l'annonce de la reprise de ses travaux a eu lieu récemment). Les Russes ont tendance à décrire cette période (d'occupation) soviétique comme avantageuse pour les Baltes et à minorer les crimes commis à leur encontre. On trouve par exemple l'idée d'un déclin économique selon laquelle les États baltes étaient beaucoup plus riches sous l'URSS, formant une « Silicon Valley soviétique », et que leur intégration à l'Ouest aurait fait disparaître leur industrie de pointe.

Le nazisme reste l'un des narratifs les plus utilisés par le Kremlin contre les Baltes (et l'Ukraine). En juillet 2017, l'OTAN a mis en ligne une vidéo honorant les « Frères de la forêt » (*Forest Brothers*), partisans estoniens, lettons et lituaniens ayant lutté contre l'occupant soviétique. La porte-parole du ministère des Affaires étrangères russe a réagi en estimant qu'ils étaient des « fascistes », « collaborateurs » de l'occupant nazi. Le vice-Premier ministre russe a tweeté « Le clip de l'OTAN sur les "Frères de la forêt" tuant nos soldats confirme que, face à l'OTAN, nous avons affaire aux héritiers des restes d'Hitler » et la mission russe à l'OTAN a également dénoncé une « tenta-

tive honteuse de réécrire l'histoire et de glorifier d'anciens combattants SS et nationalistes sans gloire[25] ».
Un autre narratif historique utilisé dans la région est la remise en cause de l'indépendance, présentée comme une erreur, un accident, un piège tendu par l'Ouest ; et l'idée que, tôt ou tard, les États baltes reviendront dans la zone d'influence de la Russie (la Ligue continentale de hockey est d'ailleurs une manière de revigorer les vieux liens soviétiques et de signifier que, dans ce domaine au moins, les Baltes sont restés dans leur zone d'influence).
L'instrumentalisation de l'histoire passe aussi par la pierre : la reconstruction et la valorisation d'objets soviétiques, notamment des tombes de soldats et des monuments aux morts. C'est le cas en Lituanie, où ils servent à la fois de « preuves de l'inclusion de la Lituanie dans l'espace géopolitique russe [et] de points de ralliement pour des soutiens aux politiques du Kremlin[26] ».
Leur réhabilitation terminée peut aussi être l'occasion d'une cérémonie, avec dignitaires locaux, diplomates et couverture médiatique. Certains sites font l'objet d'une véritable concurrence des mémoires : il en est ainsi du mémorial aux victimes du communisme à Tallinn, actuellement en construction sur le site même du mémorial soviétique aux victimes de la grande guerre patriotique, ce qui suscite des débats dans la communauté russophone et des protestations de Moscou. On se souvient par ailleurs de l'affaire du soldat de bronze, dont le déplacement en 2007 du centre de Tallinn vers un cimetière militaire en bordure de la ville avait déclenché des émeutes ainsi qu'une vague de cyberattaques contre des sites estoniens.

C. Des lieux et des mécanismes privilégiés

Les manipulations de l'information tirent leur efficacité du caractère viral de leur diffusion sur internet, par divers relais, automatisés ou non. Mais il ne faut pas s'y tromper : ce caractère viral ne doit rien au hasard. Il est le fruit d'une stratégie pensée, coordonnée et méticuleusement mise en œuvre qui s'appuie sur une chaîne d'acteurs, aboutissant non seulement à la diffusion massive d'informations manipulées, mais aussi à son « blanchiment » par sa reprise par différents acteurs institutionnels ou médiatiques.

1. Les lieux

Le lieu privilégié de la manipulation est la plateforme numérique. Une plateforme est définie comme « un service occupant une fonction

25. Donara Barojan et Ben Nimmo, « History Revisited: The Forest Brothers », DFRLab Medium.com, 18 juillet 2017. Voir aussi « The Nazi-obsession of pro-Kremlin propagandist », EUvsDisinfo, 21 juillet 2017.

26. State Security Department of the Republic of Lithuania, *National Threat Assessment 2018*, p. 44.

d'intermédiaire dans l'accès aux informations, contenus, services ou bien édités ou fournis par des tiers[27] ». À cette définition sont parfois accolées les caractéristiques suivantes : « au-delà de sa seule interface technique, elle [la plateforme] organise et hiérarchise les contenus en vue de leur présentation et leur mise en relation aux utilisateurs finaux[28] ». Ce complément met en lumière une fonction essentielle de ces plateformes qui ne se contentent pas d'éditer, de manière neutre, les contenus diffusés par ses utilisateurs. À travers les algorithmes qu'elles utilisent, les plateformes hiérarchisent et définissent les conditions de diffusion des contenus qui y sont échangés et publiés.

Une atteinte à la défense ou à la sécurité nationale

« Plus insidieusement, les plateformes numériques et notamment les réseaux sociaux peuvent façonner l'opinion et parfois être vecteurs de valeurs qui ne sont pas celles de la République. Dans certains cas, ils peuvent être instrumentalisés à des fins de désinformation et de propagande envers les citoyens français, notamment les plus jeunes. Les opinions diffusées vont alors à l'encontre des intérêts fondamentaux de la France et relèvent d'une atteinte à la défense ou à la sécurité nationale sanctionnée par la loi. »

(*Stratégie nationale pour la sécurité du numérique*, 2015, p. 20.)

Cette fonctionnalité est très souvent euphémisée par les plateformes elles-mêmes, qui préfèrent se considérer comme des « entreprises de technologie » qui hébergent, davantage qu'elles n'éditent, les informations et contenus échangés. La terminologie n'est pas neutre : les responsabilités légales des éditeurs de contenus sont bien plus contraignantes que celles des hébergeurs. Dès lors, la manière même de présenter ces fonctionnalités, déterminantes dans la définition des statuts, constitue un enjeu stratégique pour les plateformes. Ces dernières se sont longtemps présentées comme étant des entreprises de technologie qui hébergeaient, sans pour autant éditer, les informations et les contenus.

Elles ont aujourd'hui, en grande partie sous la pression extérieure, modifié leur position et leur communication à ce sujet. La déclaration de Mark Zuckerberg s'adressant au Congrès américain en avril 2018 illustre

27. Conseil national du numérique, *La Neutralité des plateformes*, juin 2014.
28. *Ibid.*

parfaitement ce changement de posture, notamment lorsqu'il reconnaît que Facebook est responsable du contenu, même s'il ne produit pas ce dernier. Cette déclaration a surpris car elle va à l'encontre de la stratégie déployée par cet acteur ces dernières années. Elle marque un changement de paradigme important : il est désormais temps pour les plateformes de repenser leur statut et par là même redéfinir les termes de leur responsabilité.

Le présent rapport s'intéresse plus particulièrement aux « grandes plateformes numériques », c'est-à-dire Google, Facebook, YouTube, Twitter. Ces dernières bénéficient des effets de réseaux, « ces externalités positives de l'économie d'information[29] » qui leur assurent un grand nombre d'abonnés, avec un fort taux de captivité. Elles sont donc le lieu privilégié des campagnes de manipulation de l'information qui, comme la définition le rappelle, ont un caractère massif et à grande échelle. En cela, d'autres plateformes numériques, plus confidentielles et moins utilisées, ne font pas l'objet, dans ce rapport, d'une attention particulière. Le terme de plateforme numérique est préféré ici à celui de réseau social qui n'épuise ni ne se confond avec les acteurs impliqués dans les campagnes de manipulation de l'information. Par exemple, la fonctionnalité « actualité » de Google ne s'apparente pas à un réseau social. Pour autant, elle joue un rôle majeur dans la diffusion de fausses informations en tant qu'elle peut augmenter ou diminuer la visibilité de ces dernières.

La twittosphère pro-russe en France

Pétiniaud et Limonier utilisent l'analyse des données issues des médias sociaux – notamment Twitter – pour comprendre la stratégie russe en France. Ils montrent que la « russosphère » française « n'est homogène ni du point de vue des profils des personnes qui la composent, ni de celui de leur orientation politique. Il s'agit au contraire d'une galaxie très diversifiée dont une bonne partie pourrait exister sans que la Russie joue un rôle quelconque. On remarque cependant que les comptes "centraux", qu'ils soient ceux de personnalités politiques ou de médias russes, jouent un rôle de mise en relation et en cohérence important[30] ».

29. Renaissance numérique, *Plateformes et dynamiques concurrentielles*, note de décryptage, octobre 2015.

30. Louis Pétiniaud et Kevin Limonier, « Cartographier le cyberespace : le cas des actions informationnelles russes en France », *Les Champs de Mars*, n° 30, vol. 2 (supplément), 2018, p. 321.

Les grandes plateformes numériques ne sont pas les seules à relayer et amplifier les campagnes de manipulation de l'information. Ces dernières impliquent d'autres acteurs dits numériques :

• Des sites d'(de dés)information, comme ceux financés par Moscou (RT, Sputnik) ou ayant des affinités idéologiques avec le Kremlin, et les sites dits clonés (ABCNews.com.co, nytimess.com).

• Des forums de discussion qui ont joué un rôle de tout premier plan dans plusieurs campagnes de manipulation de l'information. C'est notamment sur le site 4Chan que les « Macron Leaks » ont été diffusés pour la première fois et ont suscité l'attention des premiers internautes. Ces derniers ont ensuite rapidement relayé ces mêmes informations volées sur les grandes plateformes (Twitter, Facebook). En cela, les forums de discussion servent très souvent de point de départ de la campagne de manipulation et de propagation de la rumeur. Néanmoins, si les forums de discussion sont susceptibles de relayer les fausses informations, leurs utilisateurs sont le plus souvent conscients de la nature polémique des contenus échangés et de leur potentielle falsification. Le débat se fait très souvent au sein d'un groupe assez réduit d'utilisateurs échangeant leurs opinions dans l'anonymat. Même s'ils peuvent à terme permettre à la fausse nouvelle d'atteindre une visibilité critique et de marquer l'opinion publique, les forums sont avant tout utilisés pour blanchir les fausses informations en leur donnant l'impression d'émaner d'acteurs apparemment sans lien avec la visée politique poursuivie. Il est important de noter que, lors des « Macron Leaks » notamment, certains de ces forums (par exemple jeuxvideo.com) ont censuré les groupes de discussion qui rendaient compte des documents volés, rappelant que cela était susceptible de tomber sous le coup de la loi, notamment pénale.

• Les applications de messagerie de type WhatsApp et Telegram sont également un des vecteurs utilisés pour les campagnes de manipulation de l'information : à quelques reprises, les fausses informations ont en effet été diffusées via des groupes de discussion rassemblant un nombre très important d'abonnés. Le taux d'équipement mobile étant croissant et élevé, les barrières d'entrée très faibles (inscription et acquisition de l'application gratuites), les applications sont en mesure d'atteindre un fort seuil d'exposition tout en bénéficiant d'une absence totale de modération.

• Le Darknet. Les campagnes de manipulation de l'information peuvent impliquer l'utilisation de documents volés. Il arrive que ces derniers

soient mis aux enchères et diffusés sur le Darknet, un réseau qui, parce qu'il échappe aux règles de gouvernance d'internet, est particulièrement propice aux échanges d'informations illégalement acquises.

Les 7 étapes de la propagande en ligne

1. reconnaissance de la cible (recherche sur l'audience),
2. armement (préparation des narratifs et fausses nouvelles, création des histoires pour les crédibiliser et des versions alternatives à décliner selon les audiences),
3. diffusion large (par tous les moyens disponibles, médias sociaux et traditionnels),
4. activation de relais spécifiques (groupes militants sur les réseaux sociaux),
5. croissance (achat de publicités, bots, trolls),
6. maintien (en faisant varier les histoires, en répondant aux objections),
7. blanchiment (disparition des traces une fois l'objectif atteint, diversion de l'attention et suppression des posts voire des comptes).

2. Les mécanismes d'amplification

Les manipulations de l'information sont amplifiées par deux mécanismes principaux.

a. Les bots

Premièrement, les acteurs automatisés ou semi-automatisés, bots et netbots. Il s'agit de faux comptes Twitter ou Facebook permettant d'assurer une diffusion rapide des fausses informations, par le biais de retweets/likes. Par « faux comptes », on désigne soit des comptes tenus par des personnes qui prétendent être quelqu'un d'autre, soit non tenus par des personnes et qui sont automatiques (bots). Les faux comptes « sont les fantassins dans cette forme de guerre[31] ». Ils servent à amplifier les messages, introduire des hashtags, intimider ou bloquer d'autres utilisateurs.

Ces bots sont très actifs et très présents sur les réseaux sociaux : à titre d'exemple, les bots russophones sont responsables de 70 % des messages

31. Ben Nimmo, pour son audition devant le parlement singapourien (Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures, written representation 36, 22 février 2018).

postés en russe sur l'OTAN au second semestre 2017[32]. Dans le cas du référendum irlandais, il est aussi estimé que 14 % des 165 323 tweets #Savethe8th, le hashtag anti-avortement, provenaient de comptes à pseudonymes numériques et 6 % des tweets, de comptes à chiffres sans aucune localisation[33].

Si les bots jouent souvent un rôle non négligeable dans l'amplification des opérations, ce n'est pas toujours le cas : chaque campagne est différente et, dans certaines circonstances, l'attaquant préférera s'appuyer sur des relais humains. Durant la campagne de l'élection présidentielle colombienne de 2018, par exemple, l'amplification était essentiellement humaine, provenant de politiciens ou de soutiens connus des deux camps[34].

b. Les trolls

Deuxièmement, les trolls, qui sont des individus réels qui relaient, saturent certains sites de commentaires, et/ou harcèlent. Cette activité est en partie institutionnalisée, mais elle est aussi exercée de façon autonome par des individus de toute nationalité. Moscou a commencé à développer des « usines à trolls » en réaction aux manifestations de l'hiver 2011-2012, qui étaient organisées sur les réseaux sociaux (principalement VKontakte et LiveJournal) : un grand nombre de soutiens au président sont alors apparus subitement sur ces réseaux, pour créer des polémiques, semer la discorde et finalement affaiblir les communautés contestataires. Dès 2012, les médias internationaux mettaient en évidence le rôle du mouvement des Nachi, jeunes nationalistes soutenant le président Poutine, dans des actions de *trolling* et de piratage[35]. Les premières mentions d'une « usine à trolls » datent de 2013 (voir encadré ci-contre).

32. NATO StratCom CoE, *Robotrolling*, février 2017.

33. Rachel Lavin et Roland Adorjani, « L'Irlande a déjà trouvé la parade aux *fake news* (mais on ne pourra pas la reproduire) », *Slate*, 13 juin 2018.

34. Jose Luis Peñarredonda, « #ElectionWatch: Everyday Misinformation in Colombia: Humans, not bots, were the main vectors of misinformation », @DFRLab, Medium.com, 20 juillet 2018.

35. Miriam Elder, « Polishing Putin: hacked emails suggest dirty tricks by Russian youth groups », *The Guardian*, 7 février 2012.

IRA, l'usine à trolls de Saint-Pétersbourg

L'Internet Research Agency (IRA) est une entreprise russe localisée à Saint-Pétersbourg, en réalité une « usine à trolls » financée par le Kremlin, dont l'existence a été révélée dès 2013, d'abord par des journalistes russes se faisant passer pour des candidats à un poste[36]. La presse régionale, notamment finlandaise et polonaise, s'est ensuite emparée du sujet[37], puis la presse internationale[38], le renseignement américain[39], et enfin le procureur spécial Robert Mueller, qui dans le cadre de son enquête sur l'ingérence russe a, en février 2018, inculpé l'IRA et les deux entreprises détenues par Evgueni Prigozhine qui l'ont créée (Concord Catering et Concord Management and Consulting), ainsi que 13 individus dont Prigozhine lui-même.

L'IRA est notamment accusée d'avoir mené une opération d'influence durant la campagne électorale américaine. Enregistrée en juillet 2013, elle aurait commencé à viser les États-Unis autour du mois d'avril 2014 et recevait ses fonds (1,25 million de dollars par mois pendant la campagne) via 14 compagnies affiliées à Concord. En 2015, des centaines de jeunes Russes y étaient employés, travaillant 12 heures par jour de façon très compartimentée : des blogueurs écrivant des billets, des rédacteurs de nouvelles faisant référence aux billets en question, des trolls faisant des commentaires et des communicants pour diffuser l'ensemble sur les réseaux sociaux[40]. Ils étaient formés aux positions du Kremlin sur tous les débats dans lesquels ils intervenaient et un « bureau étranger » les briefait sur l'état du débat américain sur les sujets clivants qu'il s'agissait d'exacerber (racisme, armes à feu, immigration, LGBT, impôts, etc.).

Par le biais de faux comptes et de bots, quelques dizaines de personnes ont ainsi pu en atteindre 150 millions via Facebook et Instagram. À elle seule, l'IRA contrôlait, sur Twitter, 3 814 comptes humains et 50 258 bots, avec lesquels 1,4 million d'Américains ont interagi et au moins 470 comptes Facebook (avec 100 000 dollars dépensés en publicité) ayant atteint au moins 126 millions d'Américains.

L'acte d'accusation du procureur spécial américain donne des informations détaillées sur le fonctionnement de l'agence, mais n'accuse pas le gouvernement russe, ni ne reconnaît que l'IRA a réussi à influencer le vote.

36. Les premières révélations datent d'août-septembre 2013. Voir Ben Nimmo et Aric Toler, « The Russians Who Exposed Russia's Trolls: A tribute to the Russian journalists who exposed the "troll factory" », DFRLab Medium.com, 7 mars 2018.

37. Jessikka Aro, « The Cyberspace War: Propaganda and Trolling as Warfare Tools », *European View*, 10 mai 2016.

38. Shaun Walker, « "Salutin" Putin : Inside a Russian Troll House », *The Guardian*, 2 avril 2015 ; Adrian Chen, « The Agency », *The New York Times*, 2 juin 2015.

39. Office of the Director of National Intelligence (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections*, Washington DC, janvier 2017.

40. Ben Popken & Kelly Cobiella, « Russian Troll Describes Work in the Infamous Misinformation Factory », *NBC News*, 16 novembre 2017.

L'attention internationale dont l'IRA fait l'objet depuis plusieurs années semble ne pas gêner le Kremlin. En 2017, l'agence a même déménagé pour s'agrandir, passant de 4 000 à 12 000 m² de bureaux[41]. En devenant la vitrine d'un phénomène, elle détourne l'attention des autres usines à trolls, présentes ailleurs sur le territoire russe, voire à l'étranger. L'IRA n'est pas un cas isolé, et ne doit pas devenir l'arbre qui cache la forêt.

Ces mécanismes ont joué à plein au moment de la campagne présidentielle américaine de 2016. Dès 2015, des trolls et des bots d'origine russe ont exacerbé les tensions raciales (#BaltimoreVsRacism, #FergusonRemembers), la peur du djihadisme (#TexasJihad, #ISISinGarland), le débat sur les armes à feu (#NoGunsForCriminals, #GunViolenceOregon), l'homophobie (#IndianaFedUp), etc., et ont commencé à s'attaquer à Hillary Clinton. C'est au cours de l'année 2016 qu'a eu lieu la principale opération coordonnée, faite de cyberattaques et de manipulations informationnelles, contre Hillary Clinton et en faveur de Donald Trump[42].

Les trolls ne servent pas uniquement de relais : ils ont aussi des fonctions plus actives et agressives. Le *trolling* procède généralement en trois étapes, inspirées de la pêche[43] : appâter, faire mordre à l'hameçon et ferrer la prise. D'abord, le troll poste un message polémique pour faire réagir. Si personne ne s'y oppose, il peut le faire lui-même en se faisant passer pour une tierce personne qui soit réfute, soit au contraire soutient de manière tellement exagérée que cela peut aussi faire réagir. Lorsqu'un internaute a « mordu » à l'hameçon en s'engageant dans la discussion, il le ferre en s'y opposant systématiquement pour faire durer la « discussion » quitte pour cela à varier les personnages et les tons, de l'insulte à l'ironie.

Il existe plusieurs sortes de trolls. Une étude du centre d'excellence de l'OTAN pour la communication stratégique en a distingué cinq types[44] : des trolls conspirationnistes (qui voient la main américaine partout) pour susciter de la défiance, des « trolls bikinis » (se présentant sous la photo d'une jeune femme séduisante) pour attirer l'attention, des « trolls agressifs » pour intimider et dissuader les gens de participer à certaines activités ou discussions, des « trolls Wikipedia » qui éditent le contenu des pages et des « trolls lieurs » qui postent des liens vers un contenu pro-russe.

41. « Figure of the Week: 12,000 », EUvsDisinfo, 9 janvier 2008.

42. Pour une étude de l'ingérence russe dans la campagne américaine, voir Boris Toucas, *« L'Affaire russe » : la démocratie américaine ébranlée*, Notes de l'IFRI, Potomac Papers, n° 32, décembre 2017.

43. Robert Szwed, *Framing of the Ukraine-Russia Conflict in Online and Social Media*, NATO Strategic Communications Centre of Excellence, mai 2016.

44. *Internet Trolling as a tool of hybrid warfare: the case of Latvia. Results of the study*, NATO Strategic Communications Centre of Excellence, 2016.

Parmi eux, les trolls agressifs, qui procèdent par intimidation, brutalité, voire harcèlement, sont le moyen le plus direct de saturer le débat et de faire taire toute voix divergente. Plusieurs journalistes d'investigation ou personnalités, qui se sont opposés aux intérêts russes, en ont été victimes. C'est notamment le cas de la journaliste finlandaise Jessikka Aro, qui dissèque les techniques d'intimidation utilisées par les trolls[45]. Les journalistes étant particulièrement visés, Reporters sans frontières (RSF) y a consacré un rapport dédié[46].

Pour jeter le discrédit sur une personne, les trolls l'accusent souvent de collusion avec un service de renseignement étranger et/ou de trahison. Pour la faire craquer, ils utilisent l'insulte, l'humiliation et la menace (de viol, de mort), à une fréquence élevée (parfois des dizaines de messages par heure). Les illustrations (dessins et mèmes) peuvent jouer un rôle[47].

La spirale du silence est un constat bien connu des régimes autoritaires : les internautes ont tendance à ne pas oser exposer leur point de vue s'il s'oppose à l'opinion dominante sur un forum. Ainsi quelques trolls peuvent, en postant un très grand nombre de commentaires, donner l'impression d'une opinion majoritaire quand bien même elle ne le serait pas du tout – ayant ainsi un effet paralysant sur les autres. Cette technique qui consiste à donner une apparence de popularité, en faisant croire à un authentique mouvement social citoyen (*grassroot movement*), est appelée l'*astroturfing*, en référence à une marque (AstroTurf) de pelouse artificielle.

Les trolls participent ainsi au phénomène plus large de brutalisation du débat public en ligne « qui désigne à la fois la banalisation du recours à la violence expressive et la radicalisation des opinions qu'elle engendre[48] ». Certains chercheurs sont passés maîtres dans l'étude des trolls. C'est notamment le cas de Ben Nimmo, de l'Atlantic Council, qui dévoile régulièrement des réseaux de trolls et détaille leur fonctionnement[49]. Ces analyses sont extrêmement utiles pour les détecter et, *in fine*, les contrer.

45. J. Aro, « The Cyberspace War: Propaganda and Trolling as Warfare Tools », *European View*, 10 mai 2016.

46. RSF, *Online Harassment of Journalists: Attack of the trolls*, 2018.

47. Carly Nyst et Nick Monaco, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, *op. cit.*, p. 13.

48. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 65.

49. Voir par exemple Ben Nimmo, « #TrollTracker : From Tags To Trolling : How tweets to a small group precede attacks on critics of the Syrian and Russian regimes », @DFRLab, Medium.com, 27 juin 2018 et « #TrollTracker: Russia's Other Troll Team: Mueller points to existence of second Russian troll operation focused on activist groups and foreign policy », @DFRLab, Medium.com, 2 août 2018.

D. Les fuites massives de données (*leaks*)

Le phénomène est ancien (Pentagon Papers 1971, Watergate 1972-74) et s'accélère depuis quelques années – une quarantaine de cas ont été recensés entre 2006 et 2017[50] (dont les plus connus sont les télégrammes diplomatiques américains sur WikiLeaks 2010, Offshore Leaks 2013, LuxLeaks 2014, SwissLeaks 2015, Panama Papers 2016, Paradise Papers 2017, Football Leaks 2016). Initialement le fait de « lanceurs d'alerte », prétendument motivés par la transparence (tout en restant anonymes), ce procédé est de plus en plus utilisé pour servir des intérêts politiques ou économiques. C'est dans ce cadre qu'il peut s'inscrire dans des campagnes de manipulation de l'information, comme l'ont montré les élections présidentielles américaine (DNC Leaks, 2016) et française (Macron Leaks, 2017). La fuite de données volées est alors utilisée pour discréditer une cible, qui peut être soit la victime du piratage, soit une tierce partie.

Son avantage est de donner l'impression à la population qu'elle a accès à « la vérité », à une information brute, non filtrée, car faite de données interceptées (conversations, emails, documents). Si c'est parfois le cas, il se peut aussi que ces documents soient manipulés entre le moment où ils sont obtenus et celui où ils sont diffusés, comme c'était le cas dans les « Macron Leaks » (voir *infra*). On parle alors de « fuite contaminée » (*tainted leak*)[51]. Elle est d'autant plus difficile à détecter que la modification est subtile et crédible, et que les fichiers altérés sont entourés de documents authentiques. Les journalistes auront beaucoup de mal à contrôler la véracité des documents dans la mesure où ils n'ont généralement pas accès à la source. Les plus sérieux, qui couvrent ce genre d'événement avec la plus extrême prudence, traitant de la fuite autant que de son contenu, restent toutefois minoritaires : la plupart des relais diffusent sans filtre.

E. La falsification de documents

L'un des moyens les plus courants – et néanmoins grossier, relativement facile à détecter – est la falsification de documents :

- des images (qu'il n'est pas même nécessaire de retoucher lorsqu'il suffit de falsifier leur légende, c'est-à-dire de les faire passer pour ce qu'elles ne sont pas : en novembre 2017, sur les réseaux sociaux, le

50. Pierre Gastineau et Philippe Vasset, *Armes de déstabilisation massive. Enquête sur le business des fuites de données*, Fayard, 2017.

51. Adam Hulcoop *et al.*, « Tainted Leaks: Disinformation and Phishing With a Russian Nexus », *The Citizen Lab*, 25 mai 2017.

ministère russe de la Défense a présenté une image soi-disant prise à la frontière irako-syrienne comme une « preuve irréfutable » du soutien américain à Daech alors qu'il s'agissait en réalité d'une capture d'écran d'un jeu vidéo[52] ; en Suède, plusieurs cas sont fameux, comme l'image d'une voiture en feu pour illustrer la montée de la criminalité supposément causée par les migrants alors qu'elle a été prise à Sofia, ou encore celle d'un jeune garçon blond blessé prétendument par des migrants « parce que ses yeux sont bleus » alors qu'il s'agit en réalité d'une petite fille galloise attaquée par son chien en 2008, etc.) ;

• d'articles de journaux respectés (en Suède encore[53], en mai 2016, un faux article de *Dagens Nyheter*, le plus grand quotidien du pays, sur l'ancien ministre des Affaires étrangères Carl Bildt ; en France, en mars 2017, en pleine campagne présidentielle, un faux article du journal belge *Le Soir* affirmant qu'Emmanuel Macron était le candidat préféré de l'Arabie saoudite – dans tous les cas la technique est la même : il s'agit d'utiliser une marque médiatique traditionnelle pour crédibiliser une rumeur ;

• de sites internet (en Finlande, Johan Bäckman s'est notamment illustré en créant un faux site du centre d'excellence de lutte contre les menaces hybrides, tellement crédible que certains des ambassadeurs conviés à l'ouverture se sont trompés d'adresse).

Lorsque la falsification implique du texte, ce qui n'est généralement pas le cas des images – sauf pour les mèmes, qui sont très populaires –, la qualité de la langue peut être un moyen utile de détecter la contrefaçon car les manipulateurs emploient généralement des traducteurs automatiques du type Google translate. Ceci dit, à mesure que ces outils se perfectionnent, cette détection se réduit (voir *infra* la partie sur les défis futurs).

F. Les ingérences électorales

Les ingérences électorales peuvent viser les systèmes (vote électronique, listes électorales), avec comme conséquence d'affecter la confiance des citoyens dans le dispositif, ou les électeurs, avec l'objectif d'influencer leur vote.

52. Eliot Higgins, « The Russian Ministry of Defence Publishes Screenshots of Computer Games as Evidence of US Collusion with ISIS », Bellingcat, 14 novembre 2017.

53. La falsification de documents, image et texte, est apparemment une méthode préférentielle contre les Suédois : Martin Kragh et Sebastian Åsberg ont identifié 26 faux entre 2015 et juillet 2016 (« Russia's strategy for influence through public diplomacy and active measures: the Swedish case », *Journal of Strategic Studies*, 2017).

Après avoir étudié des dizaines de cas d'interférences dans des processus démocratiques avec des moyens cyber dans près de 40 pays sur 5 continents dans les 10 dernières années, le Centre de sécurité des télécommunications (CST) du Canada conclut que les trois quarts des activités employaient des méthodes sophistiquées (c'est-à-dire étaient d'origine probablement étatiques) à des fins stratégiques, et seulement un quart employait des méthodes moins sophistiquées à des fins criminelles (vol de renseignements sur les électeurs, probablement pour la revente). « On constate une hausse inquiétante des cybermenaces contre les processus démocratiques[54]. » Cette hausse est expliquée par une combinaison de facteurs : la démocratisation des cybercapacités, qui sont de plus en plus accessibles au plus grand nombre ; une faible capacité d'attribution (seulement 20 % des incidents sont attribués), de prévention et de punition (la plupart des incidents restent impunis) ; la croissance exponentielle des médias sociaux ; le fait que davantage d'organismes électoraux utilisent des processus en ligne, qui sont par définition plus vulnérables ; et enfin le fait que certains succès incitent davantage d'attaquants (par émulation ou imitation).

Les processus démocratiques ont de multiples vulnérabilités. Premièrement, les élections, à commencer par l'inscription des électeurs. Si celle-ci se fait en ligne, les adversaires peuvent modifier la base de données (y glisser de faux fichiers d'électeurs), la rendre inaccessible (en chiffrant les données par exemple), l'effacer ou la voler (pour revendre ou utiliser les renseignements personnels). Les conséquences *a minima* sont de ralentir le processus et d'amener les électeurs à douter de son intégrité. Ensuite, le vote en ligne est bien entendu le plus vulnérable, puisqu'il est alors possible d'attaquer le site ou de remplir les urnes virtuelles. Le vote manuel n'est pas non plus invulnérable, si l'on utilise des machines de comptage qui ne sont généralement pas connectées mais qui pourraient être modifiées avant le scrutin pour fausser le comptage ou effacer les données. Par ailleurs, diffuser les résultats par internet les rend vulnérables à l'interception et la modification par un tiers. Si la diffusion des résultats est affectée, les conséquences peuvent être graves (retards importants, réduction de la confiance de la population envers le processus électoral, voire remise en cause des résultats). Enfin, durant l'ensemble du processus, l'attaquant peut aussi viser les infrastructures critiques nécessaires à l'organisation des élections, comme le réseau électrique.

54. CST, *Cybermenaces contre le processus démocratique du Canada*, Ottawa, juin 2017, p. 32.

Deuxièmement, les partis et les hommes politiques. Là aussi, les menaces sont diverses. Les bases de données des partis contiennent de nombreux renseignements personnels sur des millions de personnes. Elles sont donc des cibles de choix pour des raisons autant commerciales (la revente sur le Darknet) que stratégiques, pour nuire au parti (en les supprimant, les modifiant, les chiffrant pour les rendre inaccessibles) ou à des individus ciblés (en utilisant les informations recueillies pour les discréditer, les embarrasser ou les contraindre). Par ailleurs, la présence d'un candidat sur internet (son site, ses pages sur les réseaux sociaux) peut également être ciblée (pages supprimées, bloquées, défacées). L'ensemble des risques au moins réputationnels, voire dans certains cas physiques, associés à une course électorale peut convaincre certains candidats de renoncer. Il y a également un risque de collusion, c'est-à-dire de soutien clandestin, financier ou logistique, par une puissance étrangère, à certains individus pour tenter d'influencer la campagne et l'issue du vote. C'est ce qu'illustre l'enquête du procureur spécial américain dans ce qu'il est convenu d'appeler « l'affaire russe ».

Troisièmement, les médias. C'est la partie qui a directement trait aux manipulations de l'information, en particulier sur les réseaux sociaux (voir *supra*).

Les référendums se prêtent tout particulièrement aux manipulations de l'électorat pour plusieurs raisons : ils portent en général sur des sujets polémiques et clivants, prompts à susciter des passions ; les conséquences de leurs résultats sont complexes et parfois difficiles à évaluer même lorsque les choix proposés, en général binaires, paraissent simples (indépendance/non-indépendance, sortie de l'UE/maintien dans l'UE).

Après que le référendum sur l'indépendance de l'Écosse de 2014 a montré qu'une majorité (55 %) souhaitait rester dans le Royaume-Uni, les médias russes ont tenté de discréditer le résultat, qui ne leur convenait pas, ont fait intervenir des « experts » pour expliquer que le vote ne respectait pas les standards internationaux, et ont encouragé une pétition qui a réuni plus de 100 000 signatures pour demander un nouveau vote, en vain[55]. Les référendums de 2016 sur l'approbation de l'accord d'association entre l'Ukraine et l'UE aux Pays-Bas puis sur l'appartenance du Royaume-Uni à l'Union européenne, ont été l'occasion d'autres manipulations de l'information importantes.

55. Ben Nimmo interviewé dans Severin Carrell, « Russian cyber-activists "tried to discredit Scottish independence vote" », *The Guardian*, 13 décembre 2017.

Les cinq étapes de l'ingérence électorale

En comparant les ingérences dans les élections américaine, française et allemande en 2016-2017, le chercheur finlandais Mika Aaltola a produit un modèle d'ingérence électorale en cinq étapes[56] :
1 - « Utiliser la désinformation pour amplifier les soupçons et les divisions » : accentuer la polarisation politique, les tensions, etc.
2 - « Voler des données sensibles et fuitables ».
3 - « Fuiter les données volées via des "hacktivists" présumés » ou des lanceurs d'alerte. C'est la diffusion des données, plus que le vol en soi, qui procure un effet sur la population, à condition de savoir où, c'est-à-dire à qui, et quand exactement les diffuser. Ces deux critères (ciblage et *timing*) sont capitaux.
4 - « Blanchir les données volées via des médias *mainstream* ». Boris Toucas souligne le rôle des tiers de type lanceurs d'alerte, qui utilisent leur « crédibilité critique » pour faire passer l'information manipulée dans les médias *mainstream* où elle se développe[57]. Le premier d'entre eux, WikiLeaks, est relativement discrédité depuis les élections américaines[58] mais reste populaire auprès d'une certaine population et a un grand nombre de suiveurs.
5 - « Collusion secrète » : liens entre un État étranger et un parti, un candidat, etc.
L'ingérence dans l'élection américaine, qui sert de modèle à l'auteur, est passée par les cinq étapes. Celle dans l'élection française n'a pas été au-delà de la troisième puisque les médias traditionnels n'ont pas suivi (voir *infra*), tandis que l'ingérence dans l'élection allemande n'a pas dépassé la deuxième étape.

56. Mika Aaltola, *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Aurocratic Meddling*, FIIA Briefing Paper, n° 226, novembre 2017.

57. Boris Toucas, « Exploring the Information-Laundering Ecosystem: The Russian Case », CSIS Commentary, 31 août 2017.

58. Julian Assange n'a pas dissimulé son soutien au candidat Donald Trump et WikiLeaks a relayé un certain nombre de fausses nouvelles hostiles à Hillary Clinton (notamment le fameux Pizzagate). Se rapprochant ainsi de l'*alt-right* américaine, et devenant l'allié objectif du Kremlin, WikiLeaks a déçu bon nombre de ses soutiens initiaux. Voir notamment Kevin Poulsen, « Defector: WikiLeaks "Will Lie to Your Face" », *The Daily Beast*, 8 mai 2018.

Les élections américaines de mi-mandat de 2018

L'élection présidentielle américaine de 2016 a été marquée par le piratage des serveurs du parti démocrate et la diffusion de milliers de documents sur WikiLeaks (*DNC Leaks*), entre autres mesures relevant d'une campagne de manipulation organisée. L'enquête menée par le procureur spécial Robert Mueller depuis mai 2017 a mis en évidence le rôle de la Russie dans ce qui semble donc être une ingérence. Les plateformes numériques ont également mis au jour et suspendu des milliers de comptes qui auraient été créés et contrôlés par Moscou, notamment via l'IRA (voir *supra*). Dans ce contexte qui connaît encore chaque jour son lot de révélations sur l'étendue de l'opération de 2016, les autorités américaines sont particulièrement soucieuses d'éviter toute répétition lors des élections de mi-mandat qui auront lieu le 6 novembre 2018.

Reflétant l'inquiétude de la communauté américaine du renseignement, Dan Coats, le directeur du renseignement national, estimait déjà en février 2018 que « les élections de mi-mandat de 2018 constituent une cible potentielle pour les opérations d'influence russes[59] ». Fin juillet, Facebook confirmait ses craintes en annonçant avoir découvert et neutralisé un réseau d'une trentaine de comptes et faux profils Facebook et Instagram préparant une action « coordonnée » tout à fait similaire à ce que faisait l'IRA[60].

La réaction des autorités est toutefois handicapée par un manque d'unité politique, entre Démocrates et Républicains ; un manque de coordination des nombreuses structures administratives consacrées à la lutte contre les manipulations de l'information (département d'État, département de la Justice, département de la Sécurité intérieure), services de renseignement, etc., voir *infra*) ; et une réticence à partager des informations avec le secteur privé. La première réunion entre les agences de l'État et les plateformes numériques en vue des élections n'a eu lieu que six mois avant l'échéance, fin mai, au siège social de Facebook[61], et à la demande des compagnies privées, pas du gouvernement. Plusieurs voix s'élèvent pour souligner l'importance de cette coopération public-privé et la nécessité de partager des informations avec les plateformes si l'on attend d'elles qu'elles luttent efficacement contre ces menaces[62].

59. Daniel R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, Statement for the record, 13 février 2018.

60. Nicholas Fandos et Kevin Roose, « Facebook Has Identified Ongoing Political Influence Campaign », *The New York Times*, 31 juillet 2018.

61. Sheera Frenkel et Matthew Rosenberg, « Top Tech Companies Met With Intelligence Officials to Discuss Midterms », *The New York Times*, 25 juin 2018.

62. Joshua A. Geltzer et Dipayan Ghosh, « How Washington Can Prevent Midterm Election Interference », *Foreign Affairs*, 25 juillet 2018.

Durant la crise qui a agité l'Espagne en septembre-octobre 2017 autour du référendum d'autodétermination de la Catalogne, il semblerait que le Kremlin ait une nouvelle fois soufflé sur les braises. La Catalogne en soi n'a jamais été et n'est toujours pas un enjeu pour Moscou, qui fait simplement preuve d'opportunisme en saisissant chaque occasion de diviser donc d'affaiblir les pays européens.

Les médias russes, RT et Sputnik en tête, ont fait une couverture complaisante et sensationnaliste du mouvement catalan, véhiculant toutes sortes de fausses nouvelles (« La Catalogne reconnaîtra la Crimée comme étant russe », « En Catalogne, l'espagnol est étudié comme langue étrangère », « Des fonctionnaires européens ont soutenu la violence en Catalogne », etc.), faisant croire que les îles Baléares demandaient à leur tour l'indépendance, publiant de fausses cartes des soutiens en Europe (où le Royaume-Uni, les pays scandinaves et les États baltes apparaissent comme des soutiens de l'indépendance catalane, ce qui est faux), faisant le parallèle avec l'Ukraine (la Catalogne serait le Donbass de l'Europe, l'Espagne ferait « les mêmes erreurs » que l'Ukraine) ou même avec le Kosovo, dans un article sobrement intitulé « Pourquoi l'OTAN ne bombarde-t-elle pas Madrid durant 78 jours ? »[63].

Les versions hispanophones de RT et Sputnik sont relativement influentes car largement portées par l'Amérique latine, en particulier le Venezuela et les mouvements chavistes, qui dans la crise catalane ont effectivement servi de relais à Moscou. C'est ce que confirme une étude portant sur plus de 5 millions de messages postés sur les réseaux sociaux, qui montre que la majorité des comptes les plus actifs rediffusant le contenu de RT et Sputnik étaient des comptes chavistes ou vénézueliens (32 %), suivis par des comptes anonymes (30 %) et faux ou automatisés (25 %). La géolocalisation confirme que le Venezuela est la deuxième origine des messages après l'Espagne[64].

Des personnalités du monde numérique telles que Julian Assange et Edward Snowden se sont soudainement passionnées pour la question catalane. WikiLeaks a été jusqu'à demander à *El País* de licencier David Alandete, qui enquêtait sur l'ingérence russe.

63. De nombreux autres exemples figurent dans la base de données de EUvsDisinfo et dans le rapport de The Integrity Initiative, *Framing Russian meddling in the Catalan question*, octobre 2017.

64. David Alandete, « Russian network used Venezuelan accounts to deepen Catalan crisis », *El País*, 11 novembre 2017.

III. D'autres terrains des manipulations de l'information

Si l'espace post-soviétique, l'Europe et l'Amérique du Nord ont pour l'instant concentré l'essentiel des cas de manipulation de l'information, d'autres terrains de préoccupation émergent, notamment au Moyen-Orient, en Afrique et en Amérique latine. Plusieurs facteurs augmentent la vulnérabilité à ces manipulations, dont la présence d'un conflit et/ou d'un gouvernement autoritaire, donc l'absence d'information fiable et crédible, et la peur et l'émotion, qu'elles proviennent de ces causes structurelles ou d'un événement ponctuel tel qu'une attaque terroriste ou une catastrophe naturelle. Les transitions démocratiques et les élections offrent également un terreau favorable, comme la rapide croissance de la connectivité, en particulier dans les zones rurales où la population est moins éduquée et a donc davantage tendance à croire les rumeurs en ligne.

A. Le Moyen-Orient

1. Syrie

Les opérations informationnelles russes s'étendent au Moyen-Orient. Le cas de la Syrie est le plus connu, il n'est pas le seul. On a d'ailleurs vu apparaître en janvier 2016 le site « South Front : Analysis & Intelligence » (southfront.org), qui se présente comme le produit d'une « équipe d'experts et de bénévoles de tous les coins du monde », mais qui « ressemble davantage à un projet professionnel d'infoguerre conduit ou soutenu par les militaires russes »[65].

Depuis 2013, les Casques blancs, une ONG syrienne assurant dans les zones tenues par l'opposition des missions de protection civile, ont été la cible privilégiée d'une campagne massive, systématique et coordonnée de manipulation de l'information[66]. Cette campagne n'a eu de cesse de diffuser au cours des cinq dernières années deux messages principaux : d'une part, l'organisation collaborerait étroitement avec la franchise syrienne d'Al-Qaïda et pourrait donc être qualifiée de terroriste. D'autre part, l'organisation serait responsable de plusieurs « fausses attaques chimiques » (*false flags*) visant à incriminer Damas et à provoquer des frappes occidentales. Ces accusations ont été portées à cinq reprises contre les Casques blancs depuis 2013.

65. Jessikka Aro, « The Cyberspace War: Propaganda and Trolling as Warfare Tools », *European View*, 10 mai 2016, p. 126.

66. Olivia Solon, « How Syria's White Helmets Became Victims of an Online Propaganda Machine », *The Guardian*, 18 décembre 2017.

L'écosystème médiatique derrière cette campagne de désinformation associe des médias iraniens, russes et pro-Assad, avec des échos importants sur d'autres continents, notamment en Amérique latine via TeleSur et les réseaux anti-impérialistes[67]. L'alliance stratégique de ces acteurs en Syrie se double donc d'un front uni et coordonné sur les réseaux sociaux[68].

Cette opération de diffamation systématique permet d'atteindre simultanément plusieurs objectifs stratégiques : 1) Accréditer la thèse défendue par le régime et ses alliés suivant laquelle il n'y aurait, en Syrie, d'autre choix que Bachar el-Assad ou les djihadistes, et pas d'alternative possible issue de la société civile. 2) Discréditer une source d'information de terrain sur la situation humanitaire et les exactions du régime et de ses alliés. À terme, toute initiative contre l'impunité en Syrie s'appuyant sur le témoignage des Casques blancs pourrait ainsi être récusée. 3) Accuser les Casques blancs de mettre en scène de fausses attaques chimiques permet de créer un doute sur l'imputation de telles attaques au régime syrien.

L'attaque chimique de Douma du 7 avril 2018, qui a suscité l'indignation de la communauté internationale et des frappes américaines, françaises et britanniques une semaine plus tard, a donné lieu à la publication dans les médias russes d'une grande diversité de fausses nouvelles, avec un narratif allant de la négation pure et simple (il n'y a pas eu d'attaque chimique, il n'y a pas eu de patients dans les hôpitaux, les photos et les témoignages sont des faux) à la théorie du complot (c'est un coup monté par les Casques blancs, les Occidentaux ou les Britanniques pour détourner l'attention de l'affaire Skripal) en passant par la défense du régime (« tout le monde sait » que la Syrie n'a pas d'arme chimique) et le point Godwin (les Occidentaux utilisent en Syrie les méthodes de la propagande nazie).

Cette campagne de manipulation de l'information est un élément de la stratégie combinée de la Russie, de l'Iran et des réseaux pro-régime syrien visant à discréditer toute forme d'opposition et d'organisation de l'impunité pour les crimes de guerre commis en Syrie. Elle met aussi en évidence le fait que des ONG peuvent être des cibles, ce que l'on observe également ailleurs dans le monde (fondations musulmanes aux États-Unis, ONG d'assistance aux réfugiés en Europe, etc.)[69].

67. « Los Cascos Blancos, artistas del montaje », TeleSur, 17 avril 2018.

68. Donara Barojan, « #SyriaHoax, Part Two: Kremlin Targets White Helmets », DFRLab Medium.com, 20 février 2018.

69. Sarah Oh et Travis L. Adkins, *Disinformation Toolkit*, InterAction, juin 2018.

2. Golfe

D'autres États ont pu se livrer à des manipulations de l'information vers l'étranger, c'est-à-dire à des ingérences informationnelles. Dans la nuit du 23 au 24 mai 2017, la veille de la visite officielle du président Trump en Arabie saoudite, QNA, l'agence de presse du Qatar, publie sur son site un document présenté comme un communiqué de l'émir Tamim ben Hamad al-Thani visant l'administration Trump et les « ambitions négatives » de ses voisins du Golfe, qualifiant le Hamas de « représentant légitime du peuple palestinien » et annonçant avoir d'« excellentes » relations avec Israël[70]. Quelques minutes plus tard, le compte Twitter de QNA poste trois messages révélant l'existence d'un complot contre le Qatar, attribué à l'Arabie saoudite, le Koweït, les Émirats arabes unis, Bahreïn et l'Égypte, et annonçant le rappel des diplomates qatariens dans ces cinq pays et le renvoi de leurs ambassadeurs à Doha. Les grands médias de la région, notamment saoudiens et émiratis, reprennent rapidement ces déclarations, qui déclenchent une crise.

Le gouvernement qatarien déclare alors que « l'agence de presse du Qatar a été piratée par une entité inconnue » et qu'« un faux communiqué attribué à Son Altesse a été diffusé », que le compte Twitter de QNA a aussi été piraté et que les techniciens qatariens ont mis plus de neuf heures à reprendre la main.

Une enquête du FBI conduite à la demande de Doha a conclu à la véracité du piratage[71]. Les Qatariens accusent Yousef al-Otaiba, l'influent ambassadeur des EAU à Washington, d'avoir orchestré cette virulente campagne médiatique anti-qatarienne.

La suite est connue. L'Arabie saoudite, les EAU, l'Égypte et Bahreïn ont pris dès le 5 juin des mesures pour isoler le Qatar : rappel des ambassadeurs à Doha, embargo sur les relations commerciales, refus du survol de leur territoire par les avions qataris, lancement d'une campagne médiatique à visée internationale. Il a été rapidement soumis au Qatar un ultimatum avec une liste de treize conditions pour la levée des sanctions (dont la réduction des relations avec l'Iran, la fermeture de la chaîne Al-Jazeera et d'autres médias, la fermeture de la base militaire turque en cours de construction, et la rupture des liens avec une liste d'organisations

70. Nabil Ennasri, « Reprise de la guerre froide du Golfe », *Orient XXI*, 31 mai 2017.

71. Karen De Young et Ellen Nakashima, « UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence official », *The Washington Post*, 16 juillet 2017.

qualifiées de terroristes et comprenant notamment les Frères musulmans et le Hezbollah), conditions jugées inacceptables par l'émirat.

B. L'Afrique

Les pratiques de manipulation de l'information en Afrique connaissent quelques traits distinctifs : de même que l'histoire de la téléphonie a sauté une génération technologique pour atteindre l'ère du smartphone (et de tous ses réseaux sociaux), les chemins de la désinformation se sont greffés, adaptés et développés sur cette innovation accessible à tous. Les influenceurs (acteurs de ces réseaux sociaux qui peuvent émettre, valider et/ou rediffuser, à différents degrés, ces informations) jouent un rôle déformant et extrêmement prescripteur dans l'information populaire, dans des pays où l'information publique reste largement sujette à caution (par la qualité ou par le contrôle des médias).

1. Le prochain terrain de jeu de la « guerre informationnelle » russe ?

Plusieurs signaux indiquent que l'Afrique pourrait être le prochain terrain de jeu de la « guerre informationnelle » russe, d'autant que le français et l'anglais sont des vecteurs faciles pour pénétrer le continent africain. Les travaux d'une équipe de recherche française ont révélé une propagation croissante des contenus russes à travers le web africain francophone[72]. Ce succès s'explique par plusieurs facteurs combinés. D'abord, la grande popularité des discours anti-occidentaux propagés par les grands médias internationaux russes (RT et Sputnik) auprès des opinions publiques africaines qui considèrent souvent la Russie sous le prisme de son passé soviétique anticolonial. Dans certains pays comme la Côte d'Ivoire, ces discours alimentent les débats politiques locaux. Ainsi les mouvements pro-Gbagbo trouvent dans les contenus produits par les médias russes des matériaux informationnels et des narratifs tout à fait opportuns. Le choix éditorial fait par RT et Sputnik de fortement médiatiser certains dossiers intéressant directement les opinions publiques africaines, comme celui touchant à l'avenir du franc CFA, aggrave naturellement les choses.

72. L'Observatoire de l'infosphère russophone dirigé par Kevin Limonier, maître de conférences à l'Université Paris 8, chercheur à l'Institut français de géopolitique et à la chaire Castex de cyberstratégie. Les éléments qui suivent nous ont été fournis par Kevin Limonier. Voir sa Note de recherche à paraître dans les collections de l'IRSEM.

Un autre problème est la tendance de beaucoup de journaux et médias africains en ligne à reprendre *in extenso* les contenus des médias russes sur leurs sites aux côtés de dépêches des grandes agences occidentales telles que l'AFP ou Reuters. Cette tendance permet aux contenus russes de toucher une très large audience en étant vus par un grand nombre de personnes. Ainsi, au Sénégal, de nombreux articles de Sputnik concernant l'Afrique sont repris par seneweb.com, quatrième site le plus consulté au Sénégal et suivi par plus d'un million et demi de personnes sur Facebook.

Par ailleurs, les stratégies de marketing digital employées par les agences russes sur les réseaux sociaux (*buzz*, *clickbait*) se prêtent particulièrement bien au contexte africain, où de nombreux utilisateurs ont recours à Facebook comme source d'information. Les théories du complot et autres nouvelles sensationnalistes dont sont friands les médias russes leur permettent d'augmenter considérablement leur audience dans un continent où ce genre de presse à sensation est très populaire.

La fascination d'une partie de la jeunesse africaine pour la figure de Vladimir Poutine auquel de nombreuses « fanpages » sont consacrées sur Facebook, et l'imaginaire de puissance militaire qui lui est associé, jouent également, tout comme la position de la Russie dans le conflit syrien, qui vient alimenter de très nombreux débats sur les réseaux sociaux au Maghreb (et plus particulièrement en Algérie).

Jusqu'à présent, l'activité des plateformes russes sur le continent africain n'était pas structurée, et leur popularité pouvait être considérée comme un effet collatéral des efforts déployés en direction de l'opinion publique française. Désormais, RT comme Sputnik envisagent d'étoffer leurs réseaux de correspondants en Afrique. Signe de cette nouvelle stratégie, la page Facebook de RT en français a vu son audience augmenter significativement (environ + 60 % de fréquentation) en janvier 2018. La très grande majorité des personnes à l'origine de cette augmentation sont des jeunes hommes du Maghreb et d'Afrique subsaharienne. Jusqu'à présent, aucun élément ne permet d'avancer s'il s'agit de vrais profils ou de bots.

2. La campagne antifrançaise à Goma

Le 2 janvier 2018 à Goma, en République démocratique du Congo (RDC), a été lancée une campagne numérique #BoycottFrance. La Lucha, mouvement citoyen, diffuse sur Twitter son mot d'ordre : « Condamner ne suffit pas, unissons-nous pour une campagne #BoycottFrance au Congo

et partout où les peuples africains sont opprimés avec la complicité de la France ». Des accusations plus précises encore visent la présence diplomatique française à Goma à travers l'Institut français comparé à une « cellule de renseignement française pour piller les ressources du Kivu ». Deux caricatures diffusées sur Twitter et largement reprises sur les réseaux sociaux accompagnent cette campagne. Sous les titres « Les sponsors de la barbarie en RDC » et « Les héritiers de Léopold II en RDC », elles entendent dénoncer le soutien présumé de la France à Joseph Kabila.

Leur succès tient à trois dimensions : la popularité du caricaturiste Kash, les mots d'ordre explicites de la Lucha, et le jeu sur des références empruntées à l'imaginaire de la Françafrique (le baril de pétrole de Total, le soutien militaire avec la mitrailleuse et le génocide rwandais avec les crânes au sol). Ces références se mêlent à de véritables faits, qui ne sont pas imputables à l'action de la diplomatie française : des négociations de Total en cours ou encore la présence de l'institut de formation Themiis. L'astuce de cette campagne réside ici dans la réinterprétation ou l'agglomération de faits, sans lien de causalité entre eux. La force de cette lecture est qu'elle s'inspire autant qu'elle nourrit des rumeurs populaires, et qu'il a suffi d'un stimulus de fausse nouvelle pour déclencher cette campagne. Le paradoxe est que cette attaque a été portée par des acteurs (la Lucha et Kash) avec lesquels l'ambassade de France est en contact. Les enjeux de dépollution de cette fausse nouvelle, au moins dans la forme (comment faire face à l'aspect viral de telles caricatures ?), invitent à réfléchir à des méthodes de communication alternatives et adaptées au monde des nouvelles technologies.

C. L'Amérique latine

Le délaissement relatif de l'Amérique latine par les capitales occidentales a représenté pour plusieurs entrepreneurs géopolitiques une opportunité de bâtir à peu de frais de nouveaux partenariats sous la bannière générique d'une multipolarité post-occidentale.

Depuis le milieu des années 2000, on observe ainsi différentes stratégies économiques, politiques et médiatiques en direction du continent latino-américain : la Chine (ressources naturelles, infrastructures, éducation), l'Iran (centres culturels, médias), la Syrie (mobilisation des diasporas syro-libanaises, réseaux sociaux)[73] et la Russie (commerce, coopération militaire, énergie, médias)[74].

73. Janaina Herrera, « La crise syrienne au prisme latino-américain (Venezuela, Brésil et Argentine) », *Les Carnets de l'Ifpo*, 14 septembre 2012.

74. Julia Gurganus, « Russia: Playing a Geopolitical Game in Latin America », Carnegie Endowment for International Peace, 3 mai 2018.

RT a commencé à émettre en espagnol dès 2009. La chaîne dispose aujourd'hui de bureaux en Argentine, au Venezuela, à Cuba, au Nicaragua, à Madrid, ainsi que dans les centres urbains nord-américains où se concentrent les communautés latinos, Miami et Los Angeles. D'après l'Atlantic Council[75], l'audience de RT est importante au sein de ces communautés si l'on en croit la fréquentation de la page Facebook de la chaîne en espagnol : 5,8 millions d'abonnés, contre 4,9 millions pour la page anglophone. Sputnik est également disponible en espagnol depuis 2014. C'est d'ailleurs par l'intermédiaire de ces réseaux sud-américains que les médias russes ont pu jouer un rôle dans la crise catalane (voir *supra*).

Cet investissement s'insère dans le paysage médiatique local grâce à une stratégie de partenariats et d'amplification sur les réseaux sociaux. La diffusion des programmes de RT a été facilitée par la signature de centaines d'accords spécifiques avec des médias nationaux et certaines émissions sont réalisées conjointement avec la chaîne vénézuélienne TeleSur.

Ce dispositif permet de diffuser une vision du monde commune fondée sur l'anti-impérialisme, la critique du libéralisme et la sensibilisation à des thèmes chers au Kremlin (dénonciation de la russophobie occidentale, mise en avant des échecs et crimes de l'Occident, présentation des révolutions de couleur sous un jour complotiste ou terroriste). Il convient de souligner que cette vision du monde correspond à des courants d'opinion importants en Amérique latine, et que cette orientation éditoriale n'empêche pas la réalisation de certains programmes de qualité.

Aujourd'hui, l'Amérique latine présente un terreau extrêmement favorable aux manipulations informationnelles du fait de plusieurs facteurs conjoncturels et structurels convergents :

- un usage massif des réseaux sociaux, avec un rôle particulier pour Facebook[76] et WhatsApp, qui permettent à des communautés de faire circuler de façon virale des informations non vérifiées entre connaissances et personnes de confiance ;

- un contexte socio-économique globalement défavorable, notamment au Venezuela, au Mexique et au Brésil, qui se traduit par un

75. Donara Barojan, « #ElectionWatch: RT y Sputnik Hablan Español », DFRLab Medium.com, 12 février 2018.

76. Le Brésil est le troisième pays derrière l'Inde et les États-Unis en termes d'usagers de Facebook, talonné par le Mexique. Il y a en outre 120 millions d'usagers brésiliens de WhatsAapp.

mécontentement important et une montée en puissance de la thématique de l'insécurité ;

• un cadre normatif moins exigeant qu'en Europe ou aux États-Unis en termes de droit à la vie privée et de marketing politique sur les réseaux sociaux ;

• une polarisation politique très forte qui se traduit par une montée du populisme et des candidatures d'extrême droite ;

• une série d'élections importantes dans six pays de la région, dont le Brésil, le Mexique, la Colombie et le Venezuela.

Au Brésil comme au Mexique, des rapports détaillés rendent compte d'un recours généralisé, tous partis confondus, aux bots et trolls sur les réseaux sociaux[77] et d'une polarisation extrême des échanges. Plusieurs mois avant les élections fédérales mexicaines du 1er juillet 2018, H. R. McMaster[78], alors conseiller du président Trump pour la sécurité nationale, dénonçait publiquement la mise en œuvre d'une stratégie sophistiquée d'influence russe en faveur du candidat de gauche, Andrés Manuel Lopez Obrador. Le Kremlin aurait, dans ce scénario, tout intérêt à voir un allié accéder au pouvoir à Mexico, déstabilisant son grand voisin du Nord dans un contexte de tensions déjà fortes sur des sujets d'intérêt commun (immigration, ALENA, lutte contre la drogue). On observait effectivement une ligne éditoriale de RT et Sputnik ouvertement favorable au candidat Obrador. Ceci dit, l'autre camp n'était pas en reste. La veille de l'élection – qui a vu la victoire d'Obrador –, une analyse détaillée de Ben Nimmo et ses collègues du Digital Forensic Research Lab de l'Atlantic Council, a mis en évidence un réseau de plusieurs millions de bots et douzaines de sites de désinformation qui ont été mobilisés contre Obrador, sans doute par l'entrepreneur Carlos Merlo, parfois décrit dans les médias internationaux comme un « millionnaire des *fake news*[79] ».

77. Dan Arnaudo, « Computational Propaganda in Brazil: Social Bots during Elections », in Samuel Woolley and Philip N. Howard (eds.), Working Paper 2017.8., Oxford, UK, Project on Computational Propaganda.

78. David Alire Garcia et Noe Torres, « Russia meddling in Mexican election: White House aide McMasters », Reuters, 7 janvier 2018.

79. Ben Nimmo *et al.*, « #ElectionWatch: Trending Beyond Borders in Mexico », *op. cit.*

Troisième partie

LES RÉPONSES

Ces dernières années, tous les acteurs – États, organisations internationales, société civile, acteurs privés – ont mis en place des mécanismes de lutte contre les manipulations de l'information. Cette section n'exposera que les réponses plus communes aux manipulations de l'information, en proposant une synthèse de ces mécanismes, étatiques ou non, qui sont « les premiers signes d'une réponse auto-immune[1] ». Elle commence par étudier l'affaire dite des « Macron Leaks », c'est-à-dire la tentative d'ingérence dans l'élection présidentielle française de 2017 qui, par son échec, illustre bien les vertus d'une réponse combinée de l'ensemble des acteurs. Elle s'intéresse ensuite aux réponses mises en œuvre par d'autres États sur le plan institutionnel, législatif et éducatif. Elle dresse enfin un panorama des réponses proposées à d'autres échelles : organisations internationales, société civile, acteurs privés.

Une interrogation commune est de savoir s'il vaut mieux répondre à une information manipulée à son endroit ou s'il vaut mieux l'ignorer et, si l'on choisit d'y répondre, s'il suffit de la corriger ou si l'on doit en profiter pour promouvoir un message alternatif. La réponse est un continuum à trois marches : l'ignorance, le défensif et l'offensif.

1. Jakub Janda, « Why the West is Failing to Counter Kremlin Disinformation Campaigns », *The Observer*, 30 décembre 2016.

L'ignorance est tentante, si l'on pense que l'information manipulée mourra d'elle-même. Le rythme médiatique est tel que peu d'affaires survivent au flot quotidien, et l'opinion oublie vite. Réfuter, c'est répéter, prendre le risque d'entretenir la conversation. On peut donc préférer opposer un « silence stratégique ». Mais c'est aussi prendre le risque de laisser s'infuser dans la population, ou auprès de certaines audiences, des idées fausses et potentiellement dangereuses qui, si elles ne sont pas contredites à la racine, pourraient croître avec le temps. L'ignorance ne devrait donc être réservée qu'aux manipulations mineures et inoffensives.

Réagir en défendant seulement, c'est-à-dire en corrigeant la fausse information, a l'avantage de ne pas la laisser se propager sans contradiction et, dans certains cas, si la réfutation est convaincante, d'y couper court rapidement. Mais cette tâche requiert du temps et des ressources humaines – pour surveiller les réseaux sociaux, détecter la manipulation, formuler la réponse, la diffuser, et analyser sa réception. Il y a également un risque d'effet pervers, la réponse pouvant alimenter le débat, voire fournir involontairement un nouvel angle aux trolls. Le plus efficace est de cumuler une correction défensive avec un message offensif, une nouvelle information permettant de reprendre le contrôle de la discussion – mais cela nécessite encore davantage de temps et de ressources.

I. Étude de cas : les 15 leçons françaises des « Macron Leaks »

Dans la longue liste des ingérences étrangères ayant visé des processus électoraux au cours des dernières années, la campagne présidentielle française de 2017 restera comme l'exception qui confirme la règle. Le ciblage du candidat Emmanuel Macron n'est parvenu ni à interférer dans les élections, ni à diviser la société française ; et, pour ces raisons, l'étudier est particulièrement intéressant. Par « Macron Leaks », nous n'entendons pas simplement la diffusion le vendredi 5 mai 2017 – soit deux jours avant le second tour de la présidentielle – de 9 gigabits de données piratées depuis les ordinateurs de campagne du candidat. Nous désignons, plus généralement, la campagne orchestrée contre lui et qui avait débuté des mois auparavant, via de nombreuses opérations de manipulation de l'information. Cette section s'intéresse au déroulé de ces « Macron Leaks », aux acteurs qui les ont (vraisemblablement)

orchestrés, les manières dont elles ont été efficacement contrées et, pour finir, les leçons qui peuvent en être tirées[2].

A. Que s'est-il passé ?

La fuite des documents n'a été que le paroxysme d'une campagne orchestrée depuis longtemps contre le candidat à la présidence. Celle-ci avait débuté avec la diffusion de rumeurs et insinuations qui ont pris de l'ampleur en janvier et février 2017. Par exemple, le 4 février 2017, un article de Sputnik présentait Macron comme un « agent des États-Unis » soutenu par « un lobby homosexuel très fortuné[3] ». Le Kremlin n'était pas cependant le seul joueur. D'autres attaques ont ainsi émané de la « légion étrangère » de trolls américains d'extrême droite de Marine Le Pen[4].

Le dernier élément, et non des moindres, en a été la rumeur #MacronGate. Deux heures seulement avant le dernier débat télévisé entre Emmanuel Macron et Marine Le Pen, soit le mercredi 3 mai 2017 à 19 heures[5], un internaute utilisant une adresse IP lettone a posté, sur le forum américain 4Chan, deux documents truqués suggérant que Macron détiendrait un compte offshore. Les documents ont rapidement été relayés par plus de 7 000 comptes Twitter, principalement pro-Trump, en utilisant souvent les hashtags #MacronGate et #MacronCacheCash. Pendant le débat télévisé, Marine Le Pen elle-même a mentionné l'existence d'un compte caché. Finalement, la rumeur a vite été discréditée et plusieurs enquêtes journalistiques ont prouvé que ces documents étaient des faux[6].

Incidemment, ce sont les mêmes personnes qui, ayant posté les faux documents sur 4Chan le mercredi, ont annoncé le vendredi matin que d'autres documents allaient être diffusés. En ceci, les responsables du #MacronGate ont fourni la preuve, si besoin en était, qu'ils étaient également responsables des « Macron Leaks », qui survinrent plus tard dans la journée.

L'opération avait commencé quelques mois plus tôt, avec des attaques d'hameçonnage (*phishing*). L'équipe de Macron a confirmé que leur parti

2. Cette section est le résumé d'un rapport détaillé à paraître : Jean-Baptiste Jeangène Vilmer, *The Macron Leaks: A Post-Mortem Analysis*, CSIS Europe Program, Washington D.C., automne 2018.

3. « Ex-French Economy Minister Macron Could Be "US Agent" Lobbying Banks' Interests », *Sputnik*, 4 février 2017.

4. Josh Harkinson, « Inside Marine Le Pen's "Foreign Legion" of American Alt-Right Trolls », *Mother Jones*, 3 mai 2017.

5. Tous les horaires ici exprimés le sont à GMT+2 (heure de Paris).

6. « How we debunked rumours that Macron has an offshore account », *France 24 – The Observers*, 5 mai 2017.

avait été visé à de nombreuses reprises depuis janvier 2017[7]. Plusieurs attaques ont utilisé des usurpations d'adresses électroniques. Au total, les messageries professionnelles et personnelles d'au moins cinq des proches collaborateurs de Macron ont été piratées, dont celles de sa plume, de son trésorier de campagne et de deux députés[8].

Les pirates ont attendu la dernière minute pour diffuser les documents : le 5 mai 2017, quelques heures seulement avant que la campagne cède officiellement la place au « silence électoral », c'est-à-dire la période de 44 heures avant la fermeture des bureaux de vote durant laquelle tous les médias respectent un silence politique total. Les documents ont été postés à l'origine sur Archive.org, puis sur PasteBin et 4Chan. Des comptes pro-Trump (William Craddick et Jack Posobiec) ont été les premiers à partager le lien sur Twitter, utilisant le hashtag #MacronLeaks, rapidement repris par WikiLeaks. Au total, « le hashtag #MacronLeaks a été utilisé dans 47 000 tweets, dans les seules trois heures et demie suivant le tweet initial[9] ».

D'autres faux documents ont été diffusés sur Twitter, dont certains n'avaient pas été inclus dans le *leak* d'origine, et qui venaient de ou s'adressaient à des personnes qui n'existaient même pas. Ainsi, un email, dont le caractère faux est évident, prétendument écrit par le directeur des affaires générales du candidat Macron, comprenait des déclarations du type : « Parfois, je me masturbe en écoutant des .wav de bruits d'évier qui se vident », « mon amour pour le Yaoi [manga gay japonais] et le métal progressif m'a empêché de voir la vérité » et « je baise le peuple »[10]. Ces déclarations ont été retweetées plus de 1 000 fois.

Pour conclure, les « Macron Leaks » révèlent le schéma de manipulation suivant : premièrement, le contenu est déversé sur le forum politique de la plateforme 4Chan. Deuxièmement, il est repris sur les réseaux sociaux plus conventionnels, comme Twitter. Troisièmement, le contenu est diffusé par le biais de communautés politiques, notamment l'ultra-droite américaine et l'extrême droite française. Là, des comptes catalyseurs, ou « gourous » (Craddick, Posobiec) sont retweetés par des personnes réelles

7. Michel Rose, Éric Auchard, « Macron campaign confirms phishing attempts, says no data stolen », Reuters, 26 avril 2017.

8. Frédéric Pierron, « MacronLeaks : 5 victimes et des failles de sécurité », fredericpierron.com blog, 11 mai 2017.

9. Ben Nimmo, Naz Durakgolu, Maks Czuperski et Nicholas Yap, « Hashtag Campaign: #MacronLeaks. Alt-right attacks Macron in last ditch effort to sway French election », DFRLab Medium.com, 6 mai 2017.

10. https://twitter.com/joshdcaplan/status/860868394534522880

(*sect followers*)[11] et des bots. L'utilisation de bots est particulièrement évidente, certains comptes ayant posté parfois 150 tweets par heure[12].

B. Qui est responsable ?

Il est facile de lier la partie informationnelle – c'est-à-dire la diffusion de rumeurs et de fausses nouvelles durant la campagne présidentielle – aux intérêts russes, compte tenu du fait que les médias russes, Sputnik et RT en tête, ont joué un rôle non négligeable dans cette diffusion. L'analyse des réseaux sociaux a également mis en évidence une forte congruence des communautés ayant diffusé ces rumeurs dont les principales visaient le candidat Macron et des communautés russophiles (75 % pour les comptes ayant relayé au moins trois rumeurs, et 95 % pour ceux ayant relayé cinq rumeurs). Le chercheur belge Nicolas Vanderbiest, qui a réalisé cette étude, en conclut que, « vu le niveau de concordance et la présence des acteurs clés de l'écosystème russe, […] on peut déceler une influence russe[13] ».

En revanche, il est structurellement plus difficile, voire impossible, d'attribuer une cyberattaque, et donc de répondre avec une certitude absolue à la question de savoir qui a piraté les emails de campagne du candidat Macron et qui a organisé la fuite massive de documents. Au moment où nous écrivons, plus d'un an après l'incident, la France n'a d'ailleurs toujours pas attribué officiellement l'attaque. D'autres, en revanche, l'ont fait.

La plupart des experts accusent le Kremlin, invoquant plusieurs indices, dont :

- L'adresse électronique (frankmacher1@gmx.de) utilisée initialement pour télécharger les documents sur Archive.org est enregistrée chez le même fournisseur webmail allemand qui avait déjà été impliqué dans la cyberattaque de 2016 contre le parti d'Angela Merkel[14]. Cette dernière attaque avait été attribuée à APT28, un groupe de cyberespionnage lié

11. Le mécanisme des gourous et des *sect followers* a été décrit par Lion Gu, Vladimir Kropotov et Fyodor Yarochkin, *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*, A Trendlabs Research Paper, Trend Micro, 2017, p. 42.

12. Ben Nimmo *et al.*, « Hashtag Campaign », *op. cit.*

13. Nicolas Vanderbiest, « Les institutions démocratiques : l'influence des réseaux sociaux durant une élection présidentielle », in Stéphane Taillat, Amaël Cattaruzza et Didier Danet (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018, p. 187.

14. Sean Gallagher, « Evidence suggests Russia behind hack of French president-elect », *Ars Technica*, 8 mai 2017.

à l'agence russe de renseignement militaire, GRU[15]. Bien sûr, cela seul ne prouve rien, GMX a plus de 11 millions d'utilisateurs actifs.

• Les tentatives de hameçonnage successives ont également été attribuées à APT28 par une compagnie japonaise de cybersécurité, TrendMicro[16].

• Tous les tableurs Excel de comptabilité qui ont fuité contenaient des metadata en cyrillique. Ils indiquaient que la dernière personne à avoir modifié les documents était un employé de l'entreprise russe de technologie de l'information Evrika (Eureka). Parmi les clients de l'entreprise figurent plusieurs agences gouvernementales, dont le FSB[17]. Cependant, il est difficile de déduire quoi que ce soit de cette connexion, puisque cela pourrait tout aussi bien être une intoxication (*false flag*) pointant vers Moscou.

• Les metadata des fichiers pdf de la rumeur #MacronGate sur le compte offshore montrent que ces documents ont été produits par deux machines Canon coûtant l'une 30 000 $ et l'autre plus de 100 000 $[18], ce qui indique que les responsables ont des moyens importants, plus proches de ceux d'un État que de « n'importe qui de 200 kg assis sur son lit », pour reprendre une expression fameuse[19].

• Le propagandiste et ancien député Russie unie Konstantin Rykov, parfois surnommé le « chef des trolls », et qui s'était largement vanté du rôle qu'il aurait joué dans l'élection de Donald Trump, a aussi reconnu qu'il avait échoué dans le cas de la France : « Nous avons réussi, Trump est président. Malheureusement, Marine n'est pas devenue présidente. Une opération a fonctionné, mais pas la deuxième[20]. »

---

15. Feike Hacquebord, « Pawn Storm Targets German Christian Democratic Union », *Trend-Labs Security Intelligence Blog*, 11 mai 2016. Parmi les faits d'armes plus récents d'APT28 figure la marine italienne (Jacopo Iacoboni, « Ci sono prove di un attaco degli hacker russi di APT28 anche in Italia », *La Stampa*, 17 juillet 2018).

16. Feike Hacquebord, *Two Years of Pawn Storm: Examining an Increasingly Relevant Threat*, A Trend Micro Research Paper, 25 avril 2017, p. 13.

17. Sean Gallagher, « Evidence suggests Russia behind hack of French president-elect », *op. cit.*

18. Bivol, « "Canon" for Macron: The fake news on Emmanuel Macron offshore account looks too professional », 5 mai 2017.

19. « It could be Russia, but it could also be China. It could also be lots of other people. It also could be somebody sitting on their bed that weighs 400 pounds », a déclaré Donald Trump lors de son premier débat télévisé avec Hillary Clinton, le 27 septembre 2016. Voir Jeremy Ashkenas, « Was It a 400-Pound, 14-Year-Old Hacker, or Russia? Here's Some of the Evidence », *The New York Times*, 6 janvier 2017.

20. Konstantin Rykov dans un entretien pour mediametrics.ru, dans le documentaire de Paul Moreira, *Guerre de l'info*, Arte thema, 2018.

• Facebook avait identifié deux douzaines de comptes espionnant l'entourage du candidat Macron et parle d'« agents russes se faisant passer pour des amis de proches de Macron[21] ».

Bien sûr, aucun de ces éléments pris isolément ne prouve quoi que ce soit mais, tous ensemble, ils pointent tout de même dans la direction de Moscou. Avec une exception notable : l'internaute responsable de la rumeur #MacronGate, deux jours avant la fuite, pourrait être un pirate américain néo-nazi, Andrew Auerheimer[22]. Du fait de l'alliance bien connue entre les mouvements américains d'extrême droite et la Russie[23], ces deux hypothèses ne sont cependant pas incompatibles.

La France n'a jamais officiellement attribué l'attaque. Le 1er juin 2017, Guillaume Poupard, directeur de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a déclaré que « l'attaque était tellement générique et simple qu'il pourrait s'agir de n'importe qui[24] ». Ce qui peut être retenu de façon relativement certaine, c'est que les responsables, quels qu'ils soient, étaient au moins liés aux intérêts russes et ont reçu de l'aide de l'ultra-droite américaine et de la fachosphère française, deux milieux aujourd'hui majoritairement proches de la vision du monde véhiculée par le Kremlin.

C. Pourquoi l'opération a-t-elle échoué et quelles leçons peuvent-elles en être tirées ?

In fine, la fuite n'a pas eu d'influence significative sur les électeurs français, en dépit des nombreux efforts des acteurs précédemment mentionnés. Pourquoi ? Le succès français résulte d'une combinaison de facteurs structurels, d'une dose de chance, et d'une bonne anticipation et réaction par l'équipe de campagne d'Emmanuel Macron, le gouvernement et la société civile, en particulier les médias traditionnels.

21. Joseph Menn, « Exclusive: Russia used Facebook to try to spy on Macron campaign – sources », Reuters, 27 juillet 2017.

22. David Gauthier-Villard, « U.S. Hacker Linked to Fake Macron Documents, Says Cybersecurity Firm », *The Wall Street Journal*, 16 mai 2017.

23. Casey Michel, « America's neo-Nazis don't look to Germany for inspiration. They look to Russia », *The Washington Post*, 22 août 2017.

24. Andrew Rettman, « Macron Leaks could be "isolated individual", France says », *EU Observer*, 2 juin 2017.

1. Des raisons structurelles

Comparé à celui de ses alliés, notamment les États-Unis et le Royaume-Uni, l'environnement politico-médiatique français présente une certaine résilience et apparaît moins vulnérable pour plusieurs raisons. D'abord, l'élection du président est directe, rendant toute tentative d'ingérence dans le processus électoral plus visible. Elle comporte deux tours, ce qui crée une difficulté supplémentaire pour les pirates, en ce qu'ils ne peuvent pas savoir à l'avance qui parviendra au second tour. Cela permet aussi à la population de corriger un potentiel résultat-surprise à l'issue du premier tour.

Ensuite, l'environnement médiatique français est plutôt robuste : il y a une forte tradition de journalisme sérieux. La population consulte principalement les sources d'information conventionnelles, et les médias du type tabloïds et autres sites alternatifs sont beaucoup moins populaires qu'ils peuvent l'être aux États-Unis ou au Royaume-Uni.

Enfin, et sans tomber dans les caricatures nationales, le « cartésianisme » joue également un rôle : la rationalité, la pensée critique, et un certain scepticisme sain font partie de l'ADN français et sont encouragés, dès l'école primaire et durant toute la vie professionnelle.

2. Une dose de chance

Les pirates ont été peu soigneux et ils ont commis un certain nombre d'erreurs. D'abord, ils ont fait preuve d'un excès de confiance. Ils ont surestimé leur capacité à choquer et à mobiliser les communautés virtuelles, ont sous-estimé la résistance et l'intelligence des médias conventionnels et, par-dessus tout, ils n'ont pas prévu que les membres de la campagne Macron réagiraient – et encore moins qu'ils réagiraient aussi bien. Ils ont aussi surestimé l'intérêt de la population pour une opération qui, au final, n'a absolument rien révélé. Ils ont cru que créer de la confusion serait suffisant, et que le contenu des documents serait secondaire. Mais il est rapidement devenu évident que les milliers d'emails et autres données étaient, au mieux, ennuyeux, et au pire, totalement ridicules. Le public s'en est désintéressé.

Ensuite, l'idée de lancer une offensive quelques heures seulement avant la période de silence électoral était à double tranchant : le but était certainement d'empêcher Macron de se défendre et de bâillonner les médias conventionnels. Et peut-être, en ce que les documents ne contenaient rien d'intéressant, ont-ils décidé de jouer sur l'annonce de la révélation, plutôt

que sur son contenu lui-même. Cependant, le minutage n'a pas laissé suffisamment de temps aux provocateurs pour diffuser l'information, et il a rendu la fuite plus que suspecte.

Enfin, l'attaque a également pâti de maladresse culturelle. La plupart des comptes catalyseurs (et bots) étaient en anglais, puisque les documents piratés avaient d'abord été diffusés par la communauté de l'ultra-droite américaine. Les compétences de la population française pour les langues étrangères étant ce qu'elles sont, cette stratégie n'était certainement pas la bonne.

3. Une bonne anticipation

Leçon 1 : Apprendre des autres. Paris a en quelque sorte profité des erreurs observées au cours de la campagne présidentielle américaine : dédain et désintérêt pour les opérations de manipulation de l'information, réticence à répondre au piratage du comité national démocrate, réaction tardive, etc. En janvier 2017, le ministre de la Défense reconnaissait que « nos services ont bien sûr les échanges nécessaires à ce sujet, ne serait-ce que pour en tirer des leçons pour l'avenir[25] ». Les services de renseignement américain ont également averti leurs homologues français des tentatives d'ingérence russe durant la campagne présidentielle française[26].

Leçon 2 : S'appuyer sur les bons acteurs. Deux structures ont joué un rôle particulièrement crucial : la Commission nationale de contrôle de la campagne électorale en vue de l'élection présidentielle (CNCCEP), une entité spéciale créée dans les mois précédant toute élection présidentielle française, qui sert de sentinelle de la campagne ; et l'Agence nationale de la sécurité des systèmes d'information (ANSSI), dont la mission était double, garantir l'intégrité des résultats électoraux et maintenir la confiance du public dans le processus électoral.

Leçon 3 : Sensibiliser. L'ANSSI et la CNCCEP ont alerté les médias, les partis politiques et le public sur les risques de cyberattaques et de manipulations de l'information durant la campagne. L'ANSSI a proposé, de façon proactive, de rencontrer et d'éduquer toutes les équipes de campagne très tôt dans le processus électoral : en octobre 2016, l'agence a organisé un séminaire auquel tous les partis sauf un ont participé (le Front national a rejeté la proposition).

25. Jean-Yves Le Drian (ministre de la Défense), entretien dans *Le Journal du dimanche*, 8 janvier 2017.

26. Martin Matishak, « NSA chief: U.S. warned France about Russian hacks before Macron leak », *Politico*, 9 mai 2017.

Leçon 4 : Faire preuve de fermeté et de détermination. Depuis le début de la campagne électorale, le gouvernement français a exprimé sa détermination à empêcher, détecter et, si nécessaire, à répondre aux ingérences étrangères. Le ministre de la Défense a déclaré qu'« en visant le processus électoral d'un pays, on attente à ses fondements démocratiques, donc à sa souveraineté » et que « la France se réserve le droit de riposter par tous les moyens qu'elle juge appropriés »[27]. Le ministre des Affaires étrangères a déclaré que « la France n'acceptera aucune ingérence dans son processus électoral[28] ». Un message similaire a été transmis par le ministre à son homologue russe, et par le président Hollande au président Poutine. Cela n'a visiblement pas suffi à empêcher l'attaque, et c'est pourquoi il serait exagéré de parler de dissuasion, mais cela l'a peut-être contenue à un niveau de menace qui aurait pu être plus élevé.

Leçon 5 : Prendre des mesures techniques. L'ANSSI a relevé le niveau de sécurité pour les bureaux de vote en sécurisant l'ensemble de la chaîne électorale pour garantir son intégrité. Suivant les recommandations de l'ANSSI, le ministère des Affaires étrangères a annoncé, début mars 2017, l'annulation du vote électronique pour les citoyens à l'étranger, en raison d'un risque élevé de cyberattaques.

Leçon 6 : Exercer une pression sur les plateformes numériques. Dix jours avant le vote, Facebook annonçait avoir supprimé 30 000 comptes suspects en France. Des révélations ultérieures montreront que ce chiffre était en réalité de 70 000[29]. C'est une mesure sans précédent qui est le résultat d'une pression croissante, des États et des opinions publiques, sur les plateformes numériques.

4. Une bonne réaction

Leçon 7 : Communiquer sur toutes les tentatives de piratage. Durant toute la campagne, l'équipe En Marche ! a communiqué abondamment et de façon ouverte sur son exposition à un piratage, et très tôt sur le piratage lui-même. À l'apogée de la crise, quand les documents ont été divulgués, En Marche ! a réagi en l'espace de quelques heures. À 23 h 56, le vendredi 5 mai, quelques heures seulement après que les documents ont été déposés

27. Jean-Yves Le Drian (ministre de la Défense), entretien dans *Le Journal du dimanche*, 8 janvier 2017.

28. Martin Untersinger, « Cyberattaques : la France menace de "mesures de rétorsion" tout État qui interférerait dans l'élection », *Le Monde*, 15 février 2017.

29. Joseph Menn, « Exclusive: Russia used Facebook to try to spy on Macron campaign – sources », *op. cit.*

en ligne, et quatre minutes avant que ne débute le silence électoral, l'équipe de campagne a produit un communiqué de presse[30].

Leçon 8 : Battre les pirates à leur propre jeu. Puisque les piratages ne pouvaient pas être évités, l'équipe En Marche ! avait placé plusieurs pièges : de fausses boîtes de courriels, de faux mots de passe, de faux documents. Cette tactique de diversion qui consiste à noyer les pirates dans une masse d'informations non pertinentes, voire parfois délibérément ridicules, est appelée *blurring* cyber ou numérique. Grâce à elle, la charge de la preuve a été renversée, revenant finalement aux pirates eux-mêmes : l'équipe de campagne de Macron n'a eu à justifier aucune information potentiellement compromettante contenue dans les « Macron Leaks » ; bien plutôt, les pirates ont eu à se justifier sur les raisons pour lesquelles ils avaient volé et divulgué des informations qui semblaient, au mieux, inutiles, au pire, fausses ou trompeuses.

Leçon 9 : Riposter sur les réseaux sociaux. La forte présence de l'équipe de campagne du candidat Macron sur les réseaux sociaux leur a permis de réagir rapidement. Ils ont systématiquement répondu aux posts ou commentaires qui mentionnaient les « Macron Leaks ».

Leçon 10 : Utiliser l'humour. L'intégration, par la campagne Macron, de touches d'humour et d'ironie dans les réponses aux pirates a augmenté la visibilité, la rapidité et la popularité de la riposte sur les différentes plateformes.

Leçon 11 : Saisir la justice. Le vendredi soir, alors que le *leak* était en cours et seulement quelques heures après la divulgation initiale, le parquet de Paris a ouvert une enquête, confiée à la Brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI).

Leçon 12 : Décrédibiliser les médias propagandistes. Le 27 avril, l'équipe Macron a confirmé avoir refusé les accréditations presses à RT et Sputnik pour le reste de la campagne. Même après les élections, ils ont été privés d'accès au palais de l'Élysée ou aux conférences de presse du ministre des Affaires étrangères. La décision peut se justifier pour deux raisons au moins. D'une part, ces médias ne font pas un travail journalistique, mais de propagande : ce n'est pas seulement la position d'Emmanuel Macron, qu'il a exprimée clairement durant la campagne, et de façon plus notable encore devant le président Poutine à la conférence de presse à Versailles quelques semaines seulement après les élections[31], mais c'est là la position du Parlement européen depuis

30. « En Marche a été victime d'une action de piratage massive et coordonnée », communiqué de presse, En Marche !, 5 mai 2017.

31. Emmanuel Macron, conférence de presse conjointe avec M. Vladimir Poutine, Versailles, 29 mai 2017. Voir Marc de Boni, « Devant Poutine, Macron dénonce la "propagande" des médias pro-russes », *Le Figaro*, 29 mai 2017.

novembre 2016[32]. D'autre part, la participation à ces conférences de presse se fait par invitation. En cela, les institutions françaises n'ont pas à justifier l'exclusion de ces deux organes.

Leçon 13 : Banaliser le contenu divulgué. Le communiqué de presse de l'équipe En Marche ! déclarait que les documents divulgués « révèlent le fonctionnement normal d'une campagne présidentielle ». De fait, rien d'illégal, ou même d'intéressant n'a été trouvé.

Leçon 14 : Compartimenter l'information. Si les messages fuités ne contenaient rien de croustillant, c'est parce que l'équipe de campagne d'En Marche ! avait conscience que tout ce qu'ils écrivaient dans des courriels pourrait se retrouver sur la place publique. Ils ont donc compartimenté la communication en trois niveaux : « L'anodin et la logistique par mail, le confidentiel sur les applis [cryptées] et le sensible en face-à-face[33]. »

Leçon 15 : Appeler les médias à agir de façon responsable. Dans la nuit du vendredi, l'équipe Macron a renvoyé l'affaire devant la CNCCEP qui a produit un communiqué de presse dès le lendemain, demandant « aux organes de presse, et notamment à leurs sites internet, de ne pas rendre compte de ces données, en rappelant que la diffusion de fausses informations est susceptible de tomber sous le coup de la loi, notamment pénale[34] ». La majorité des médias traditionnels a répondu à cet appel en choisissant effectivement de ne pas rendre compte du contenu des informations divulguées. Certains sont même allés plus loin, en dénonçant une tentative d'ingérence électorale et en appelant leurs lecteurs à ne pas se laisser manipuler. La réaction du *Monde*, par exemple, a été exemplaire de ce point de vue[35].

Conclusion

Dans les cinq étapes de l'ingérence électorale décrites par Mika Aaltola dans le contexte de l'élection présidentielle américaine de 2016[36] (voir *supra*), les « Macron Leaks » n'atteignent que la troisième étape. Il y a bien eu une campagne de manipulation de l'information, un piratage de données, une fuite à grande échelle, mais pas de blanchiment ou de banalisation. Ce qui

32. Parlement européen, résolution du 23 novembre 2016 sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers (2016/2030(INI)).

33. Nathalie Raulin et Guillaume Gendron, « Piratage : l'équipe Macron sur le pont », *Libération*, 10 août 2017.

34. Communiqué de presse, CNCCEP, 6 mai 2017.

35. « Le Monde et les documents des "MacronLeaks" », *Le Monde*, 6 mai 2017.

36. Mika Aaltola, *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Autocratic Meddling*, *op. cit.*

a été parfaitement empêché est « le "blanchiment" de cette fausse monnaie numérique que sont les nouvelles inventées, diffusées puis reprises par une autorité qui les légitime aux yeux du public[37] », le processus par lequel les informations, histoires, narratifs sont rincés de toute trace les reliant à l'ingérence originelle. Finalement, des facteurs structurels mais également une stratégie de riposte efficace ont permis à la France de limiter de façon significative les dommages des « Macron Leaks ».

II. Les réponses étatiques

Les États européens sont aujourd'hui plus conscients du défi posé par les manipulations informationnelles et plus résolus à y répondre. Davantage de pays s'intéressent au phénomène et comprennent que ce ne sont pas les actions les plus visibles, comme l'affaire Lisa en Allemagne ou les ingérences dans les élections aux États-Unis et en France, qui sont les plus dangereuses, mais le minage quotidien de la confiance dans les institutions et les valeurs démocratiques et libérales. L'ingérence étrangère a pour but non pas tel ou tel coup, mais le façonnement à long terme de l'environnement politique. De ce point de vue, les États ont pris ou sont en train de prendre un certain nombre de mesures.

A. Organisation interne : des réseaux et quelques centres

Un consensus domine : compte tenu de la nature du problème, il faut adopter une approche globale et donc décloisonner, faire travailler ensemble des services généralement trop ensilotés. Partout, les États organisent des réseaux : cette manière de travailler est traditionnelle dans les pays du Nord (la Finlande parle d'« organes de collaboration intersectorielle ») et moins habituelle ailleurs, mais tous les États reconnaissent cette nécessité. Certains ont des réseaux formels déjà constitués :

- La Suède a une *task force* sur les campagnes d'influence sous l'autorité du Bureau du Premier ministre, et l'Agence de sécurité civile (MSB), dont l'une des missions est d'identifier et de contrer les campagnes d'« influence informationnelle », joue également un rôle de *hub* pour l'ensemble des services concernés.

- La Finlande traite le sujet dans un réseau généraliste de haut niveau (le comité de sécurité, composé de 19 membres et 3 experts représentant

37. Jean-Yves Le Drian, *Discours de clôture* du 4 avril 2018, *op. cit.*

l'ensemble des ministères et services concernés, ainsi que la communauté d'affaires, se réunit neuf fois par an) et dans un réseau dédié : l'Information Influencing Network. Créé en décembre 2014, celui-ci est informel au sens où il n'a pas donné lieu à une nomination officielle, mais il a tout de même été approuvé par le comité de sécurité. Sa mission est d'identifier, analyser et répondre aux tentatives hostiles d'ingérence étrangère. Il comprend une trentaine d'experts gouvernementaux occupant des postes clés dans leurs ministères respectifs ainsi que des représentants du CICR et d'ONG, qui se réunissent une fois par mois.

• Le Danemark a une *task force* présidée par le ministère de la Justice et réunissant également les ministères de la Défense et des Affaires étrangères, et les services de renseignement. Le ministère des Affaires étrangères danois a aussi une *task force* interne, impliquant trois départements – Public Diplomacy (communication), Security Policy et European Neighborhood & Russia. En tout, ces sujets occupent une dizaine de personnes dans le ministère. Cette équipe transversale est placée sous l'autorité directe du directeur politique, ce qui rend les décisions plus rapides.

• Le Royaume-Uni dispose d'une cellule interministérielle de communication stratégique hébergée au bureau des Affaires étrangères et du Commonwealth (FCO) avec des moyens interministériels conséquents (une vingtaine de personnes) et un budget important. Cette cellule a pour mission de contrer les narratifs de manipulation de l'information en identifiant leurs sources et en analysant leurs effets, ainsi que d'accroître la résilience des États tiers les plus soumis à ces manipulations. Elle développe aussi des partenariats avec les médias, les acteurs technologiques et la société civile afin de créer un réseau de vérificateurs.

• Les Pays-Bas ont un réseau animé par le coordinateur national contre le terrorisme (NCTV) sous l'autorité du ministère de la Justice, impliquant les Affaires étrangères, la Défense, les services de renseignement, le NCTV et les Affaires sociales.

• La Lettonie a un groupe de travail sur les menaces informationnelles présidé par la division de la politique médiatique du ministère de la Culture et impliquant d'autres ministères, les services de renseignement et des représentants du parlement.

• Singapour a un réseau coordonné par le ministère des Communications et de l'Information.

Parallèlement à cette tendance à la mise en réseau, certains États ont aussi créé des centres dédiés :

• Les États-Unis (voir *infra*) ont créé en 2016 un Global Engagement Center (GEC) au sein du département d'État, initialement pour lutter contre la propagande de Daech, puis avec une compétence étendue l'année suivante aux menaces étatiques, en premier lieu provenant de Russie. Parfois décrit comme coordonnant le travail interagences (notamment entre le DoD, la communauté du renseignement, l'USAID, le BBG et le département d'État), le GEC est surtout constitué de personnels du Pentagone, plus nombreux et mieux formés sur ces questions que les agents du département d'État. Au GEC s'ajoutent 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. Contrairement à d'autres pays, les États-Unis ne souffrent pas d'un manque de ressources dans ce domaine, plutôt d'un manque de coordination : il y a tellement de structures qu'il est difficile de comprendre qui fait quoi et, surtout, qui donne une direction générale (voir *infra*). C'est pourquoi des sénateurs démocrates demandent la création d'une cellule interagences de haut niveau sur le modèle du Centre national de contre-terrorisme (NCTC), pour coordonner tous les efforts américains contre les opérations d'influence russes[38].

• La République tchèque a créé en janvier 2017 un centre de lutte contre le terrorisme et les menaces hybrides (CTHT) au sein du ministère de l'Intérieur. Composé de 15 à 20 personnes, il combine une double fonction de communication stratégique (un dispositif de surveillance et de réaction) et de *policy-making*. Contre les manipulations de l'information, il ne fait pas de contre-discours, seulement de la réfutation. Il a aussi une dimension publique (organise des événements, est présent sur les réseaux sociaux, etc.).

• La Suède devrait créer une nouvelle autorité de « défense psychologique », a annoncé le Premier ministre en janvier 2018. Elle pourrait absorber la section contre-influence du MSB, qui est l'une des structures les mieux organisées et les plus innovantes que nous ayons visitées.

À noter que ces centres ne se substituent pas aux réseaux mais s'y ajoutent : il n'y a pas deux modèles, l'un souple (le réseau), l'autre rigide

38. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, *op. cit.*, p. 4.

(le centre), mais un consensus sur l'importance du réseau et, chez certains, une cristallisation supplémentaire dans un centre dédié.

L'efficacité de ces structures dépend des moyens qui leur sont consacrés, c'est-à-dire de leurs ressources humaines et financières, qui elles-mêmes dépendent de la volonté politique. Elles doivent en outre surmonter des difficultés, dont les principales sont le rattachement institutionnel, qui peut susciter des batailles territoriales entre services, et la communication, à la fois vis-à-vis de l'extérieur, pour montrer que l'entité n'est pas un « ministère de la vérité » orwellien et, à l'intérieur, pour convaincre de son utilité.

B. L'implication des parlements

Les États-Unis et le Royaume-Uni ont entamé des enquêtes parlementaires particulièrement approfondies pour établir les responsabilités dans les ingérences dont ils ont été victimes. Le caractère public de ces enquêtes, très suivies par les médias, permet de sensibiliser la population, de l'informer de manière très précise (les connaissances accumulées sont impressionnantes) et sans doute d'avoir un effet dissuasif. Certains comités ont produit ou vont produire des rapports importants, qui contribuent grandement à la compréhension du problème. On peut notamment citer, aux États-Unis, le travail des sénateurs démocrates américains (*Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, publié en janvier 2018 pour la commission des Affaires étrangères) et, au Royaume-Uni, le rapport à venir du comité pour le numérique, la culture, les médias et le sport de la Chambre des communes (*Disinformation and "fake news"*, un rapport d'étape a été publié en juillet 2018, le définitif est attendu pour l'automne).

Autre cas intéressant, dans une autre région du monde : Singapour. Les autorités sont conscientes de la vulnérabilité de leur population, très diverse (multiethnique et multireligieuse) donc potentiellement parcourue de lignes de tension, anglophone donc aisément pénétrable, et très exposée à l'influence chinoise. Le parlement s'est donc saisi du sujet et, pour préparer une nouvelle loi contre la désinformation, il a créé en janvier 2018 un Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures, qui a depuis mené un grand nombre d'auditions, y compris d'experts internationaux. L'ensemble des documents est disponible sur le site du comité et constitue en soi une mine d'informations[39].

39. Parliament of Singapore, Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures.

C. Sensibilisation et éducation

Pour sensibiliser l'opinion aux dangers des manipulations de l'information, les États ont notamment mis en œuvre les mesures suivantes :

- production de doctrine (les *Central Government Communications Guidelines* de 2016 en Finlande, etc.) ;
- soutien à la recherche par la collaboration avec les universités (le MSB suédois a préparé un *Handbook* sur les opérations d'influence avec l'université de Lund) et le financement de projets de recherche (le MSB finance 2 à 5 projets de recherche pour un budget total de 2 millions d'euros) ;
- campagnes massives de sensibilisation, y compris en diffusant par voie postale (le MSB a tiré 4,7 millions d'exemplaires d'une brochure expliquant quoi faire en cas de crise, incluant les cas d'attaques terroristes ou campagnes de manipulation de l'information. Elle est adressée à tous les foyers – auparavant, ces pages spéciales étaient dans le bottin mais la dématérialisation a réduit la diffusion des informations, notamment dans les zones rurales) ;
- formation des fonctionnaires, journalistes, entreprises (le MSB a déjà formé 11 000 fonctionnaires) ;
- éducation aux médias (à partir de 2018, toutes les écoles primaires suédoises enseigneront les bases de la programmation et la capacité de distinguer entre des sources fiables et d'autres qui ne le sont pas ; la Lettonie va introduire des sujets de défense dans les écoles à partir de 2020, dont l'éducation aux médias, la cybersécurité et l'éducation de défense ; Singapour a adopté le concept suédois de « défense totale » et l'enseigne dans les écoles ; le ministère italien de l'Éducation a lancé un programme innovant de formation à la vérification des faits qui donne déjà des résultats encourageants[40]) ;
- présence internationale, en envoyant du personnel à Bruxelles (EU East StratCom Task Force), Riga (NATO StratCom CoE) et Helsinki (Hybrid CoE), et lors des rencontres annuelles importantes (StratCom Summit à Prague, Riga StratCom Dialogue, StratCom de l'Atlantic Council à Washington DC) ;

40. Christopher Livesay, « Italy Takes Aim At Fake News With New Curriculum For High School Students », NPR, 31 octobre 2017 ; et entretiens à Rome, 30 novembre 2017.

• élaboration d'outils simples d'identification et de diagnostic à la disposition du public. Dans cette perspective, le rapport du MSB suédois et de l'université de Lund propose l'application régulière d'un diagnostic « DIDI » aux activités informationnelles : pour être qualifiée de manipulation de l'information, une activité informationnelle doit 1) contenir des éléments trompeurs (*deception*), 2) avoir l'intention de blesser (*intention*), 3) être perturbatrice (*disruption*) et 4) constituer une ingérence (*interference*). Un tel diagnostic offre la possibilité aux communicants et à l'opinion publique de différencier les manipulations de l'information d'opérations d'influence plus sincères[41].

D. Mesures vis-à-vis des médias

Les quatre principales mesures étatiques à l'égard des médias sont l'enregistrement, l'interdiction, la régulation et la dénonciation.

1. Enregistrement

Les États-Unis utilisent le *Foreign Agent Registration Act*, une législation datant des années 1930 et initialement adoptée pour contrer la propagande nazie, afin de forcer les entités se livrant à de l'information politique et financées par un agent étranger à se présenter comme telles et à faire état de leurs relations financières avec l'étranger. En application de cette législation, le département de la Justice a demandé à RT America et à Sputnik de suivre cette procédure d'enregistrement, ce qu'ils ont fait malgré les protestations de Moscou[42].

La législation FARA présente l'avantage de ne pas se prononcer sur le contenu des messages promus par les « agents étrangers » (ce n'est pas un instrument de censure), mais simplement d'accroître la transparence sur les sources de financement des acteurs, laissant les citoyens tirer leurs propres conclusions quant à la crédibilité des messages publiés. Il est clair cependant que le dispositif trouve ses limites face aux acteurs hybrides, qui ne sont ni des entreprises ni des lobbyistes enregistrés, et dont les éventuels liens financiers avec une puissance étrangère ne sont pas facilement démontrables.

41. James Pamment *et al.*, *Countering Information Influence Activities: The State of the Art,* Department of Strategic Communication, Lund University, research report, version 1.4, 1er juillet 2018, p. 14.

42. Jack Stubbs et Ginger Gibson, « Russia's RT America registers as "foreign agent" in U.S. », Reuters, 13 novembre 2017.

Par ailleurs, une course à l'enregistrement est engagée avec la Russie. En novembre 2017, Moscou a amendé sa loi de 1992 sur la presse pour permettre à un média d'être qualifié d'agent de l'étranger. C'est la réponse russe à la décision américaine d'appliquer la loi FARA à RT. Désormais, « toute personne morale enregistrée dans un pays étranger ou toute structure étrangère sans statut de personne morale qui diffuse à une quantité illimitée de personnes des matériaux écrits, audio ou audiovisuels (médias étrangers) peut être reconnue comme un média étranger, exerçant la fonction d'agent de l'étranger ». Cela lie de fait la loi sur les médias à celle sur les ONG « agents de l'étranger » qui a été adoptée en 2012. Le pouvoir se réfugie derrière la symétrie (nous faisons comme les Américains) mais la différence est que la loi américaine a pour motivation la transparence et ne remet pas en cause leur liberté de travailler tandis que la crainte est que, sous couvert de transparence, la loi russe exercera une pression sur les médias qui les poussera à la fermeture.

2. Interdiction

En Ukraine, l'interdiction des médias russes a commencé en 2014, par les principales chaînes, pour finalement atteindre 73 chaînes interdites en 2016. Des quotas de contenus en ukrainien ont également été imposés à la radio et à la télévision. Par ailleurs, des sites russes tels que VKontakte, Odnoklassniki, Yandex et Mail.ru ont été interdits en mai 2017, ce qui a fait chuter leur fréquentation. Le gouvernement ukrainien a enfin créé un ministère de la politique de l'information. Kiev a été fortement critiqué pour ces mesures, non seulement par Moscou mais aussi en Occident. L'Ukraine s'est défendue en arguant de l'état de guerre dans lequel elle se trouve. De nombreux autres pays, dont l'Indonésie, ont également choisi de bloquer des sites ou des réseaux sociaux pour lutter contre les manipulations de l'information.

3. Régulation

C'est l'option médiane, préférée par la plupart des démocraties libérales. Celle-ci peut signifier le renforcement des autorités de régulation des médias. L'Ofcom britannique est régulièrement cité comme un exemple dans ce domaine, en ce qu'il n'hésite pas, régulièrement, à dénoncer les biais de RT, par exemple. En France, le Conseil supérieur de l'audiovisuel a prononcé une mise en demeure de la chaîne RT France, le 27 juin

2018, pour « manquements à l'honnêteté, à la rigueur de l'information et à la diversité des points de vue[43] », parce que, dans un reportage en Syrie diffusé le 13 avril, la chaîne avait falsifié la traduction d'un témoin de la Ghouta, lui faisant dire que l'attaque chimique était simulée, alors qu'il parlait de la famine sévissant dans la région. La chaîne avait plus tard invoqué « une erreur purement technique ».

Plus généralement, la régulation peut signifier le fait de passer une « loi anti-désinformation ». De nombreux États ont adopté ou tentent actuellement d'adopter une nouvelle législation en ce sens. L'Institut Poynter en tient à jour un recensement[44]. La plus connue est sans doute la loi allemande dite « NetzDG » (pour *Netzwerkdurchsetzungsgesetz*), en vigueur depuis janvier 2018, qui oblige les plateformes de plus de 2 millions de membres (Facebook, YouTube, Twitter) à supprimer des contenus « évidemment illégaux » dans les 24 heures sous peine d'amendes pouvant atteindre 50 millions d'euros.

Les difficultés se trouvent généralement dans la définition de l'objet (surtout s'il est désigné par une catégorie aussi vague que *fake news*, comme c'est souvent le cas) et l'équilibre avec la protection des libertés publiques, en particulier la liberté d'expression et la liberté de la presse. Dans les pays démocratiques, la société civile, notamment les ONG et les associations de journalistes, comme un certain nombre de parlementaires, sont souvent sceptiques sur la nécessité et l'efficacité d'une nouvelle législation, et pointent les risques d'effet pervers.

4. Dénonciation

Certains États permettent à leurs citoyens de dénoncer les fausses informations sur un site gouvernemental. En Italie, par exemple, un portail permet à tout un chacun, avec un courriel et un lien vers l'information incriminée, d'attirer l'attention de la Polizia Postale, l'unité de la police en charge de la cybercriminalité. Le gouvernement thaïlandais, via le ministère de la Santé publique, a lancé une application mobile, Media Watch, développée par le Fund for Development of Safe and Creative Media for Mental Health, par laquelle chacun peut signaler une fausse nouvelle. L'armée chinoise a aussi mis en ligne un site permettant à la population

43. Conseil supérieur de l'audiovisuel, « Manquements à l'honnêteté, à la rigueur de l'information et à la diversité des points de vue : la chaîne RT France mise en demeure », *Assemblée plénière du 27 juin 2018*, 28 juin 2018.

44. Daniel Funke, « A Guide to anti-misinformation actions around the world », Poynter, 2 juillet 2018.

de signaler de fausses nouvelles (avec toute l'ambiguïté que ce genre de mesure a dans un contexte non démocratique).

E. Le cas des États-Unis

L'appareil institutionnel américain a offert pendant toute la période de la guerre froide une architecture de réponse aux manipulations de l'information soviétiques des plus abouties[45]. La lutte contre la désinformation et « les mesures actives » du Kremlin est devenue une priorité pour la sécurité nationale américaine au début des années 1980[46]. Cette organisation a été démantelée après la chute du mur et s'est militarisée après le 11-Septembre dans le cadre de la longue guerre contre la terreur. Depuis les attentats de septembre 2001, en l'absence d'un arsenal de diplomatie publique similaire à celui opérant lors de la guerre froide et, pour faire face à la principale guerre idéologique menée par les groupes djihadistes Al-Qaïda puis Daech contre les États-Unis, les capacités de riposte américaines en matière de contre-propagande se sont essentiellement organisées autour des IO (*Information Operations*) et des actions de contre-propagande militaire. Elles se seraient rendues particulièrement nécessaires du fait du manque de moyens, et de la « bunkerisation » ou de la disparition, sur certains théâtres, des principaux agents de terrain en matière de diplomatie publique, que sont les *public affairs officers* (PAOs). Or, l'ensemble de ces actions pensées et élaborées à la fois au niveau national et au sein des commandements régionaux (Centcom, Africom, Pacom, etc.) peut paraître redondant ou contre-productif, ce qui génère des débats interagences sur les répartitions des responsabilités de la réponse, l'efficacité et le coût des activités de « diplomatie publique » militaires ou civiles[47].

Suite à l'interférence russe dans le processus électoral américain de 2016 (caractérisée par un usage ciblé des plateformes internet et des

45. Pour toute cette section, voir Maud Quessard, *La Diplomatie publique américaine et la désinformation russe : un retour des guerres de l'information ?*, Note de recherche de l'IRSEM, n° 54, 30 avril 2018.

46. Le 15 janvier 1983, le président Reagan signe la directive 77 (National Security Decision Directive 77), qui renforce le rôle attribué à la diplomatie publique en la définissant comme « l'ensemble des actions entreprises par le gouvernement des États-Unis dans le but de générer du soutien [à l'étranger] pour nos objectifs de sécurité nationale ». La directive 77 fait de la diplomatie publique un élément clé du processus décisionnel de la politique étrangère, et officialise une stratégie multidirectionnelle visant à affaiblir la poussée soviétique en soutenant les efforts des dissidents dans l'ensemble de l'Europe de l'Est. Cette réorganisation significative des affaires étrangères a pour unique but de mener à bien le Projet Vérité (*Project Truth*) conçu dès 1981 par le président Reagan et ses conseillers pour contrer les effets de la propagande soviétique.

47. Wallin Matthew, « Military Public Diplomacy. How the Military Influence Foreign Audiences », White Paper, *American Security Project*, février 2015.

réseaux sociaux) et à l'implantation, aux États-Unis, de médias d'État russes, Sputnik et RT, les médias américains ont relayé de nombreuses inquiétudes quant à ce qui est perçu par les politiques comme de nouvelles stratégies d'influence russes. Ces inquiétudes traduisent une préoccupation plus profonde qui est partagée dans les milieux politiques, diplomatiques ou militaires américains, celle d'un manque de préparation et de coordination pour engager une riposte adaptée et proportionnelle à la menace.

À Washington, l'atmosphère fait écho aux grandes heures du maccarthysme, et les réponses officielles des nouveaux « combattants de la désinformation » (*warriors of disinformation*) semblent s'inspirer de l'expérience de guerre froide. En effet, pour faire face à l'ensemble des stratégies de l'influence russe (médiatiques et cyber), l'ex-directeur du renseignement, James Clapper, soutenu, entre autres, par le directeur du Cyber Command, l'amiral Mike Rogers, appelait dès janvier 2017 à ressusciter « la machine de l'information » de guerre froide, l'USIA (United States Information Agency) en la mettant « sous stéroïdes », ajoutant à la confusion entre diplomatie d'influence et contre-propagande[48]. Le débat public américain contemporain, dans les médias, au Congrès et dans les milieux militaires, fait état d'une forme de nostalgie vis-à-vis de « la machine d'information de guerre froide », essentiellement représentée par l'USIA. Le conflit de guerre froide y est présenté comme l'archétype de la « guerre totale » (*Total Cold War*), impliquant l'ensemble des piliers de la puissance nationale autrement appelés DIME (*Diplomatic*, *Information*, *Military*, *Economic*).

Si les divers travaux parlementaires entrepris depuis 2017[49] ne permettent pas de dégager de doctrine homogène en matière de contre-propagande américaine, cela vient du fait que les acteurs menant la contre-offensive agissent pour le compte de ministères, d'agences ou d'institutions indépendantes sans qu'il existe une coordination efficace entre les différentes actions menées, ce qui constitue un écueil récurrent de la bureaucratie américaine.

La coordination de la réponse est particulièrement difficile, sur le plan intérieur autant que pour la politique extérieure, les efforts des agences étant souvent concurrents et parfois contradictoires. Le département de la Sécurité intérieure (Department of Homeland Security, DHS) a créé une

48. Carlo Muñoz, « Clapper calls for U.S. Information Agency "on steroids" to counter Russian propaganda », *The Washington Times*, 5 janvier 2017.

49. Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services House of Representatives, « Crafting an Information Warfare and Counter-Propaganda Strategy for the Emerging Security Environment », 115th Congress, 1st session, Washington, USGPO, 15 mars 2017.

task force anti-désinformation qui est opérationnelle depuis janvier 2018 et compte pour l'instant une dizaine de personnes (elle devrait s'agrandir). Elle vise à mieux coordonner les efforts des différentes agences, bâtir des capacités et engager les acteurs privés. Le mois suivant, en février 2018, le Procureur général a lui aussi créé une Cyber-Digital Task Force au sein du département de la Justice, chargée notamment de lutter contre les opérations hostiles d'influence étrangère – un rôle depuis longtemps dévolu au Département, en particulier au FBI qui, en novembre 2017, avait lui-même créé une Foreign Influence Task Force (FITF), dont l'une des missions est la coordination avec les autres agences, dont le DHS, le département d'État, la NSA et la CIA, tout en nouant des relations avec les autorités fédérées et locales ainsi que le secteur privé et les plateformes numériques[50]. En juillet 2018, la NSA et le Cyber Command annonçaient qu'ils allaient désormais travailler ensemble pour lutter contre le risque d'ingérence russe, en vue des élections de mi-mandat de novembre. Reconnaissant le manque de coordination du dispositif américain, le général Paul Nakasone, commandant du Cyber Command et directeur de la NSA, a déclaré « faire ce qu'il pouvait » en l'absence d'« une approche globale dirigée par le président ou la Maison-Blanche »[51].

Plusieurs études récentes de think tanks américains (Atlantic Council, Brookings, American Security Project) et européens (London School of Economics) tentent de tirer des enseignements de cet héritage en proposant de l'adapter aux enjeux contemporains. Or, la nécessité de reconstituer une agence paragouvernementale de type USIA ou un comité de coordination interagences (Active Measures Working Group [AMGW]) est devenue criante bien avant les soupçons d'une intervention russe dans le processus électoral américain de 2016. Elle se faisait déjà sentir, pour des raisons d'efficacité, dans la lutte contre la propagande djihadiste notamment. Cependant, ces velléités à Washington, encouragées par les nouveaux combattants de la désinformation, traduisent une lecture des enjeux contemporains parfois trop inspirée de l'expérience de guerre froide des années 1980, et semblent omettre les dérives qui ont pu l'accompagner, dans des moments de tensions, comme lorsqu'il s'est agi d'user des armes de l'adversaire et donc de pratiquer ouvertement une guerre de l'information.

50. U.S. Department of Justice, *Report of the Attorney General's Cyber-Digital Task Force*, 2018, p. 8.

51. Ellen Nakashima, « NSA and Cyber Command to coordinate actions to counter Russian election interference in 2018 amid absence of White House guidance », *The Washington Post*, 17 juillet 2018.

En 2016, le Congrès avait autorisé le remplacement du Center for Strategic Counterterrorism Communications (CSCC) par le Global Engagement Center (GEC) au sein du département d'État pour lutter essentiellement contre la propagande de Daech et privilégier une stratégie adaptée au nouvel environnement informationnel. L'idée en était de favoriser la coordination d'un grand nombre d'acteurs publics ou privés (agences paragouvernementales, ONG, entreprises) au niveau national et international. Ses partisans les plus fervents ont voulu en faire, très rapidement, le principal organe de réponse aux activités subversives du Kremlin[52], mais ils se sont heurtés à la complexité de l'appareil bureaucratique américain. Le *National Defense Authorization Act* de 2017 (NDAA), devait en effet étendre les prérogatives et les missions du GEC à des activités visant à contrer les propagandes d'États comme la Russie, la Chine, l'Iran et la Corée du Nord.

Or, cette entité interagences, qui n'a cessé de se complexifier ces derniers mois, ne représente qu'une dimension de la nature plurielle de la réponse. Les multiples stratégies qui en découlent sont encore appelées *talk-back* par les uns, dans une logique de guerre froide, ou *stratcom* par les autres. Les éléments d'information apportés aux débats contemporains concernant les capacités d'influence et de contre-propagande américaines ont présenté une vision parfois trop cloisonnée des programmes de diplomatie publique d'une part, et des opérations d'information militaires (IO) d'autre part. Elles constituent pourtant deux facettes distinctes du dispositif de communication stratégique américain.

Au bilan, l'Active Measure Working Group représente la dernière occurrence d'une coordination effective de la réponse. Sur son modèle, les professionnels de la diplomatie publique, militaires ou civils, ont préconisé, au cours du travail d'enquête parlementaire post-électoral de 2017 :

– la création ou le renforcement d'une structure réunissant l'ensemble des acteurs gouvernementaux, paragouvernementaux, publics et privés (Pentagone, département d'État, agences, CIA, NSA, grandes entreprises du GAFAM, acteurs privilégiés des mutations des guerres de l'information) ;

– l'insistance sur la nécessité de moderniser la diplomatie publique. Le virage numérique annoncé par le département d'État dès la fin du second mandat de George W. Bush, n'a pas été un succès, et les coopérations

52. Le *National Defense Authorization Act* devait étendre les missions du GEC en en faisant un organisme de lutte contre « la propagande d'État », qu'elle soit russe, chinoise, iranienne ou nord-coréenne.

public-privé, enclenchées à cette époque et fortement développées par les multiples initiatives menées par Hillary Clinton (avec les GAFAM) alors qu'elle dirigeait le département d'État, auraient nécessité d'être poursuivies.

Sur cette base, les opérationnels, diplomates ou militaires, préconisent de faire du GEC un équivalent de l'Office of the Director of National Intelligence afin de coordonner le travail interagences et de synchroniser les actions. Pour organiser la riposte dans les guerres de l'information 3.0, il serait nécessaire, selon eux, de favoriser une approche globale impliquant et rassemblant l'ensemble des acteurs institutionnels autour d'une stratégie commune[53].

Les recommandations formulées au cours des auditions parlementaires ou dans les rapports des think tanks (Atlantic Council, Brookings) soulignent le rôle primordial du responsable de cette entité interagences dans le processus de décision du conseil de sécurité nationale. Le responsable de cette entité pourrait se voir accorder un rôle au plus haut sommet de l'État en tant que sous-secrétaire d'État ou conseiller spécial. En effet, sans une coopération étroite entre le président et le directeur de l'organisme responsable de l'élaboration des stratégies de diplomatie publique, le manque de cohérence des réponses apportées aux « mesures actives » contemporaines du Kremlin risque de demeurer patent. Pour mémoire, les administrations Kennedy et Reagan avaient choisi des hommes de médias reconnus ou influents (le journaliste Edward Murrow de CBS ou le producteur hollywoodien, Charles Wick). Proches du président, les directeurs de l'Agence d'information comme de la CIA étaient alors associés au Conseil de sécurité nationale (NSC), notamment en temps de crises sécuritaires majeures, durant lesquelles la maîtrise de la communication stratégique s'est avérée cruciale (crise de Cuba ou crise des euromissiles).

Or, la nomination de Mike Pompeo, ancien directeur de la CIA, à la tête du département d'État, pourrait selon les agents du Foreign Service, représenter une opportunité pour renforcer la coopération interagences et le partage d'informations dans la lutte contre les manipulations de l'information. Pour l'heure, la volonté de l'administration Trump a bien été de renforcer le rôle du GEC en sanctuarisant finalement son budget pour l'année fiscale 2018 (via 40 millions transférés du département de Défense au GEC). Ceci a permis la création de l'*Information Access Fund* (depuis février), à savoir un fond de soutien aux initiatives citoyennes, entrepreneuriales (GAFA) ou paragouvernementales (ONG).

53. Michael Lumpkin, coordinateur nommé par Barack Obama en 2016, ex-secrétaire d'État adjoint pour les opérations spéciales.

III. Les organisations internationales

A. L'Union européenne

Les phénomènes de manipulation de l'information ont fait l'objet dans l'Union européenne d'une prise en compte progressive et d'abord relativement éclatée entre institutions. Le sujet a initialement été appréhendé sous l'angle des relations extérieures de l'Union et de la nécessité de protéger l'image de l'UE dans son voisinage oriental. Les conclusions du Conseil européen des 19-20 mars 2015 soulignaient ainsi « la nécessité de contrer les campagnes de désinformation menées par la Russie » et invitaient la haute représentante à élaborer un plan d'action sur la communication stratégique[54].

C'est pour répondre à cette préoccupation que la division « communication stratégique » du Service européen pour l'action extérieure (SEAE) a créé trois pôles, incarnés dans trois équipes, qui reflètent des priorités géographiques : la plus ancienne et la mieux dotée est la « *task force* de communication stratégique orientée vers le voisinage oriental » (East StratCom Task Force). Elle a commencé ses activités en septembre 2015 et s'est fixé trois objectifs principaux : 1) la veille, en collaboration avec la société civile et avec d'autres institutions européennes, tel le centre du renseignement INTCEN ; 2) la lutte contre la désinformation, en favorisant la prise de conscience du phénomène auprès des consommateurs de nouvelles ; 3) le renforcement de médias indépendants et visant l'objectivité dans le voisinage oriental.

Les promoteurs de la East StratCom Task Force prennent soin de préciser qu'« il ne s'agit pas de faire de la contre-propagande[55] ». Son travail est diffusé 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*). Son slogan est *Don't be deceived: question even more*, en référence au slogan de RT (*Question More*). Sa page en russe serait assez fréquentée car elle concentre à elle seule le quart du trafic du site du SEAE[56]. Depuis 2017, elle avait déjà recensé plus de 2 500 cas, en 18 langues, de désinformation, c'est-à-dire d'« histoires contredisant des faits publiquement disponibles[57] ». Elle a d'abord dû convaincre de l'importance du sujet :

54. Conseil européen, Note de transmission du secrétariat général aux délégations au sujet de la réunion du Conseil européen (19-20 mars 2015), EUCO 11/15, 20 mars 2015.

55. « L'UE crée une équipe pour contrer la propagande russe », *Le JDD*, 31 août 2015.

56. Philippe Regnier, « Tacler la désinfo russe », *Le Soir*, 24 novembre 2016, p. 12.

57. « Cybermenaces et désinformation : les pays occidentaux se mobilisent », AFP, 16 février 2017.

> Quand nous avons commencé en septembre 2015, explique l'un de ses représentants, c'était déprimant parce qu'on avait l'impression que 95 % des gens à Bruxelles ne croyaient pas à la propagande russe et le 5 % restant disait que la menace n'était pas sérieuse. Maintenant, la situation est différente et la plupart des gens à Bruxelles la voient bien comme une menace. Nous voyons que l'intérêt pour le sujet monte, davantage de médias écrivent dessus, davantage d'États prennent des mesures, etc.[58].

En dépit de ces résultats, cette *task force* manque de moyens humains et financiers. Composée de seulement quatorze personnes, elle n'existe et ne survit que grâce à la volonté d'une poignée d'États membres, qui la financent et lui prêtent du personnel. Les institutions européennes ne semblaient pas, jusqu'à une date récente, très investies, et il est parfois reproché au SEAE de ne pas prendre la menace de la désinformation russe au sérieux. Ces difficultés témoignent surtout de la désunion européenne sur la question.

Les approches vis-à-vis de la désinformation demeurent en effet contrastées en Europe, du fait de perceptions divergentes sur la menace. Le think tank praguois European Values distribue les États dans un classement annuel constitué de cinq groupes[59] : en tête figurent les États baltes, le Royaume-Uni et la Suède, qui sont les plus offensifs. Ils sont suivis par le Danemark, l'Espagne, la Finlande, la France, les Pays-Bas, la Pologne, la République tchèque et la Roumanie qui, pour des raisons diverses et parfois récentes, sont sensibilisés et prennent la menace au sérieux. Vient ensuite un groupe d'États qualifiés d'« hésitants » (Belgique, Bulgarie, Croatie, Irlande, Slovaquie), puis ceux considérés comme étant « dans le déni » (Autriche, Hongrie, Italie, Luxembourg, Malte, Portugal, Slovénie). En queue de peloton arrivent enfin Chypre et la Grèce, qui non seulement ne font rien pour lutter contre la menace, mais bloquent même systématiquement tout effort européen sur le sujet. Le parlement européen « est préoccupé par le fait que certains États membres sont peu conscients de constituer des publics et des espaces de propagande et de désinformation » et il insiste sur « la nécessité de favoriser la sensibilisation[60] ».

Les deux autres équipes de la division « communication stratégique » du SEAE sont une *task force* « Sud », créée en 2015 et composée de quatre personnes, qui lutte contre le discours djihadiste, et une *task force* « Balkans

58. Cité par Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 76.

59. *2018 Ranking of countermeasures by the EU28 to the Kremlin's subversion operations*, European Values, 13 juin 2018.

60. Parlement européen, résolution du 23 novembre 2016, *op. cit.*

occidentaux », mise en place plus récemment, en juillet 2017, composée de trois agents, qui se concentre sur la défense de l'image de l'UE dans la région.

Dans une résolution de juin 2017, le parlement européen « demande à la Commission d'analyser en profondeur la situation et le cadre juridique actuels en ce qui concerne les fausses informations et de vérifier la possibilité d'une intervention législative afin de limiter la publication et la diffusion de faux contenus[61] ». Fin 2017, la Commission s'est donc saisie de la question au titre de ses activités pour une société numérique européenne, sous l'autorité de la commissaire pour l'économie et la société numériques, Mariya Gabriel. Elle a ainsi constitué un groupe d'experts qui a rendu son rapport le 12 mars 2018, préconisant d'accroître la transparence des contenus en ligne, de promouvoir l'éducation aux médias et de développer la recherche et le partenariat avec la société civile[62].

La Commission européenne a ensuite publié le 26 avril 2018 une communication sur la lutte contre la désinformation, sur la base du rapport mais aussi d'une consultation publique[63]. La communication propose l'élaboration d'ici juillet 2018, sous les auspices d'un forum réunissant les acteurs du numérique et des représentants des médias et de la société civile, d'un « code de bonnes pratiques contre la désinformation » afin de promouvoir les mesures de vérification et d'autorégulation.

Ce code, publié le 17 juillet 2018, s'articule autour des cinq champs d'action suivants : 1) améliorer la surveillance des placements publicitaires afin de réduire l'attrait économique de la désinformation ; 2) garantir la transparence des publicités politiques ou thématiques afin de permettre aux utilisateurs d'identifier rapidement les contenus orientés ; 3) garantir l'intégrité des services délivrés par les plateformes numériques en identifiant et supprimant les faux comptes et en ayant recours aux mécanismes appropriés pour signaler les interactions automatisées (bots) ; 4) faciliter pour les utilisateurs la découverte et l'accès à des sources d'information différentes offrant des points de vue alternatifs ; 5) renforcer le pouvoir des communautés de recherche en leur donnant accès aux données des plateformes nécessaires pour pouvoir analyser de manière continue la désinformation en ligne. Le comité consultatif du Forum formulera un premier avis début septembre 2018 et adoptera une

61. Parlement européen, résolution du 15 juin 2017, sur les plateformes en ligne et le marché unique numérique, P8_TA(2017)0272, para. 36.

62. *A multi-dimensional approach to disinformation, Report of the independent High-Level Group on fake news and online disinformation,* mars 2018.

63. Communication de la Commission au parlement européen, au Conseil, au Conseil économique et social et au Comité des régions, *Lutter contre la désinformation : une approche européenne*, Bruxelles, 26 avril 2018, COM(2018) 236 final.

version finale de ce code à la fin du même mois. Ce code sera ensuite évalué par la Commission fin 2018, cette dernière se réservant la possibilité de décider de l'opportunité de mesures additionnelles. La Commission exprime aussi son intention de veiller à la sécurisation des processus électoraux, notamment dans la perspective des élections européennes de 2019, en lien avec les États membres à qui échoit cette responsabilité première. À ce stade cependant, aucune mesure législative n'est annoncée, et il est probable qu'aucune proposition législative n'émanera de la Commission d'ici la fin de la législature.

Le budget européen de 2018 prévoit de consacrer davantage de fonds à la communication stratégique, dont 1,1 million d'euros pour contrer la désinformation (débloqué en juillet 2018 pour les StratCom *task forces)*. De plus, une partie des fonds dédiés au programme Horizon Europe (ex-Horizon 2020) sera dédiée à la recherche dans les domaines de l'intelligence artificielle et des algorithmes, pouvant contribuer à la lutte contre la désinformation.

Transparence, diversité, crédibilité et approche inclusive

« De l'avis de la Commission, les mesures pour lutter contre la désinformation devraient être guidées par les principes et objectifs généraux suivants :

• Premièrement, améliorer la transparence en ce qui concerne l'origine des informations, et la manière dont elles sont produites, sponsorisées, diffusées et ciblées afin de permettre aux citoyens d'évaluer les contenus auxquels ils accèdent en ligne et de révéler d'éventuelles tentatives de manipulation de l'opinion.

• Deuxièmement, favoriser la diversité des informations, pour permettre aux citoyens de prendre des décisions éclairées guidées par l'esprit critique, en soutenant le journalisme de qualité, l'éducation aux médias et le rééquilibrage de la relation entre les créateurs et les diffuseurs d'informations.

• Troisièmement, promouvoir la crédibilité des informations en fournissant une indication sur leur fiabilité, notamment à l'aide de signaleurs de confiance, et en améliorant la traçabilité des informations et l'authentification des fournisseurs d'informations influents.

• Quatrièmement, élaborer des solutions inclusives. La sensibilisation des utilisateurs au problème, une extension de l'éducation aux médias, une large mobilisation des parties prenantes et la coopération des pouvoirs publics, des plateformes en ligne, des annonceurs, des signaleurs de confiance, des journalistes et des médias sont nécessaires pour parvenir à des solutions efficaces à long terme. »

(Commission européenne, Communication de la commission au parlement européen, au Conseil, au Comité économique et social européen et au Comité des régions. *Lutter contre la désinformation en ligne : une approche européenne*, Bruxelles, 24 avril 2018, COM(2018) 236 final, p. 8-9.)

Enfin, le centre de renseignement et de situation de l'UE (INTCEN) se penche de manière approfondie sur la désinformation, perçue avant tout comme une menace venant de la Russie. Cette question soulève d'ailleurs un enjeu plus général d'influence dans les instances européennes, où les postes numéros deux et trois, pourtant très importants (pouvoir de nomination et de budget), sont souvent recherchés et occupés par les Britanniques. À ce sujet, le Brexit va amorcer une reconfiguration intéressante.

Pour les acteurs de l'INTCEN, les efforts d'influence de puissances étrangères, dont les manipulations de l'information ne sont qu'un volet, sont jugées efficaces, en partie parce qu'ils reposent sur la stratégie de « ballons d'essais / tirs dans le tas » qui par définition ne peut être perdante car elle demeure fondamentalement non coûteuse.

La stratégie d'INTCEN consiste avant tout à échanger, sensibiliser et décloisonner. En mettant en place un réseau d'échange d'informations, INTCEN est en mesure d'augmenter le niveau d'alerte (*awareness*) et d'affiner les grilles de lecture des acteurs pour qu'ils perçoivent mieux les efforts d'influence. Pour cela, il a mis en place plusieurs changements organisationnels : tenue de rendez-vous réguliers avec les différents acteurs pertinents (East StratCom TF, correspondants nationaux, OTAN), création de la Hybrid Threat Fusion Cell développée pour se consacrer de manière transversale aux menaces plus spécifiquement « hybrides », alerte auprès des États attaqués (aider et non pointer les faiblesses), etc. La Hybrid Threat Fusion Cell met l'accent plus particulièrement sur l'importance de réfléchir avec un coup d'avance et sans préconceptions. Sa priorité est avant tout de protéger les infrastructures critiques des États membres, d'où l'importance d'avoir des correspondants nationaux.

La Hybrid Threat Fusion Cell de l'INTCEN est composée de sept membres et son approche est avant tout politique. Elle travaille avec trois sources d'informations : les sources ouvertes – et donc en lien avec la société civile, think tanks, ONG ; les États membres directement (ex : affaire Lisa) ; les institutions dédiées (East Stratcom Task Force, centre d'excellence d'Helsinki).

Le Parlement européen contre la propagande hostile

Le Parlement européen « 1. souligne que la propagande hostile contre l'Union européenne prend diverses formes et utilise divers outils, souvent conçus de façon à correspondre au profil des États membres, dans le but de déformer la vérité, d'instiller le doute, de diviser les États membres, d'entraîner un découplage stratégique entre l'Union européenne et ses partenaires d'Amérique du Nord, de paralyser le processus décisionnel, de discréditer les institutions de l'Union et les partenariats transatlantiques – dont le rôle dans l'architecture de sécurité et économique européenne est reconnu – aux yeux et dans l'esprit des citoyens de l'Union et des pays voisins, et de saper le discours politique européen fondé sur des valeurs démocratiques, les droits de l'homme et l'état de droit ; rappelle que l'un des principaux outils utilisés est l'incitation à la peur et à l'incertitude chez les citoyens de l'Union, ainsi que l'exagération de la puissance des acteurs étatiques et non étatiques hostiles ;
2. demande aux institutions de l'Union de reconnaître que la communication stratégique et la guerre d'information ne sont pas seulement un problème externe, mais aussi interne, à l'Union et s'inquiète des nombreux relais dont dispose la propagande hostile à l'Union en son sein ; est préoccupé par le fait que certains États membres sont peu conscients de constituer des publics et des espaces de propagande et de désinformation ; demande à cet égard aux acteurs de l'Union de remédier à l'actuel manque de clarté et au désaccord sur ce qui doit être considéré comme de la propagande et de la désinformation et, en coopération avec des représentants et des experts des médias des États membres de l'Union, d'élaborer un ensemble commun de définitions et de regrouper des données et des faits sur l'utilisation de la propagande ».

(Extrait de la résolution du Parlement européen du 23 novembre 2016 sur la communication stratégique de l'Union visant à contrer la propagande dirigée contre elle par des tiers.)

B. L'OTAN

L'Alliance atlantique a une longue expérience sur ces questions, ayant été confrontée pendant la guerre froide aux tactiques soviétiques de « guerre psychologique » utilisant des « mesures actives ». Encore aujourd'hui, l'Alliance appréhende le phénomène principalement sous l'angle de la menace en provenance de Russie. La vulnérabilité de l'Alliance à cette menace est accrue par sa présence militaire de réassurance à l'Est, cible privilégiée de tentatives de manipulation de l'information tendant à exagérer le volume et la nature de la présence militaire de l'OTAN dans les États baltes et en Pologne notamment (voir *supra*). D'autres tentatives de diffusion de rumeurs sur des crimes qui auraient été commis par des soldats allemands sous commandement OTAN en Lituanie ont été détectées.

La stratégie de réponse de l'OTAN dans ce domaine comporte trois volets principaux : la détection, en provenance des nations ou de l'intérieur de la structure de l'Alliance (cellules chargées de la communication stratégique au sein de la présence avancée de l'OTAN à l'Est par exemple) ; l'analyse de l'origine et du contenu ; et la réaction, en opposant des faits objectifs à la tentative de désinformation et en en assurant une large diffusion.

Au cœur de ce diapositif figure le centre d'excellence de l'OTAN sur la communication stratégique (NATO StratCom COE), créé en 2014 à Riga. Il travaille notamment sur les doctrines, les opérations et la formation, et publie un grand nombre d'analyses. La Division Diplomatie publique (PDD) du secrétariat international, à Bruxelles, joue avant tout un rôle de coordination, en faisant notamment le lien avec les nations et les organisations dédiées, qu'elles soient affiliées à l'OTAN (comme le Riga StratCom COE mais aussi le plus récent centre d'excellence contre les menaces hybrides d'Helsinki) ou non (la East StratCom Task Force du SEAE), ainsi qu'avec la société civile engagée sur le sujet. Une équipe d'une dizaine de personnes à PDD suit les tentatives de désinformation avec des outils dédiés.

L'Alliance a ainsi sur son site internet une page dédiée à la réfutation des accusations de la Russie à son égard, qualifiées de « mythes », sur le mode de la correction (une longue liste d'« allégations » systématiquement suivies d'une réponse commençant par « Dans les faits… »). PDD en diffuse une version abrégée sous la forme d'une fiche d'information sur « Les cinq principaux mythes entretenus par la Russie au sujet de l'OTAN ». L'Alliance a également le souci d'objectiver le débat, en publiant des

preuves (notamment des photos satellitaires montrant l'implication de la Russie en Ukraine).

La position française qui limite le rôle de l'OTAN dans ce domaine à la détection, l'analyse et la riposte concernant ses propres activités (et non les tentatives de désinformation et de déstabilisation dans leur ensemble) fait l'objet d'un large consensus au sein de l'Alliance. Des lignes de fracture apparaissent néanmoins entre les alliés sur la question de la posture de riposte et sur l'opportunité de « prendre la Russie à son propre jeu » en semant le doute, y compris auprès de publics russophones, sur les activités et les intentions de Moscou ou en proposant une relecture de certains chapitres de l'histoire. Cette posture est cependant loin de faire l'unanimité au sein de l'Alliance, où des divergences subsistent par ailleurs sur l'appréciation de la menace, reflétant en partie des différences d'analyse entre alliés sur le rôle de la Russie et la posture à adopter par l'OTAN face à Moscou.

C. L'OSCE

Les instances de l'OSCE doivent tenir compte des positions de l'ensemble des États participants, y compris de la Russie, ainsi que des situations très contrastées dans la zone OSCE en matière de respect de l'état de droit et des droits fondamentaux, dont la liberté d'expression.

Il n'existe pas à l'OSCE d'engagements spécifiques sur la lutte contre la propagande, qui s'inscrive dans le cadre des engagements sur la liberté d'expression, à l'exception de l'Acte final d'Helsinki qui aborde l'enjeu spécifique de la « propagande de guerre ou de haine ». Le Représentant de l'OSCE pour la liberté des médias, actuellement Harlem Désir, aborde ces questions sous l'angle du respect de la liberté d'expression, mettant l'accent sur la transparence des sources, le pluralisme des médias et l'éducation aux médias. Cela le conduit, par exemple, à s'opposer à la pénalisation de la désinformation, qui peut être une voie de répression de la liberté d'expression dans des régimes autoritaires.

En mars 2017, la Représentante de l'OSCE pour la liberté des médias, le Rapporteur spécial des Nations unies sur la liberté d'opinion et d'expression, le Rapporteur spécial de l'Organisation des États américains sur la liberté d'expression et le Rapporteur spécial sur la liberté d'expression et l'accès à l'information de la Commission africaine des droits de l'homme et des peuples ont publié une déclaration conjointe sur la liberté d'expression

et les « fausses nouvelles », la désinformation et la propagande[64]. L'objectif de ce texte est notamment de rappeler aux États que la lutte contre la désinformation ne doit pas devenir un prétexte pour restreindre les libertés publiques, en l'occurrence la liberté d'expression, au-delà de ce que le droit international prévoit.

IV. La société civile

La société civile est en première ligne face aux manipulations de l'information. Quelles que soient les mesures mises en œuvre par les États, le degré de résilience d'une société dépend en premier lieu de la mobilisation de ses citoyens. Les réponses ont d'abord été ponctuelles et réactives, avec la vérification des faits (*fact-checking*). Compte tenu des limites intrinsèques à cette méthode, la société civile a développé des initiatives complémentaires car de plus long terme, normatives ou impliquant la recherche.

A. La vérification des faits

La vérification de la véracité des faits est la réponse la plus naturelle aux fausses nouvelles, et donc la plus répandue. Il y aurait au moins 149 sites de vérification des faits actifs en 2018[65], et tous ne sont pas récents : l'un des plus anciens est le site américain Snopes, lancé en 1994, qui est depuis devenu une référence – tout comme un autre site américain, PolitiFact, créé en 2007, qui a gagné le Prix Pulitzer en 2009 pour son analyse de la campagne présidentielle de 2008. La tendance se généralise partout dans le monde, jusqu'à certains États : en Malaisie, par exemple, la Communications and Multimedia Commission a lancé en mars 2017 un portail de vérification des faits (sebenarnya.my). La vérification gouvernementale a toutefois une efficacité discutable puisque les personnes susceptibles de croire et diffuser de fausses nouvelles sont généralement celles-là mêmes qui n'ont pas confiance dans les institutions publiques. Ce genre de site peut même avoir l'effet pervers de confirmer les théories conspirationnistes et d'encourager les narratifs du type « ministère de la vérité ». Il est assez consensuel de considérer qu'autant que possible, l'État

64. *Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda*, 3 mars 2017.

65. Selon le Reporters'Lab, un centre de recherche sur le journalisme de la Sanford School of Public Policy de Duke University, aux États-Unis, qui tient à jour un inventaire des sites de vérification des faits dans le monde (reporterslab.org/fact-checking/).

ne doit pas se mêler de vérification des faits, sauf bien entendu en cas de crise menaçant l'ordre public.

C'est donc au sein de la société civile que les initiatives prolifèrent. Les médias, en particulier, sont progressivement passés de la production à la vérification d'informations – ce qui constitue en soi une évolution importante du journalisme des dix dernières années. Les grands médias ont développé leurs propres sites de vérification des faits (AFP Fact Check, Reality Check de la BBC, Decodex du *Monde*, rubrique « Hoax or not » du site indonésien Detik, etc.) ; Google a lancé CrossCheck, un dispositif associant plus d'une trentaine d'entreprises de presse françaises. Certains projets ont évolué et ne se limitent plus à la vérification des faits, comme le site ukrainien StopFake, créé en 2014 par des enseignants, des étudiants et des diplômés de l'école de journalisme Mohyla, qui est aujourd'hui devenu un site d'analyse de référence sur la propagande du Kremlin. Le réseau international de vérificateurs de faits de l'Institut Poynter a adopté un « code » de principes communs pour garantir une vérification transparente et non partisane[66].

En Irlande, lors du référendum sur le huitième amendement et dans l'optique de lutter contre l'activité des comptes automatisés anti-avortement, un groupe de bénévoles pro-abrogation a créé le Repeal Shield, un instrument permettant de bloquer une liste de plus 16 000 comptes qualifiés de « trolls, bots et faux comptes déversant des mensonges et des messages haineux ». Plus de 4 500 utilisateurs y ont eu recours durant la campagne référendaire[67].

La vérification des faits fonctionne notamment en raison de son potentiel d'humiliation pour les personnes qui sont des relais de fausses nouvelles non pour des raisons idéologiques mais des raisons réputationnelles, d'ego (elles veulent être les premières à apprendre des choses aux autres) : ces personnes seront humiliées dans leur cercle si la nouvelle diffusée se révèle fausse.

Cependant, la vérification des faits a aussi de nombreuses limites structurelles. Premièrement, le cerveau humain est relativement résistant à la correction. Les études montrent que la correction d'une croyance préalable n'est généralement pas efficace : la plupart des gens continuent d'utiliser en tout ou partie une information dont ils reconnaissent pourtant la fausseté. C'est un phénomène connu en psychologie sous le nom d'effet

66. *Code of principles*, International Fact-Checking Network (IFCN), Poynter.

67. Rachel Lavin et Roland Adorjani, « L'Irlande a déjà trouvé la parade aux *fake news* (mais on ne pourra pas la reproduire) », *op. cit*.

d'influence continue (*continued-influence effect*)[68]. Et il est d'autant plus fort que les croyances réfutées sont profondément ancrées : la vérification des faits fonctionne mieux sur les sujets nouveaux, ne suscitant pas d'idées préconçues. Le problème bien entendu est que « les fausses informations concernent aujourd'hui essentiellement des thèmes politiques qui reflètent des convictions idéologiques profondes[69] ».

Ensuite, la vérification des faits est par définition un outil d'après-coup : sa nature corrective signifie qu'il n'arrive que lorsque le mal est fait, après la diffusion de la fausse nouvelle. S'il permet de dénoncer ce qui est faux, tronqué ou fabriqué tout en faisant œuvre de pédagogie, il n'efface pas l'impact psychologique important associé à la lecture d'une fausse nouvelle.

Par ailleurs, il n'atteint pas toujours, voire pas souvent, sa cible, c'est-à-dire que la correction n'est en général pas lue par les personnes qu'il s'agissait de convaincre : « les audiences les plus susceptibles d'être influencées par la désinformation russe pourraient aussi être les moins susceptibles de consommer régulièrement ou même d'accéder à des sites contrant la désinformation[70] ». « Puisque les *fake news* sont le signe d'une défiance populaire à l'égard des élites politiques et intellectuelles, comment leur vérification par ces mêmes élites peut-elle réussir à convaincre ceux qui les propagent[71] ? »

Enfin, il y a aussi le risque que la vérification des faits devienne elle aussi un marché, dont se saisissent un nombre croissant d'acteurs (ONG, médias mais aussi plateformes digitales comme Facebook) : la logique du gain et/ou la volonté d'apparaître vertueux prennent parfois le pas sur la recherche de vérité, ce qui tend à décrédibiliser aux yeux de certains le recours à l'outil. Sans compter que cet outil est parfois détourné par ceux-là mêmes qui diffusent le plus de fausses nouvelles : RT a par exemple lancé un FakeCheck en quatre langues.

Toutes ces limites ne signifient pas que la vérification des faits n'est pas importante : elle est absolument nécessaire, mais aussi insuffisante. C'est un soin palliatif, qui doit être complété par d'autres mesures.

---

68. Stephan Lewandowsky *et al.*, « Misinformation and its correction: Continued influence and successful debiasing », *Psychological Science in the Public Interest*, 13:3, 2012, p. 106-131.

69. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 50.

70. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 76-77.

71. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 48.

B. Initiatives normatives

Nous consommons des informations comme nous consommons de la nourriture. Les deux sont potentiellement bénéfiques et néfastes. Il faut donc faire un tri. De ce point de vue, la lutte contre les manipulations de l'information peut s'inspirer de l'étiquetage nutritionnel. C'est ce que certains appellent le « modèle Michelin[72] » : des labels, index et classements permettant de distinguer les médias sérieux des autres. En 2014 déjà, Pomerantsev et Weiss recommandaient la création d'un classement international de la désinformation s'inspirant de la méthodologie des classements de Freedom House ou Transparency International[73].

Plusieurs initiatives sont en cours, dont un projet d'index global (disinformationindex.com). La plus prometteuse est sans doute l'initiative pour la confiance dans le journalisme (*Journalism Trust Initiative*) de Reporters sans frontières (RSF). Le président Macron l'avait évoquée pour la soutenir dans ses vœux à la presse du 3 janvier 2018 (« une forme de certification des organes de presse respectant la déontologie du métier me paraît à cet égard non seulement intéressante, mais souhaitable »). RSF l'a officiellement lancée trois mois plus tard, le 3 avril, avec ses partenaires, l'agence France-Presse, l'Union européenne de radio-télévision et le Global Editors Network. Plutôt que d'identifier et blâmer les désinformateurs, il s'agit de « renverser la logique en donnant un avantage réel à tous ceux qui produisent des informations fiables, quel que soit leur statut », explique son secrétaire général Christophe Deloire, et de décerner un label de qualité aux médias qui le méritent, c'est-à-dire qui respectent un certain nombre de critères tels que l'indépendance éditoriale, la transparence ou la déontologie[74]. Les médias seraient alors incités à les satisfaire afin de rasséréner les annonceurs publicitaires qui recherchent des environnements stables et non contestés. Les plateformes digitales pourraient, à terme, décider de valoriser les contenus de qualité en mettant en avant dans leurs algorithmes les médias certifiés. L'approche de RSF se veut donc incitative.

72. Voir Clint Watts and Andrew Weisburd, « Can the Michelin Model Fix Fake News? », *The Daily Beast*, 22 janvier 2017.

73. Peter Pomerantsev et Michael Weiss, *The Menace of Unreality*, *op. cit.*, p. 40.

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

C. La recherche

Les think tanks et les universités s'emparent également du sujet. Pour ne citer que quelques exemples, le think tank tchèque European Values organise depuis 2016 un StratCom Summit à Prague qui est l'un des rendez-vous annuels les plus importants du secteur. Le dernier en date, en avril 2018, a réuni 200 experts, gouvernementaux et de la société civile, d'une trentaine d'États. Aux États-Unis, l'Atlantic Council a mis en place une structure dédiée, le Digital Forensic Research Lab (DFRLab), qui est vite devenue une référence. Ce laboratoire, qui travaille étroitement avec l'équipe de Bellingcat, une plateforme d'investigation digitale, assure un rôle important de détection et d'enquête sur les principales campagnes de désinformation. À Bruxelles, le EU Disinfo Lab produit également des analyses remarquées. Signalons enfin l'Alliance for Securing Democracy (ASD), une organisation transatlantique bipartisane dont l'objectif est de répondre aux ingérences russes dans les processus démocratiques aux États-Unis et en Europe. Créée en juillet 2017 par d'anciens hauts fonctionnaires des services de renseignement américains et du département d'État, elle est hébergée au German Marshall Fund. L'ASD est surtout connu pour son tableau de bord « Hamilton 68 » qui suit 600 comptes Twitter liés au réseau d'influence russe et met donc en évidence, en temps réel, les thèmes et hashtags promus par le Kremlin[75]. C'est un outil intéressant pour la recherche. Un équivalent en allemand a été lancé en septembre 2017.

L'université n'est pas en reste, notamment au Royaume-Uni : l'université d'Oxford a un projet de recherche *Computational Propaganda* ; King's College London s'est doté d'un Centre for Strategic Communications ; la London School of Economics d'un programme (appelé Arena) pour « répondre aux défis de la désinformation », au sein de l'Institute of Global Affairs, etc. Ailleurs dans le monde, on peut également citer le Cyber News Verification Lab de l'université de Hong Kong et l'université de Lund qui travaille étroitement avec le MSB suédois.

75. GMF - Alliance for Security Democracy, Hamilton 68, Tracking Russian Influence Operations on Twitter.

Décrédibiliser la désinformation grâce aux sources ouvertes

La profusion et la vitesse des informations sur internet est tout à la fois ce qui fait de la désinformation un problème plus grave qu'auparavant, et ce qui fournit des armes pour lutter contre elle. Il est en effet possible de récolter, en sources ouvertes, un grand nombre d'informations vérifiables et de les utiliser pour déconstruire de fausses nouvelles. C'est ce que montre le rapport du SCRS avec l'exemple de la Syrie[76].

Accusé de bombarder les civils en Syrie, le Kremlin répond en utilisant « trois stratégies : 1. Nier les faits […] 2. Militariser les victimes […] Moscou et Damas ont réussi à donner l'impression que tous les groupes qu'ils prenaient pour cible étaient des extrémistes. 3. Attaquer les témoins […] dont l'un des plus importants était l'organisation d'aide humanitaire d'abord appelée Défense civile syrienne, mais vite surnommée "Casques blancs" ». Les Casques blancs ont notamment publié des photos de fragments de bombes à sous-munitions incendiaires que Moscou nie utiliser. Parfois, c'est la communication du Kremlin elle-même qui laisse passer des informations compromettantes : le 18 juin 2016, par exemple, dans un reportage de RT sur la visite du ministre russe de la Défense à la base aérienne de Hmeimim, on pouvait voir des bombes à sous-munitions incendiaires RBK 500 ZAB-2,5S/M sous un bombardier Su-34. Cette partie de la vidéo a été coupée et est donc absente de la version désormais disponible sur YouTube.

L'hyperconnectivité est donc à la fois le problème et une partie de la solution, en donnant accès à une masse considérable d'informations et en permettant au journalisme citoyen de mener des enquêtes approfondies (comme en font des sites comme Bellingcat.com par exemple). Cette démarche qui permet « aux gens non seulement de découvrir des informations sur la guerre de Poutine en Syrie, mais aussi de les vérifier eux-mêmes » est « aux antipodes de la campagne de désinformation opaque de la Russie, qui repose sur des discours idéologiques plutôt que sur des faits vérifiables ». Un exemple de la puissance du journalisme collaboratif en est la brillante enquête du *New York Times* – menée notamment avec le groupe d'investigation Bellingcat – qui prouve la responsabilité du régime el-Assad dans l'attaque chimique de Douma[77].

76. SCRS, *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui : points saillants de l'atelier*, *op. cit.*, chap. 6. Les citations suivantes en sont tirées.

77. Malachy Browne *et al.*, « One building, One Bomb: How Assad Gassed His Own People », *The New York Times*, 2018.

D. Les mouvements citoyens (*grassroots initiatives*)

Plusieurs réponses citoyennes intéressantes sont nées dans les États baltes, qu'elles soient individuelles, comme la campagne hashtag #Кремльнашуисториюнеперепишешь (*#Kremlin you will not falsify our history*) lancée par le Lituanien Andrius Tapinas, ou collectives, comme les tribus d'« elfes » (par opposition aux trolls), originaires de Lituanie, qui seraient environ 4 000 dans toute la région.

E. Les journalistes

Les journalistes sont naturellement en première ligne du combat contre les manipulations de l'information et, bien souvent, ils participent, voire sont à l'initiative, de certaines des actions précédentes, notamment la vérification des faits. Certains d'entre eux se sont également distingués, à titre individuel, comme la Finlandaise Jessikka Aro qui a étudié les usines à trolls et l'Allemand Julian Röpcke qui s'intéresse à l'influence russe en Allemagne. Ou encore collectivement, en créant des groupes comme le Baltic Center for Media Excellence dont l'objectif est d'accroître les standards journalistiques et l'environnement médiatique dans les pays du partenariat oriental ; ou comme le portail Re:baltica et la startup Toneboard qui a reçu une bourse de Google pour créer une plateforme de vérification de la véracité des nouvelles.

La difficulté, même pour de grands médias, à exercer les fonctions de vérification nécessaires à un journalisme de qualité est bien illustrée par des événements récents comme l'affaire Babtchenko en Ukraine : l'intégralité des grands médias de qualité ont titré le 30 mai 2018 sur la mort d'Arkadi Babtchenko, sur la base de renseignements considérés comme fiables émanant du gouvernement ukrainien, avant de devoir reconnaître dès le lendemain avoir été trompés.

V. Les acteurs privés

Si les grandes plateformes numériques ont longtemps manifesté un fort désintérêt pour le sujet de la lutte contre les manipulations de l'information, qu'elles ont présenté comme peu pertinent eu égard à leur « statut de non-éditeur » et à la nécessité de garantir la liberté d'expression et de commerce, elles ont infléchi leur communication et leur politique de réponse à deux reprises : suite d'abord au débat sur l'interdiction des

contenus à caractère terroriste et illégal, puis à celui sur les ingérences dans les campagnes électorales.

A. D'un non-sujet à une préoccupation majeure

La question de la responsabilité des plateformes quant à la nature des contenus diffusés à travers elles s'est posée pour la première fois de manière saillante dans le contexte de la lutte contre le terrorisme. Elles ont notamment été accusées publiquement de laisser les terroristes communiquer entre eux et diffuser des contenus visant à choquer et/ou à mobiliser en leur faveur.

Il convient bien évidemment de distinguer ce qui relève de la lutte contre les contenus terroristes de la lutte contre les manipulations de l'information. Si, dans le cas de la lutte contre le terrorisme, le principe de liberté d'expression ne prime pas sur l'impératif de sécurité, les termes du débat sont moins clairs pour les manipulations de l'information. Pour autant, il s'agit dans les deux cas de reconnaître le fait que les plateformes sont bien en mesure d'observer ce qui est diffusé et échangé à travers elles. Et qu'elles peuvent s'organiser pour s'assurer que certains contenus apparaissent moins, voire n'apparaissent plus, à travers elles.

Longtemps réticentes à évoquer publiquement le sujet des manipulations de l'information, les grandes plateformes ont été progressivement contraintes, par la pression des États et de la société civile, à se justifier puis à agir. La campagne présidentielle américaine de 2016 a été un double déclencheur.

En premier lieu, les montants – importants – en roubles dépensés dans des publicités politiques visant à nuire à la campagne de la candidate Clinton ont suscité une première prise de conscience auprès d'une grande partie de la classe politique américaine. Habitués à voir les médias traditionnels être particulièrement vigilants sur la vente et la diffusion de publicités, d'autant plus lorsqu'elles sont achetées par un acteur étranger, les politiques américains ont été déconcertés par l'absence de considération et d'intérêt de la plateforme à ce sujet. Pour un acteur en mesure de mettre en place un ciblage publicitaire extrêmement précis, l'absence de mécanismes de contrôle et de vérification de ces mêmes publicités a heurté, apparaissant aux yeux de beaucoup comme un manque flagrant de responsabilité.

L'affaire Cambridge Analytica a, quelques mois plus tard, achevé d'imposer cette idée. Ce n'est plus la vente de publicités qui a suscité moult

questionnements mais l'utilisation par une société privée de données personnelles récoltées, sans l'accord de ces derniers, sur Facebook. Via cette récolte illégale, l'entreprise a été en mesure de mettre en place un micro-ciblage publicitaire particulièrement sophistiqué visant à faire basculer le résultat de l'élection en faveur du candidat Trump, que ce soit à travers la promotion des convictions et promesses de campagne de ce dernier ou à travers le dénigrement de ces mêmes éléments portés par la candidate Clinton.

Facebook est cette fois-ci pointé du doigt pour le manque de protection des données de ses utilisateurs. Fait intéressant : le modèle européen, d'habitude critiqué au sein du Congrès, est explicitement mis en avant pour l'attention qu'il apporte à ce point.

Les raisons d'une telle prise de conscience ne trouvent pas seulement leurs racines dans l'élection présidentielle américaine. D'autres facteurs ont sans doute contribué à cette remise en cause : la fin du mandat d'Obama (le « premier président numérique » particulièrement disposé en faveur des grands groupes numériques), la volonté d'une partie des démocrates de se dédouaner de la perte d'une élection jugée imperdable, des rapports de force à rééquilibrer entre administrations et acteurs privés, etc.

Ce que l'affaire Cambridge Analytica révèle de la persuasion de demain

« La récente affaire dite de Cambridge Analytica révèle […] que la persuasion de demain pourrait ne rien avoir à voir avec les rumeurs à l'ancienne et tout avec le ciblage de chaque électeur. En effet, la méthode consiste à « utiliser des données pour changer des comportements », autrement dit à accumuler une connaissance si fine de chaque citoyen en croisant de multiples informations sur ses comportements, ses liens, ses habitudes, ses envies, ses peurs, etc., que l'ordinateur sera en mesure de lui adresser une incitation à voter ou à acheter répondant exactement à son attente. Il ne s'agit plus de convaincre l'individu ainsi profilé et devenu prévisible d'adhérer à un corpus d'idées, mais de lui faire apparaître un choix politique comme spontané : je pense A, donc je reçois un message me disant que le candidat Y le pense aussi.
Selon ce schéma, nous serions passés, en somme, d'une persuasion politique de masse déversée par les médias à une sollicitation de proximité, au plus intime de nos désirs. »

(François-Bernard Huyghes, « Que changent les *fake news* ? », *La Revue internationale et stratégique*, n° 110, février 2018, p. 83-84.)

Chacun de ces facteurs a contribué à installer un renversement de la charge de la preuve. Les États européens qui ont longtemps souffert de leur image d'acteurs sur la défensive, préférant la régulation à l'innovation, ont vu une grande partie des sénateurs et de l'opinion publique s'aligner sur leurs critiques. *A contrario*, les plateformes numériques sont apparues sous un jour moins flatteur, peu soucieuses de la vie privée et du bon fonctionnement des institutions démocratiques, reposant sur un modèle économique problématique. Ce sont elles qui doivent désormais se justifier.

L'audition de Mark Zuckerberg en avril 2018 a sans doute constitué l'acmé de cette prise de conscience : c'est la première fois qu'un président-directeur général d'un grand groupe numérique s'est vu publiquement contraint de rendre des comptes sur le fonctionnement et la responsabilité de son entreprise. Si de nombreux observateurs s'interrogent sur les conséquences à long terme de cette vague de contestation, l'audition de Zuckerberg ne s'est pas traduite pour le moment par un retrait significatif des utilisateurs ou par une baisse de la capitalisation boursière des plateformes. Force est de constater que les plateformes ont multiplié les effets d'annonce et la publicité autour de leurs mesures pour lutter contre les manipulations de l'information.

B. La réponse des grandes plateformes numériques aux manipulations de l'information

Les plateformes ont très largement développé leurs mesures de lutte contre les manipulations de l'information en réaction, et donc en fonction, des critiques qui leur ont été adressées. L'intensification de ces dernières a contraint les plateformes à proposer un grand nombre de mesures, dans un laps de temps très court, sans avoir toujours développé en amont une véritable stratégie de réponse. En cela, les différentes mesures proposées n'ont pas le même objectif (répondre ponctuellement ou de manière plus structurelle), la même temporalité (agir en amont ou *ad hoc*), la même échelle (mesures qui ne s'appliquent qu'à un pays ou à l'ensemble des utilisateurs). Elles peuvent cependant être classées selon les six catégories suivantes.

1. Sensibiliser l'utilisateur aux risques et enjeux des manipulations informationnelles

Une grande partie des mesures visaient à encourager l'internaute à prendre conscience des mécanismes à l'œuvre dans la diffusion et la hiérarchisation des contenus échangés sur les plateformes : publication par Facebook de guides expliquant les bonnes pratiques à avoir sur les réseaux sociaux face aux informations qui y circulent, efforts de pédagogie menés par Google afin d'expliciter les critères de hiérarchisation de l'information par les moteurs de recherche. Cet effort de sensibilisation n'a pas seulement été mené en amont : les plateformes ont aussi décidé d'alerter les utilisateurs qui avaient été en contact avec de fausses informations. C'est notamment le cas de Facebook qui a communiqué avoir envoyé un message d'avertissement aux utilisateurs dont les données ont été recueillies par Cambridge Analytica durant la campagne présidentielle américaine (s'élevant à ce jour à 87 millions d'utilisateurs). L'objectif affiché est, pour chacun de ces exemples, de « donner les clés » à l'internaute pour que ce dernier puisse lui-même détecter et agir face aux manipulations de l'information.

En outre, certains acteurs – notamment Facebook – ont directement sensibilisé les différents candidats de l'élection présidentielle afin que ces derniers aient connaissance des risques encourus et développent de bonnes pratiques d'utilisation. Plus largement, parce que les campagnes de manipulation de l'information exploitent souvent les données personnelles – en volant ces dernières ou en s'appuyant sur elles pour construire sur mesure les narratifs qu'elles déploient –, les plateformes ont également renforcé la sécurisation des données personnelles. Facebook a ainsi grandement amélioré l'interface permettant à ses utilisateurs de régler le degré de visibilité des données concernant leur vie privée (notamment en centralisant tous les réglages). Les plateformes sont également bien plus vigilantes quant aux risques de voir les données de leurs utilisateurs être piratées : début mai 2018, alerté par une fuite qui aurait pu exposer les mots de passe de ses utilisateurs, Twitter a été très réactif et a immédiatement demandé à ces derniers d'en changer.

Enfin, à travers les auditions publiques, les grandes plateformes participent à une meilleure prise de conscience des opinions publiques quant à la nécessité d'être davantage vigilantes face aux campagnes de manipulation de l'information.

2. Améliorer la détection des manipulations de l'information

Les campagnes de manipulation de l'information s'appuient très souvent sur des comptes automatisés (bots), des réseaux de comptes automatisés (netbots) et sur des comptes anonymes. Longtemps réticentes à identifier et supprimer ces derniers pour diverses raisons (modèle économique, peur d'être qualifiées d'éditeurs), les plateformes ont récemment sauté le pas. Elles ont d'abord étudié de plus près les comptes de leurs utilisateurs afin de supprimer les différents comptes faux, automatiques et/ou suspectés d'avoir participé à des campagnes de manipulation de l'information. Twitter a notamment annoncé avoir supprimé plus de 50 000 comptes « liés aux interférences russes » pour reprendre les termes du porte-parole de l'entreprise. Il est cependant difficile de juger de l'efficacité de ces campagnes de suppression de comptes. Très souvent, elles ne ciblent pas que les comptes susceptibles de relayer les campagnes de manipulation de l'information : elles suppriment surtout les faux comptes vendus par des agences d'e-réputation dont le but est d'augmenter la visibilité de leurs clients. Instagram a ainsi lancé fin 2014 une opération de nettoyage de 300 millions de comptes (#PurgeInstagram). Suite à celle-ci, d'intenses répercussions sur la visibilité de comptes de stars américaines (Kim Kardashian, Katy Perry, Oprah Winfrey, Justin Bieber ou encore Rihanna) se sont fait sentir. Facebook avait eu une démarche similaire en 2012, lors d'une grande chasse aux faux *like* avec une efficacité limitée. Depuis 2016, la chasse aux *fake* est devenue l'enjeu de batailles chiffrées dont il demeure difficile de mesurer la réelle portée. Au premier trimestre 2018, Facebook revendiquait ainsi la suppression de 583 millions de faux comptes et de plus d'1,3 milliard sur six mois.

Facebook, Twitter, Google ont également mis en place, avec le gouvernement américain, une initiative visant à créer une base de données commune listant les faux comptes et répertoriant les stratégies développées par les trolls pour éviter de se faire repérer. Il s'agit d'optimiser la détection des manipulations de l'information en échangeant les informations sur les modèles et les acteurs de ces dernières. D'autres mesures, s'appuyant sur l'intelligence artificielle, ont été mises en place pour détecter ces comptes et les supprimer, parfois même avant leur mise en ligne. Twitter a ainsi rendu impossible l'utilisation de comptes en simultané (méthode très souvent utilisée par les trolls). Dans la même lignée, Facebook a également annoncé avoir développé un outil permettant de détecter les messages et

commentaires qui seraient publiés de manière à la fois similaire et répétitive. Soit autant de techniques communément utilisées lors des campagnes de manipulation.

3. Endiguer la diffusion et l'impact des campagnes de manipulations informationnelles

Les plateformes ont développé plusieurs mesures visant à accélérer le retrait de contenus jugés problématiques. Si les techniques fondées sur l'intelligence artificielle sont utilisées en amont (soit avant que le contenu ne soit publié), les plateformes continuent à s'appuyer sur la modération humaine pour vérifier, et parfois supprimer, les contenus échangés et les publicités problématiques. Facebook a ainsi annoncé en décembre 2017 avoir recruté 1 000 employés supplémentaires chargés de vérifier les publicités et de les effacer si elles ne devaient pas convenir aux standards d'acceptabilité (soit des publicités qui ciblent précisément les personnes selon leurs opinions politiques, religion, ethnicité, milieu social). Facebook a également augmenté de plus de 60 % les équipes dédiées à la vérification des contenus jugés douteux, avec un effectif mondial qui s'élèverait aujourd'hui à 8 000 personnes. Si ce renforcement de la modération est significatif, il convient de noter qu'il concerne avant tout la vérification des contenus jugés illégaux et/ou étant à caractère terroriste. En juillet 2018, toutefois, Facebook a annoncé mettre en œuvre une « nouvelle politique » de suppression des contenus susceptibles de causer des violences, en commençant prioritairement par « des pays où nous voyons des exemples où la désinformation a […] entraîné des violences[78] », comme le Sri Lanka par exemple, où des messages faisant croire que les musulmans empoisonnaient la nourriture des bouddhistes ont été supprimés par le réseau social.

Twitter aussi a accéléré le nettoyage, en introduisant en mai-juin 2018 de nouvelles mesures pour combattre le trolling et les propos haineux et extrémistes[79], et en suspendant en seulement deux mois 70 millions de comptes, soit deux fois plus que le taux de suspension d'octobre 2017[80].

Les plateformes ont également optimisé les mécanismes de signalement : les procédures permettant aux internautes de signaler un contenu

78. Sheera Frenkel, « Facebook to Remove Misinformation That Leads to Violence », *The New York Times*, 18 juillet 2018.

79. Yoel Roth et Del Harvey, « How Twitter is fighting spam and malicious automation », blog.twitter.com, 26 juin 2018.

80. « Twitter is sweeping out fake accounts like never before », *The Washington Post*, 6 juillet 2018.

problématique ont été simplifiées. Depuis peu, Google permet à ses utilisateurs de signaler les contenus qu'ils jugent « trompeurs ou inexacts ». Facebook porte davantage d'attention aux retours et commentaires des internautes ayant identifié de fausses nouvelles. Plus généralement, Facebook cherche à systématiser son processus de réponse contre les manipulations de l'information à travers le développement d'un cadre d'analyse qu'il a intitulé *Problems, Surfaces and Actions framework*. Ce dernier vise à objectiver les seuils de réponse (quand et comment répondre), à coordonner les différents acteurs et à imposer une procédure de réponse standard. Cette dernière implique notamment la mention d'articles de *fact-checking* (qui traitent des mêmes faits que l'information douteuse publiée) qui mettent à distance la fausse information ; la notification du nombre d'utilisateurs qui ont jugé l'information fausse ou trompeuse ; l'alerte sur le fait que l'internaute est susceptible de relayer une fausse information. Dans cette même perspective, YouTube a fait le choix d'afficher à côté de certaines vidéos conspirationnistes le lien vers un article de Wikipedia qui déconstruit directement le propos.

Enfin, les plateformes ont également développé les outils de détection des *deep fake*, ces fausses informations qui parviennent à reproduire complètement l'effet de réel. Google a ainsi annoncé avoir mis en place un outil capable de détecter ces vidéos (notamment celles en mesure de faire parler un acteur public) et de les supprimer avant qu'elles ne soient publiées.

4. Réguler et coopérer

Pour de multiples raisons (culturelles, économiques, techniques), les plateformes sont réticentes face à la régulation : elles favorisent généralement la coopération informelle avec les autorités et avec les médias.

Ainsi, Facebook collabore régulièrement avec les médias institutionnels pour échanger avec eux les listes des différents articles qui circulent sur son site et qui ont été signalés comme étant faux. Google a annoncé avoir fait de même lors des campagnes présidentielles américaines et françaises. Les deux plateformes ont également mis en place plusieurs initiatives qui associent très étroitement la société civile et les médias dans la lutte contre les manipulations de l'information (voir *supra*).

Facebook a également annoncé avoir collaboré directement avec le gouvernement allemand lors des dernières élections. Les termes de cette collaboration ont été largement dictés par la loi allemande sur l'application du droit sur les réseaux sociaux, qui impose notamment aux réseaux

sociaux de supprimer dans un délai court (de 24 heures à 7 jours pour les cas litigieux) les contenus manifestement illégaux, notamment les appels à la haine ou à la discrimination. D'autres États envisagent également la mise en place de dispositifs législatifs qui contraindraient les plateformes à davantage agir vis-à-vis des contenus jugés problématiques.

5. Promouvoir les bonnes pratiques et les acteurs institutionnels

C'est très souvent par une forme de promotion positive que les plateformes entendent lutter contre les manipulations de l'information. Renforcer la visibilité des contenus jugés fiables et/ou produits par les médias institutionnels dans les moteurs de recherche et fils d'actualité est un axe majeur de la politique de réponse des différentes plateformes. Cela implique notamment l'actualisation de l'algorithme de hiérarchisation des références ou encore le blocage des sites qui n'indiquent pas leur pays d'origine. Cela suppose également, en creux, un travail actif qui consiste à détecter les sources habituelles de désinformation (sites conspirationnistes, sites se présentant comme institutionnels et relayant de fausses informations) afin de diminuer la visibilité de ces dernières (sans toujours les supprimer).

YouTube, Google et Facebook ont également mis en place le *Trust Project Initiative*, en partenariat avec l'université de Santa Clara, qui consiste à valoriser les contenus jugés fiables en donnant la possibilité aux éditeurs de ces derniers de partager des informations sur les politiques de vérification des faits qu'ils ont mises en place, la structure et l'identité de leur direction et de leurs actionnaires, l'histoire du média sur lequel ils opèrent. Ces différentes informations, indiquées sous forme d'onglets, visent à mettre en avant la déontologie ainsi que la fiabilité de ces médias.

Enfin, les plateformes promeuvent également la création d'espaces de discussions et de débats dits « constructifs » : Twitter entend notamment développer des indicateurs permettant de vérifier la variété des opinions échangées, la réceptivité des utilisateurs, l'attention portée au sujet dans les médias. L'application Snapchat, très utilisée par les jeunes publics, a quant à elle choisi de diviser les contenus diffusés en son sein en deux catégories : « découverte » et « social ». Cette division permet indirectement à la plateforme de promouvoir les articles des médias institutionnels, ces derniers étant les seuls médias à être publiés dans la catégorie « découverte » (les autres types de contenus se présentant comme des informations – articles de blog, commentaires, reprise d'articles – étant relégués dans la catégorie « social »).

6. Analyser les mécanismes des campagnes de manipulations informationnelles

Vivement critiquée pour leur naïveté et leur manque de discernement face à l'impact et à l'ampleur des campagnes de manipulation de l'information, les plateformes ont tout d'abord souligné la nécessité de mieux comprendre le phénomène. Pour cela, elles ont mis en place diverses politiques de partenariat et d'échange avec le monde de la recherche. Ainsi, Facebook a récemment accepté de partager un certain nombre de données avec l'université de Stanford afin que cette dernière puisse se pencher sur les campagnes de manipulation de l'information, notamment à travers le *Project on Democracy and the Internet*.

De même, les plateformes participent au financement d'initiatives visant à développer une meilleure prise de conscience des enjeux éthiques liés à l'utilisation des plateformes, y compris dans le domaine de l'information. C'est notamment ce que Google a fait en créant la *DeepMind Ethics & Society*.

Si les plateformes sociales se sont donc largement emparées de la lutte contre les manipulations de l'information, de nombreux efforts restent néanmoins à fournir. Comme le rappelle le *Wall Street Journal*, « le directeur général de Twitter, Jack Dorsey [lui-même], a partagé au moins 17 tweets d'un troll russe dénommé Crystal1Johnson entre fin 2016 et mi-2017[81] ».

C. L'apport de la recherche en publicité et marketing

Le milieu de la publicité est souvent présenté comme le chantre de la désinformation, en ce qu'il entend manipuler les esprits à des fins lucratives et commerciales[82]. Comment faire vendre ? Comment rendre un produit attirant pour tel public ? Comment faire choisir ce produit plutôt qu'un autre ? Ces questions sont au fondement même des pratiques de manipulation de l'information, mais aussi des réponses qui y sont apportées. Comment faire en sorte que les messages diffusés par les médias conventionnels jugés fiables continuent à tenir la dragée haute aux médias propagandistes ?

81. Étude du *Wall Street Journal* citée dans Georgia Wells et Rob Barry, « Les trolls russes continuent de mettre le bazar sur les réseaux sociaux américains », *L'Opinion*, 20 juin 2018.

82. François Géré, *Dictionnaire de la désinformation,* Armand Colin, 2011.

Les outils développés par les recherches en marketing et publicité nous semblent offrir deux avantages au moins quant à l'étude des manipulations de l'information. D'une part, en analysant la réaction d'un groupe cible à une campagne particulière, ces outils permettent de mieux comprendre l'impact – visuel, émotionnel, rationnel, intellectuel – d'un message sur un public donné. D'autre part, en pointant les faiblesses et « vides » d'un message produit, ainsi que les raisons pour lesquelles un usager se tournera vers un message plutôt qu'un autre, ils renseignent sur la manière dont les médias conventionnels jugés fiables peuvent améliorer leur attractivité et capter l'attention d'un public qui leur échappe.

En publicité, les recherches tentent d'analyser l'influence d'une campagne sur un groupe test *ex ante*[83]. Des études cherchent à prédire l'efficacité qu'aura une publicité sur le marché en analysant le niveau d'attention du public, son lien avec la marque, le divertissement que la publicité engendre chez l'usager, les chutes d'attention et les émotions produites. De tels outils permettent également d'identifier les points faibles d'une campagne. Les études sont également faites *ex post* afin de surveiller l'évolution des préférences chez les populations, en particulier chez les jeunes générations, nouveaux consommateurs inconnus à séduire. Ces outils incluent des entretiens avec des groupes test mais également le suivi du regard de l'usager face à une campagne.

Appliquées aux manipulations de l'information, de telles pratiques pourraient comporter une forte dimension explicative. L'on peut en effet imaginer mener une étude similaire comparant un article conventionnel à un article « détourné » afin d'identifier ce qui, dans la fausse nouvelle, séduit le public, permettant ainsi de renforcer l'influence des médias jugés fiables sur différents publics. Des outils comme le *eye tracking*, ou suivi du regard de l'usager, permettent également de mieux comprendre les réactions des usagers aux fausses nouvelles pour mieux les contrer.

En marketing, l'ambition des études consiste à analyser la disponibilité du marché à un produit[84]. Ainsi, les études vont analyser la réaction des consommateurs à une marque (comment la marque est-elle perçue ? Quels en sont les principaux attributs ? Comment se situe-t-elle par rapport aux autres marques ?), à un produit (diffusion du produit sur un groupe test, évaluation des nouvelles tendances, évaluation du nom du produit, de son prix). Ces outils visent également à comprendre les consommateurs eux-mêmes (segmentation : qui sont-ils ? ; décision de l'acheteur : pourquoi

83. Joel J. Davis, *Advertising Research: Theory and Practice* (2nd ed.), Pearson, 2011.
84. Paurav Shukla, *Essentials of Marketing Research,* Ventus Publishing ApS, 2008.

achète-il ? ; renseignement sur internet : surveiller les forums en ligne, les services après-vente virtuels pour analyser la satisfaction des consommateurs, etc.).

Les manipulateurs de l'information utilisent déjà une méthode de marketing appelée le « test A/B », permettant de comparer l'impact de deux variables, en l'occurrence deux messages (par exemple, ils diffusent initialement les messages selon lesquels « les noirs sont des terroristes » et « les noirs sont des criminels », s'aperçoivent que le second fonctionne mieux que le premier. Ils misent donc sur lui et continuent d'affiner le message en fonction de ce qui est le plus viral). Ces techniques et d'autres pourraient certainement avoir une utilité explicative (pourquoi une fausse nouvelle fonctionne-t-elle ?) et opérationnelle (comment améliorer l'attractivité des médias jugés fiables et conventionnels face à RT et Sputnik ?).

Le champ des recherches publicitaires et marketing offre donc des perspectives intéressantes dans la lutte contre la manipulation des informations, en dépit de la mauvaise presse associée à ce milieu. Contrer les manipulations implique de saisir la recette de leur succès chez les différents publics : Pourquoi ce produit attire-t-il ? Quel est l'état de la demande sur ce marché de l'information ? La lutte contre les manipulations requiert également le renforcement des médias conventionnels jugés fiables, en analysant notamment leurs manquements et les efforts à mener afin de les rendre séduisants pour des publics qui leur échappent.

Quatrième partie

DÉFIS FUTURS

I. Comment penser ce qui vient ?

Il est difficile d'anticiper quels seront les défis futurs. Nos adversaires sont créatifs et s'adaptent vite, les technologies et les supports médiatiques évoluent rapidement, et l'arrivée de nouveaux acteurs est aisée (les coûts d'entrée sont nuls, les risques d'être pris très faibles grâce aux difficultés de l'attribution et les gains potentiels très élevés). Pour l'ensemble de ces raisons, il faut s'attendre à ce que les manipulations de l'information se généralisent et impliquent toujours davantage d'acteurs.

Quiconque aurait dit, il y a dix ans, que les grands réseaux sociaux qui venaient d'être créés (Facebook en 2004, Twitter en 2008, Instagram n'existait pas encore) auraient autant d'effet sur la vie de milliards de personnes et feraient partie d'un problème informationnel massif menaçant nos démocraties, aurait eu du mal à être cru. Il est donc difficile d'imaginer ce qui, dans dix ans, façonnera nos relations sociales et nous posera les problèmes les plus importants. On peut par exemple faire l'hypothèse d'une perte de vitesse des réseaux ouverts actuels et du développement des réseaux fermés (WhatsApp, Telegram, etc.) qui poseront d'autres types de difficultés aux autorités, notamment en matière de cryptographie.

A. Les défis technologiques

Dans tous les cas, l'innovation technologique sera déterminante. Non seulement l'innovation, mais aussi sa démocratisation : l'accessibilité et le coût vont décroître, en même temps que l'efficacité, la performance et la vitesse de propagation vont s'accroître. L'intelligence artificielle rendra les bots plus humains, donc moins détectables. Elle fera progressivement sauter les barrières de la langue et de la culture (qui sont pour certains pays autant de remparts aux efforts d'influence étrangers), notamment avec le perfectionnement des logiciels de traduction. Les logiciels d'édition photo, audio et vidéo, par exemple, permettront demain (certains même aujourd'hui), de faire dire n'importe quoi à n'importe qui, en rendant la désinformation indétectable. Les *deepfake videos,* consistant à modifier numériquement les visages de personnalités afin de leur faire dire ou faire ce que l'on veut, sont déjà très crédibles. Ces vidéos altérées ont d'ailleurs été identifiées par le département de Défense américain comme un enjeu des élections de mi-mandat de 2018. À ce titre, la US Defense Advanced Research Projects Agency (DARPA) a même financé le Media Forensics Project dont l'objectif est de développer des technologies capables de cibler et identifier automatiquement ces *deepfake videos*[1]. Un plus grand danger encore, car plus subtil que la création d'un faux, est l'altération discrète d'une partie seulement d'un contenu audio ou vidéo, un discours par exemple. Ou encore la possibilité d'en faire un grand nombre de variations – diffuser une vingtaine de variantes du même discours, par exemple, pour diluer l'authentique dans la confusion.

Les personnalités fictives sont un autre risque. Pendant trois ans, de 2014 à 2017, Jenna Abrams était une militante pro-Trump connue, icône de l'*alt-right* américaine, citée par les grands médias (dont *The Washington Post*, *The New York Times*, *The Independent* et France 24) et suivie par 70 000 comptes sur Twitter. Mais Jenna Abrams n'existait pas : son compte était une création de l'IRA, l'usine à trolls de Saint-Pétersbourg[2]. L'intelligence artificielle rendra ces personnalités fictives plus sophistiquées, moins détectables. Elles pourront donner des interviews, écrire des tribunes dans la presse, avant d'être découvertes.

1. Jeremy Hsu, « Experts Bet on First Deepfakes Political Scandal », *IEEE Spectrum*, 22 juin 2018.

2. Ben Collins, Joseph Cox, « Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World », *The Daily Beast*, 11 février 2017.

Ces tendances vont participer d'une atomisation extrême de l'information, avec la disparition ou la fragilisation des acteurs pouvant servir de « tiers de confiance » (notamment les grands médias jouissant de la confiance du public, la parole publique continuant pour sa part à être décrédibilisée d'avance). Dans un tel univers, la question centrale sera de savoir comment recréer des tiers de confiance. Outre le renforcement du modèle économique et de la crédibilité des médias traditionnels, d'autres approches ont déjà été proposées et mériteraient d'être explorées (comme l'utilisation de la technologie dite de la chaîne de blocs (*blockchain*) permettant d'accroître la traçabilité de l'information).

Même les progrès de la recherche en psychologie sociale, en particulier sur la manière dont nous prenons des décisions, pourront être « arsenalisés », en permettant de faire du *micro-targeting* plus précis et plus efficace. La puissance qui alliera ces trois ingrédients – connaissances en psychologie sociale, *big data* et intelligence artificielle – pourra fabriquer une arme de division massive.

B. Les futures tendances de la « guerre de l'information » russe

Il est par définition difficile d'anticiper les prochains coups d'un acteur qui se caractérise par sa capacité à faire du sur-mesure et à apprendre de ses erreurs. Cependant, nous estimons que le Kremlin va dans les directions suivantes.

1. Cinétisation

On observe déjà un intérêt croissant des acteurs russes pour la couche physique, c'est-à-dire les infrastructures des communications. Cet intérêt n'est pas apparu pendant l'annexion de la Crimée mais a assurément été renforcé par cette opération, au cours de laquelle Moscou a pu intervenir directement sur l'information reçue par la population de la péninsule en coupant littéralement certains câbles internet et téléphoniques. Le cas criméen reste toutefois un cas particulier compte tenu de la géographie du lieu et de sa connaissance préalable par le renseignement russe. Sur le long terme, les deux couches physiques qui intéressent le plus Moscou sont le sous-marin, pour les câbles dont on sait depuis des années qu'ils peuvent être piratés, et le spatial, pour les satellites autour desquels on observe parfois certaines manœuvres. On peut donc s'attendre à une plus grande imbrication entre les dimensions cinétiques

et non cinétiques dans les opérations russes ou, en d'autres termes, à la cinétisation de la guerre de l'information.

2. Personnalisation

La personnalisation des attaques n'est pas nouvelle, en témoigne l'utilisation par les services soviétiques puis russes de la méthode du *kompromat*, c'est-à-dire la compromission d'une cible qui est ainsi tenue et manipulée. Dans le domaine informationnel qui nous intéresse ici, cette tendance pourrait, dans les années à venir, prendre les formes suivantes. Des attaques personnalisées pourraient viser des militaires en opération, comme c'est déjà le cas en Ukraine : la version moderne du largage aérien de tracts est l'envoi de messages textuels par téléphone (SMS). Les soldats ukrainiens reçoivent déjà des messages qui visent à altérer leur moral ou leur cohésion, leur signifiant par exemple qu'ils sont « encerclés et abandonnés ». Puis, quelques minutes plus tard, ce sont leurs familles qui reçoivent un message leur annonçant la mort de leur fils, leur frère ou leur père, tué par l'ennemi – ce qui suscite généralement des appels des familles vers les soldats, et permet par la concentration de signaux de détecter leur localisation pour ensuite les bombarder[3] – faisant des SMS envoyés une sorte de prophétie autoréalisatrice.

On a également observé une recrudescence de l'activité des agents russes vis-à-vis de militaires occidentaux en opération, par exemple ceux déployés dans les États baltes dans le cadre de la présence avancée renforcée de l'OTAN. Cette activité des services russes implique des méthodes traditionnelles (tentative d'approche physique) mais également plus novatrices. Ces dernières reposent par exemple sur une exploitation de leurs informations personnelles via les réseaux sociaux. Les attaques personnalisées pourraient aussi viser des civils, que ce soient des hommes politiques, des hauts fonctionnaires ou des personnalités. Une vigilance particulière doit être exercée sur les attaques ciblées qui seraient noyées dans des campagnes légitimes, provenant d'acteurs divers, comme Paradise Papers ou #metoo ; les fuites massives, désormais trop évidentes après les « DNC Leaks » et les « Macron Leaks », sont moins à redouter.

3. Col. Liam Collins, « Russia Gives Lessons in Electronic Warfare », Association of the United States Army, 26 juillet 2018.

3. Normalisation

On observe un élargissement des médias relayant les thèses du Kremlin. Les médias qui apparaissent comme lui étant trop liés (RT et Sputnik) et/ou qui défendent trop ouvertement ses positions sont désormais clairement identifiés comme des outils de propagande. Même s'ils gagnent en audience et élargissent leurs publics cibles, ils pourraient être de plus en plus concurrencés par d'autres formes de diffusion de l'information. Le Kremlin investira sans doute davantage dans le fait de « convertir » certaines personnalités non connues pour être pro-russes, ou de faire passer certains messages dans les plus grands médias traditionnels, c'est-à-dire dans la « mainstreamisation » ou normalisation de sa guerre de l'information, qui sera plus difficile à combattre. La désinformation grossière, les fausses nouvelles absurdes, les sites d'*infotainment* sont des armes de distraction massive : elles offrent une diversion, au profit de manipulations plus subtiles, donc plus dangereuses.

4. Proxysation

L'Europe et l'Amérique du Nord étant devenus des espaces trop évidents et du même coup saturés de contre-mesures, avec des populations très éduquées et largement sensibilisées, il faut s'attendre à une extension du champ de bataille aux nouveaux fronts identifiés précédemment (voir *supra*), en particulier l'Afrique et l'Amérique latine. Ces régions ont en effet l'avantage, du point de vue de l'attaquant, d'être aisément pénétrables puisqu'elles parlent des langues communes (anglais, français, espagnol), dans lesquels les dispositifs informationnels existent déjà ; d'héberger des populations moins éduquées donc plus influençables, et néanmoins très connectées grâce à la démocratisation des technologies de l'information et de la communication ; d'être traversées de passions faciles à instrumentaliser, dont des tensions ethniques et religieuses, et un ressentiment à l'égard des anciennes puissances coloniales. Pour affaiblir l'Europe, les Russes pourront donc utiliser ces populations comme proxy.

On l'observe déjà dans le cas du Maghreb, où l'investissement russe est massif, et pas seulement pour des raisons énergétiques. Les populations maghrébines sont largement exposées à la propagande des médias russes en arabe, qui véhicule des messages anti-européens dont elles ne sont que la cible indirecte, le vecteur. L'objectif est que ces populations, qui sont en lien quotidien avec leurs familles et leurs proches vivant en Europe,

leur transmettent ces messages et les convainquent que les médias européens leur mentent et que les Européens leur sont hostiles. La propagande anti-immigration que l'on voit en Europe visant à exciter les communautés nationalistes n'est donc qu'une face de l'opération. Pour diviser, monter les communautés les unes contre les autres, il faut aussi convaincre les populations issues de l'immigration qu'elles sont maltraitées et, de ce point de vue, le fait de passer par des relais en Afrique du Nord est particulièrement habile.

Ces tendances, qui devraient s'accentuer à l'avenir, sont préoccupantes. Ce qui l'est davantage encore est de comprendre qu'elles seront de moins en moins isolées : ce qu'il faut craindre en effet est leur généralisation et la diversification des acteurs – le fait que beaucoup d'autres feront demain ce que les Russes ont longtemps été les seuls à faire, ou à faire aussi bien.

II. Quelques scénarios

166 *Les scénarios suivants sont des fictions. Leur but est d'attirer l'attention sur certaines vulnérabilités.*

• Scénario 1. Dans le cadre des consultations citoyennes qui ont débuté en avril et s'achèveront en octobre 2018, on observe des actions coordonnées qui allient manipulations en ligne – diffusion massive via des bots de fausses informations et de posts – et sponsoring de « chevaux de Troie » physiques – identifiés en amont comme portant un discours favorable aux intérêts de la puissance agissante – afin d'inciter à la radicalisation des débats et/ou la décrédibilisation des consultations. Dans un second temps, le contenu des restitutions au Conseil économique et social européen peut faire lui-même l'objet d'une campagne de manipulation de l'information et/ou de dénigrement, avec relais automatisé des posts les plus subversifs.

• Scénario 2. Alors que les négociations post-Brexit s'annoncent longues et difficiles, on assiste à des tentatives de piratage de boîtes de courriels donnant accès aux adresses des personnalités politiques et des experts chargés des négociations, et donc à leurs échanges confidentiels. En cas de succès, ces attaques aboutissent à la diffusion sélective de contenus – pouvant faire l'objet de faux – pour discréditer le processus de négociation et/ou semer la zizanie entre les partenaires européens, et entre l'UE et le Royaume-Uni. Des campagnes de

manipulation de l'information ponctuelles sont également à prévoir sur des points précis des négociations, afin de provoquer des réactions émotionnelles au sein des opinions publiques britannique ou européenne, et de renforcer ainsi la crise de confiance entre les peuples et les institutions européennes.

• Scénario 3. Plusieurs campagnes de manipulation de l'information ont lieu afin de renforcer les tensions entre les États membres de l'UE. L'une s'attaque au contenu des rencontres du groupe de Visegrád, attribuant aux pays de l'Est des intentions qu'ils n'ont pas en réalité – notamment sur des questions de gouvernance démocratique « illibérale » ou sur des enjeux de positionnement différencié en politique étrangère – et renforçant la défiance grandissante entre l'Est et l'Ouest de l'Europe à l'approche des élections. L'autre s'en prend au leadership et à la volonté de réforme du couple franco-allemand, et fait rejouer les tensions intra-européennes apparues lors de la crise de l'euro, en répandant de prétendues velléités de mettre au pas les États membres d'Europe du Sud (Italie, Espagne, Portugal, Grèce), notamment sur les questions de gouvernance monétaire et de rationalisation de la dépense publique.

• Scénario 4. Des attaques ciblant expressément la France ont lieu afin d'affaiblir le gouvernement en créant un ou plusieurs scandale(s) politique(s) majeur(s). Une campagne malveillante contre un membre particulier du gouvernement est lancée à partir d'une affaire préexistante ou montée de toutes pièces, à fort impact médiatique (évasion fiscale, corruption, harcèlement ou scandale sexuel). On voit également surgir une campagne momentanée contre les réformes institutionnelles du gouvernement, qui mettra en cause le gouvernement dans son ensemble et engagera sa responsabilité en jouant sur la charge émotionnelle de certains mécanismes (usage du 49.3, ordonnances, fausses feuilles de route, etc.).

50 RECOMMANDATIONS

I. Recommandations générales

1. Définir et distinguer clairement les termes, comme nous avons tenté de le faire en introduction. Ceci devrait permettre de lutter contre le relativisme répandu consistant à dire que « tout est propagande » et que tous les médias pratiquent la désinformation. Ce qu'il faut condamner n'est pas la défense des intérêts nationaux – les médias russes ont le droit de défendre un point de vue russe, et même celui du régime – mais la manipulation de l'information. L'utilisation du diagnostic « DIDI » (*deception, intention, disruption, interference*) préconisé par le MSB suédois et l'université de Lund pourrait contribuer, grâce à une grille de critères objectifs, à distinguer véritables manipulations de l'information et activités d'influence plus bénignes[1].

2. Ne pas minorer la menace, même si elle n'est pas perceptible tous les jours. Une bonne préparation à la lutte contre les manipulations de l'information devra nécessairement se construire sur une évaluation pertinente de la menace, c'est-à-dire l'élaboration constante et actualisée de scénarios de menace prenant en compte les évolutions des conflictualités et des risques[2].

1. James Pamment *et al.*, *Countering Information Influence Activities, op. cit.,* p. 7.
2. Finnish Government, *Security Strategy for Society. Government Resolution,* The Security Committee, 2 novembre 2017.

3. Sortir du court terme. Les opérations informationnelles servent des objectifs de court et de long termes. Le court terme est lié à un événement particulier, en général une élection, un conflit armé ou social, une catastrophe naturelle, un assassinat (Nemtsov) ou une tentative (Skripal), un accident aérien (MH17), etc. Les faux comptes et fausses histoires utilisés peuvent être plus évidents, plus brutaux, moins subtils, parce qu'ils ont de toute façon une durée de vie limitée et seront soit exposés soit supprimés une fois l'objectif atteint. Les opérations de long terme, en revanche, s'en prennent à des idées, des positions, pour les affaiblir, ou des communautés, pour exacerber les tensions qui les divisent. C'est un travail de sape, quotidien, avec des acteurs plus discrets, plus subtils, et des conséquences plus difficiles à évaluer. Pourtant, ce sont bien ces opérations sur le long terme qui sont les plus dangereuses. Elles suivent le modèle de l'érosion : si l'eau finit par entamer la roche, c'est par la durée, la répétition, la permanence. Il est donc important de sortir du court terme, qui est souvent un prisme électoral (consistant à ne se préoccuper que des menaces informationnelles en période électorale) pour prendre conscience que le combat est quotidien.

4. Renforcer la résilience de nos sociétés. Les manipulations de l'information se nourrissent des divisions et des tensions qui parcourent nos sociétés. On ne luttera donc efficacement, c'est-à-dire durablement, contre ces manipulations qu'avec une volonté politique de renforcer la résilience de nos sociétés. On peut de ce point de vue beaucoup apprendre de certains États, en particulier la Finlande qui a fait de la résilience contre les menaces dites « hybrides » un véritable concept national[3].

5. Ne pas abandonner le web aux extrémistes. Si les théories du complot prolifèrent, c'est aussi parce qu'elles manquent de contradicteurs[4]. « Les internautes qui épousent une forme de rationalité scientifique considèrent l'échange avec des "croyants" comme une perte de temps et préfèrent les moquer ou les ignorer. De la même façon, les internautes "progressistes" ne voient pas forcément l'intérêt qu'il y a à entrer en discussion avec des internautes racistes, misogynes ou homophobes pour

3. René Nyberg, « Hybrid Operations and the Importance of Resilience: Lessons From Recent Finnish History », Carnegie Endowment for International Peace, 8 février 2018.

4. Gérald Bronner, *La Démocratie des crédules*, *op. cit.*

déconstruire leurs arguments. Résultat, l'espace du débat en ligne est saturé par des propos mensongers ou agressifs[5]. »

Il faut toutefois et en même temps prendre en compte le risque d'un effet boomerang, car réfuter, c'est répéter. Toute correction accroît donc indirectement la diffusion de la fausse information. Cet effet de propagation est inévitable et doit conduire à choisir ses combats, c'est-à-dire ne réfuter substantiellement que les manipulations les plus dangereuses.

6. Ne pas céder à la tentation de la contre-propagande. Comme l'écrivait déjà Fred Iklé en 1989, « la vérité est la meilleure arme POLWAR [de guerre politique] et PSYOP [de guerre psychologique] des démocraties » car « les buts de la démocratie ne peuvent être accomplis qu'avec des méthodes compatibles avec la démocratie »[6]. Pour les démocraties, la meilleure réponse aux manipulations de l'information reste « une preuve factuelle convaincante fournie au bon moment[7] ».

7. Ne pas croire au solutionnisme technologique, contre lequel nous prévient Evgeny Morozov dans son livre au titre évocateur, *Pour tout résoudre cliquez ici*[8]. D'une manière générale, il n'y a pas de solution unique, la réponse doit être multifactorielle (puisque le problème l'est).

II. Recommandations aux États

8. Avoir une empreinte légère. Le premier rempart contre les manipulations de l'information, dans une société démocratique et libérale, doit rester la société civile (les journalistes, les médias, les plateformes numériques, les ONG, etc.). La première des recommandations pour l'État est donc de conserver une empreinte légère – non seulement par conformité à nos valeurs, mais aussi par souci d'efficacité : l'une des causes du problème étant la défiance à l'égard des élites, l'approche « par le haut » a ses limites. Mieux vaut favoriser les approches horizontales, collaboratives, sollicitant la participation de la société civile. Cela correspond d'ailleurs aux attentes de la population : la plus grande enquête sur le sujet (74 000 sondés dans

5. Romain Badouard, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, *op. cit.*, p. 174.

6. Fred Iklé, « The Modern Context », in Carned Lord et Frank R. Barnett (eds.), *Political Warfare and Psychological Operations*, Washington DC, National Defense University Press, 1989, p. 7.

7. Linda Robinson *et al.*, *Modern Political Warfare*, *op. cit.*, p. 232.

8. Evgeny Morozov, *Pour tout résoudre cliquez ici : l'aberration du solutionnisme technologique*, FYP, 2014.

37 pays en 2018) montre que les répondants estiment que la responsabilité de la lutte contre les manipulations de l'information incombe d'abord aux médias (75 %) et aux plateformes (71 %) et seulement ensuite aux États, surtout en Europe (60 %) et en Asie (63 %), moins aux États-Unis (40 %)[9].

Il faut reconnaître les limites d'une réponse purement gouvernementale, qui sera toujours suspectée d'être biaisée et elle-même propagandiste. La réponse doit être globale. Cela fait longtemps qu'on le sait : dans une conférence de 1952 sur la contre-propagande, le chef de l'Information Research Department, une section secrète du Foreign Office britannique qui a eu jusqu'à 300 personnes chargées de combattre l'influence soviétique au Royaume-Uni, déclarait déjà : « Nous devons dissiper toute idée que les problèmes fondamentaux et les actions qui en découlent ne relèvent que des gouvernements et des organismes contrôlés par eux. L'information parrainée par le gouvernement, les prospectus tendancieux, les déclarations officielles et toutes les tentatives évidentes d'influencer les opinions libres sont pires qu'inutiles, ou devraient l'être[10]. »

De ce point de vue, il est préférable que l'État organise les choix sans les forcer, conformément à l'approche par le *nudge* (encouragement) en économie comportementale[11].

9. Créer une structure dédiée. La plupart des États concernés l'ont déjà fait. Les autres devraient mettre en place une structure nationale chargée de détecter et contrer les manipulations de l'information. Cette structure peut prendre différentes formes, de la simple mise en réseau de personnes ressources aujourd'hui disséminées dans différents services à la création d'un centre doté de son personnel propre. Une question essentielle, car elle implique des luttes bureaucratiques, est celle du rattachement institutionnel : parmi l'existant, certaines structures sont coordonnées par une instance inter ou supraministérielle, quand d'autres sont hébergées au sein d'un ministère. La nature du lien (pouvoir exécutif ou simple rôle de secrétariat) est également variable. En revanche, certaines constantes donnent des indications sur les clés de la réussite d'un bon réseau :

9. *Reuters Institute Digital News Report 2018*, p. 9.

10. *Counter-Propaganda: A Basic Analysis. Extracts from a lecture on counter-propaganda given by the Head of Information Research Department in a secret series of lectures on Communism*, SECRET (18674), n° PR 89/45 G, TNA FCO 141/7460, septembre 1952, posté sur psywar.org, le 30 avril 2012.

11. Richard H. Thaler et Cass R. Sunstein, *Nudge: Improving Decisions about Health, Wealth, and Happiness*, Yale University Press, 2008.

a) la permanence : les structures permanentes avec des compétences et objectifs clairement définis fonctionnent mieux que les initiatives *ad hoc* au sein desquelles les responsabilités sont souvent diffuses[12] ;

b) la géométrie variable : ces réseaux sont en général constitués d'un « noyau » à dominante sécuritaire (Affaires étrangères, Défense, Intérieur, renseignement) qui se rencontre régulièrement et, en fonction de l'ordre du jour, d'un groupe élargi à d'autres ministères (Éducation, Culture, Justice) voire à des parlementaires et des acteurs de la société civile ;

c) l'objet large : ils se présentent publiquement comme luttant contre les manipulations de l'information *en général*, même si dans les faits ils sont souvent focalisés sur la Russie. Théoriquement, ils peuvent traiter d'autres acteurs étatiques (Chine, Iran, etc.) et non étatiques (groupes djihadistes). Un certain nombre d'entre eux travaille d'ailleurs à établir des ponts entre lutte contre les manipulations de l'information et lutte contre la radicalisation ;

d) la composition : les réseaux qui fonctionnent rassemblent un petit groupe de personnes ayant une expérience du monde numérique, qui se connaissent et se font confiance. Si le groupe est trop grand ou trop disparate hiérarchiquement, la discussion sera moins efficace. L'équipe interdisciplinaire doit inclure des spécialistes des systèmes d'information, trop souvent cantonnés à la résolution d'incidents et qui doivent prendre part à la réflexion stratégique. Enfin, les groupes qui fonctionnent le mieux sont ceux qui contiennent au moins certaines personnes à temps plein, entièrement dédiées au sujet ;

e) la production : outre les réunions et le partage d'informations, les meilleurs réseaux sont productifs. On peut penser à trois types de publications internes : des notes d'alerte, des analyses périodiques et des rapports thématiques. Cette structure pourrait aussi diriger la rédaction d'un rapport annuel sur les manipulations de l'information (des services de renseignement – le KAPO estonien – ou même des forces armées – lituaniennes – le font déjà) ;

f) la communication : la transparence étant importante pour dissiper les tentations conspirationnistes, ces réseaux sont publics et communiquent parfois à l'extérieur. Certains, qui sont exposés à la pression la plus forte, en Europe centrale et orientale, notamment les États baltes, n'hésitent pas à mettre en avant le rôle des forces armées et de sécurité dans cet effort quand d'autres adoptent

12. Veronika Vichova et Jakub Janda (dir.), *The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe*, European Values, Kremlin Watch Report, 30 avril 2018, p. 3 et 28.

la stratégie inverse de valoriser les institutions les plus proches de la société civile pour rassurer la population. Au Canada, la responsabilité première de la lutte contre la désinformation revient à la ministre des Institutions démocratiques – dans la mesure où les manipulations de l'information menacent les élections, donc l'intégrité des processus démocratiques.

Quel que soit le rattachement institutionnel de la structure dédiée, le ministère des Affaires étrangères a un rôle important à jouer dans la veille et l'alerte précoce, en particulier concernant les campagnes de manipulation ciblant les intérêts nationaux à l'étranger. Les réseaux diplomatiques peuvent en effet être utilement mis à contribution aussi bien pour alerter sur les campagnes en cours (antennes) que pour diffuser la communication stratégique du ministère (haut-parleurs).

10. Sonder le web pour connaître les communautés propagatrices. Il est difficile d'anticiper la menace. Elle peut en revanche être détectée, et l'objectif est qu'elle le soit le plus tôt possible. Il faut pour cela poser des sondes dans des communautés à risque (extrémistes, conspirationnistes, religieuses, etc.). Ces sondes peuvent être des comptes passifs, qui ne font qu'écouter, ou actifs, qui participent. Des solutions techniques d'écoute des réseaux sociaux existent (DigiMind, AmiSoftware, Linkfluence, etc.).

Les réponses officielles (sites, pages, comptes) ont une efficacité limitée. Les opérations clandestines (manipuler les manipulateurs) sont risquées car, si découvertes (et il est de plus en plus difficile de garantir qu'elles ne le seront pas un jour), elles peuvent décrédibiliser la source et conforter les conspirationnistes, donc renforcer ceux-là mêmes qu'il s'agissait d'affaiblir. Que faire alors ?

La première étape est d'effectuer un travail sur le web pour connaître les communautés propagatrices sur les réseaux sociaux : détecter les principaux acteurs (ce qui peut vouloir dire plusieurs choses : les plus suivis, les plus actifs, les plus connectés, les plus cités, etc.) ; déterminer le type de communauté, sa structure (est-elle centralisée, verticale, horizontale, tribale, etc. ?) et son esprit (est-elle coopérative ou compétitive ? la différence est importante car une communauté compétitive, dans laquelle les membres cherchent la reconnaissance des autres, ne sera pas affectée par le retrait d'un membre clé, un autre prendra simplement sa place). Ce travail de fourmi est important pour comprendre la propagation des messages et pouvoir anticiper et agir.

On peut ensuite a) identifier les comptes à l'origine des manipulations et, au contraire, les comptes « amis » ou au moins neutres, rationnels, dotés

d'une bonne audience ; b) neutraliser les premiers (cyberattaques, suspension) et soutenir les seconds (par des offres de formation par exemple) ; c) dévoiler la manipulation, nommer la source (*naming and shaming*) et discréditer le contenu de la fausse nouvelle – soit directement, officiellement, soit indirectement via les comptes « amis ».

11. Mieux communiquer. Se contenter de réagir augmente le risque de perdre la guerre informationnelle. Pour la gagner, il faut non seulement assurer une présence permanente, avoir une stratégie de communication, des messages à faire passer, réfuter les fausses informations, mais aussi être proactif pour faire sortir l'adversaire de sa zone de confort. Si nos services détectent des trolls ou des bots dormants avant même qu'ils soient utilisés, par exemple, il faut les dénoncer publiquement.

Lorsqu'on est attaqué, il faut communiquer. Les milieux de la défense peuvent avoir tendance à classifier au lieu d'utiliser l'information. On peut dénoncer une attaque sans l'attribuer et laisser les médias faire leur travail. C'est l'une des raisons du succès de la réponse d'En Marche ! à la tentative d'interférence durant la campagne française, et c'est aussi ce que les Allemands ont fait durant leur pré-campagne. La proactivité dans la communication est désormais considérée comme un modèle.

Pour les États dont l'anglais n'est pas une langue officielle, il faut aussi communiquer davantage en anglais sur leur doctrine, leur stratégie nationale, leur expérience.

12. Légiférer lorsque nécessaire. Les États doivent pouvoir prendre les mesures suivantes s'ils l'estiment nécessaire :

a) adopter une législation contre les fausses nouvelles si elle n'existe pas déjà, ou la mettre à jour pour l'adapter au contexte numérique ;

b) sanctionner davantage les dérives médiatiques, en suivant l'exemple de l'Ofcom britannique (qui a sanctionné RT à plusieurs reprises, ce qui semble avoir été efficace, c'est-à-dire dissuasif), et renforcer la législation punissant le harcèlement en ligne, en particulier des journalistes ;

c) envisager l'enregistrement des médias étrangers, en suivant l'exemple américain, ce qui n'affecterait pas leur diffusion (et ne serait donc pas de la censure) mais constituerait simplement une mesure de transparence : le public a le droit de savoir qui parle, selon une logique analogue à celle de la sécurité alimentaire : la traçabilité de l'information doit assurer sa qualité.

Faire évoluer notre dispositif juridique

« J'ai décidé que nous allions faire évoluer notre dispositif juridique pour protéger la vie démocratique de ces fausses nouvelles. Un texte de loi sera prochainement déposé à ce sujet. En période électorale, […] les plateformes se verront ainsi imposer des obligations de transparence accrue sur tous les contenus sponsorisés afin de rendre publique l'identité des annonceurs et de ceux qui les contrôlent, mais aussi de limiter les montants consacrés à ces contenus. […] En cas de propagation d'une fausse nouvelle, il sera possible de saisir le juge à travers une nouvelle action en référé permettant le cas échéant de supprimer le contenu mis en cause, de déréférencer le site, de fermer le compte utilisateur concerné, voire de bloquer l'accès au site internet. Les pouvoirs du régulateur, qui seront par ailleurs profondément repensés durant l'année 2018, seront accrus pour lutter contre toute tentative de déstabilisation par des services de télévision contrôlés ou influencés par des États étrangers. Cela permettra au CSA repensé notamment de refuser de conclure des conventions avec de tels services en prenant en compte tous les contenus édités par ces services, y compris sur internet. Cela lui permettra aussi, en cas d'agissement de nature à affecter l'issue du scrutin, que cela soit en période préélectorale ou électorale, à suspendre ou annuler la convention. […] Ce nouveau dispositif impliquera un devoir d'intervention de la part des intermédiaires techniques afin de retirer rapidement tout contenu illicite porté à leur connaissance. »

(Emmanuel Macron, discours à l'occasion des vœux à la presse, 4 janvier 2018.)

Il faut toutefois veiller à ne pas surréguler, c'est-à-dire à préserver l'équilibre entre la protection de populations et la défense des libertés publiques qui fait nos démocraties libérales. La surrégulation est un réel danger, voire un piège tendu par nos adversaires, qui loin d'être gênés par une réglementation trop zélée, tireront profit des polémiques et des divisions qu'elle créera. Nous devons rester attentifs à ce risque d'effet pervers.

13. Mener des enquêtes parlementaires lorsque nécessaire. Une enquête publique, comme le montrent les exemples américain et britannique, a de nombreux avantages en termes de sensibilisation de la population, d'accumulation de connaissances, voire de dissuasion.

14. Responsabiliser les plateformes numériques. Le rôle des réseaux sociaux dans les manipulations de l'information n'est plus à démontrer : ils sont devenus les principales sources d'information, donc

de désinformation, pour la majorité de la population (ils sont devenus nos « infomédiaires »). En dépit du fait que ces manipulations leur coûtent cher en termes réputationnels et qu'ils ont donné des gages en prenant dernièrement un certain nombre de mesures d'autorégulation, leur volonté de mettre fin à ces pratiques est ambivalente. Nous devons donc trouver les leviers pour, à l'échelle européenne :

a) les obliger à rendre publique l'origine des publicités – en exigeant une transparence équivalente à celle demandée aux médias traditionnels ;

b) les inciter à mettre en place des mesures pour combattre les manipulations de l'information sur leurs sites et contribuer à l'éducation aux médias et à la sensibilisation de la population.

Il revient au législateur de trouver le bon équilibre entre responsabilisation des plateformes numériques dans la lutte contre les fausses nouvelles et respect de la liberté d'expression.

15. Partager des informations avec les plateformes numériques. On ne peut pas, d'un côté, attendre des plateformes qu'elles fassent davantage pour lutter contre les manipulations et, de l'autre, ne pas leur donner les informations qui leur seraient parfois nécessaires pour avancer. La coopération public-privé est capitale et requiert un partage de connaissances dans les deux sens. C'est notamment l'une des recommandations faites par deux anciens hauts fonctionnaires de l'administration Obama à l'administration Trump en vue des élections de mi-mandat de 2018[13].

16. Investir l'international. Ces dernières années, sur la scène internationale, le sujet était dominé par le même groupe d'États d'Europe du Centre, de l'Est et du Nord, ainsi que le Royaume-Uni et les États-Unis. La France et l'Espagne commencent à être plus présentes, parce qu'elles ont été attaquées. Sans attendre de l'être, les autres devraient s'investir davantage. D'une manière générale, on peut recommander de :

a) participer davantage à l'existant. Les États qui en ont les moyens devraient systématiquement envoyer un expert à au moins l'une des *task forces* de l'UE, prioritairement la East ; contribuer aux travaux du centre d'excellence européen pour la lutte contre les menaces hybrides (Hybrid CoE) d'Helsinki ; et participer aux rencontres annuelles importantes (StratCom

13. Joshua A. Geltzer et Dipayan Ghosh, « How Washington Can Prevent Midterm Election Interference », *Foreign Affairs*, 25 juillet 2018.

Summit de Prague, Riga StratCom Dialogue, StratCom de l'Atlantic Council de Washington DC) ;

b) faire se rencontrer les communautés régionales. La scène euratlantique domine mais elle n'est pas la seule : il se passe des choses très intéressantes en Asie, où Singapour s'impose comme une référence. Non seulement les autorités sont proactives et très tournées vers l'extérieur, comme en témoignent les auditions parlementaires et le fait que le ministère de la Défense enverra prochainement un expert en résidence au centre d'excellence de l'OTAN à Riga, mais la société civile n'est pas en reste. Le Centre of Excellence for National Security (CENS) de la S. Rajaratnam School of International Studies (RSIS) organise un séminaire annuel sur la désinformation qui est l'un des très rares points de rencontre entre les communautés de chercheurs et de praticiens issus d'Europe, d'Amérique du Nord, d'Asie et d'Afrique. Pour les habitués de la scène euratlantique qui ont tendance à ne penser le sujet qu'à travers le prisme russe, ce pluralisme est rafraîchissant. Les situations sont certes très différentes (les manipulations de l'information en Inde, en Birmanie ou en Indonésie sont préoccupantes mais endogènes, donc assez éloignées des ingérences russes en Europe et Amérique du Nord), mais à mesure que la Chine se fait plus offensive dans la région, comme en témoigne le cas australien, les parallèles avec la Russie – et la question de savoir ce qu'elles apprennent l'une de l'autre – se feront plus intéressants ;

c) innover en créant de nouveaux mécanismes. Les manipulations de l'information étant souvent internationales, la question de la coordination est essentielle. On peut par exemple imaginer un mécanisme international d'alerte précoce pour connecter tous les réseaux/centres/agences des pays de l'UE et de l'OTAN. Il ne faut pas nécessairement créer un nouveau réseau : entre la East StratCom Task Force de l'UE, le centre d'excellence d'Helsinki et celui de Riga, les *hubs*, points de rencontre pour les équipes nationales, existent déjà.

Certains, notamment aux États-Unis, proposent la création d'une coalition internationale. Dans leur rapport de janvier 2018, les sénateurs démocrates recommandent la création d'une « coalition internationale contre les menaces hybrides », dont Washington prendrait la tête. Ils suggèrent au président de convoquer un sommet mondial annuel sur les menaces hybrides, sur le modèle des sommets de la Coalition mondiale contre Daech ou pour contrer l'extrémisme violent, qui ont lieu depuis 2015. La société civile et les acteurs privés y participeraient[14].

14. Bob Corker *et al.*, *Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security*, *op. cit.*, p. 5.

Deux mois plus tard, Fried et Polyakova font une proposition similaire : la création d'une « coalition anti-désinformation » par « les États-Unis et l'UE », « un groupe public-privé réunissant de manière fréquente des acteurs gouvernementaux et non gouvernementaux aux vues similaires, y compris des sociétés de médias sociaux, médias traditionnels, fournisseurs d'accès et société civile[15] ». L'idée de créer un réseau intégrant les acteurs non gouvernementaux est excellente mais, formulée de cette manière, elle nous semble problématique non seulement parce qu'elle oublie le Canada, mais aussi parce que cette alliance transatlantique existe déjà (l'OTAN) et qu'il faudra expliquer à Moscou, qui ne manquera pas de le demander, pourquoi il ne peut pas, lui aussi, rejoindre cette *coalition of the willing*, au risque d'apparaître davantage anti-russe qu'anti-désinformation. Les structures existantes, de l'UE ou de l'OTAN, ne prêtent pas le flanc à cette critique.

En mai 2018, l'ancien vice-président américain Joe Biden, l'ancien secrétaire à la Sécurité intérieure Michael Chertoff et l'ancien secrétaire général de l'OTAN Anders Fogh Rasmussen ont créé une Commission transatlantique sur l'intégrité électorale. C'est un nouvel acteur à suivre, même s'il est encore trop tôt pour savoir quel rôle il jouera.

Enfin, le G7 constitue un forum naturel pour partager les meilleures pratiques et décider d'approches communes pour la lutte contre les manipulations informationnelles. Le Canada en a fait l'une des priorités de sa présidence du G7 en 2018, en proposant différents mécanismes d'échange et d'action commune. La France, qui prendra la présidence du G7 en 2019, devrait s'appuyer sur ces premiers résultats pour poursuivre les efforts dans ce forum, sous l'angle de la préservation et de la défense de la démocratie.

17. Former les adultes comme les enfants (éducation aux médias et pensée critique). L'éducation aux médias est l'une des recommandations les plus consensuelles, quoiqu'inégalement appliquée par les États comme en témoigne le classement de l'Open Society Institute[16]. Toutefois, si on la limite aux écoles, comme c'est souvent le cas, c'est aussi une mesure de long terme, qui ne produira ses effets que lorsque les enfants seront devenus adultes. Il faut considérer l'éducation aux médias et plus largement le développement de l'esprit critique de l'ensemble de la population, à tous

15. Daniel Fried et Alina Polyakova, *Democratic Defense Against Disinformation*, Atlantic Council, 2018, p. 13-14.

16. Open Society Institute (Sofia), *Media Literacy Index 2018*. Voir Marin Lessenki, *Common Sense Wanted: Resilience to "Post-Truth" and its Predictors in the New Media Literacy Index 2018*, mars 2018.

les âges de la vie. Former les adolescents et les étudiants est particulièrement important car ils sont en général plus vulnérables aux manipulations de l'information pour des raisons diverses (manque de repères, besoin de s'affirmer, environnement socio-culturel) et ils n'ont pas nécessairement bénéficié d'une éducation aux médias en amont. Proposer un module de tronc commun en première année d'université (analyses de texte, images et identification des sources) serait utile et facile à mettre en place, au moins dans l'ensemble des cursus en sciences humaines.

L'idée est de faire en sorte que, face à une information, chaque personne interroge sa validité (arguments, preuves) et sa source (fiabilité, motivations). C'est une mesure d'hygiène publique – comme il a fallu, au XIX^{e} siècle, apprendre à se laver les mains. On peut d'ailleurs suivre le modèle suédois et publier un *Guide d'hygiène informatique* pour les politiciens et partis politiques.

Autrement dit, il faut former le grand public, dès le plus jeune âge mais pas seulement, à l'éducation à l'image et aux médias audiovisuels, à la pensée critique et à l'argumentation rationnelle. Vérifier la fiabilité des informations peut s'apprendre. Les cours de pensée critique et d'argumentation rationnelle sont courants dans certains pays et même considérés comme des prérequis indispensables à l'université. On y apprend à reconnaître des paralogismes et des sophismes, des raisonnements fallacieux. Ces pratiques d'« autodéfense intellectuelle » doivent se répandre[17].

a) En général, les mesures mises en place sont limitées par au moins deux facteurs : les enseignants sont insuffisamment formés et ils n'ont pas assez de temps pour insérer cette activité dans le programme. Les gouvernements doivent y être attentifs et trouver des solutions.

b) Une partie de l'éducation devrait consister à faire prendre conscience de ce qu'il est déjà possible de faire (trolls, bots, *deep fake*, etc.). Dans les écoles, faire non seulement déconstruire mais aussi construire de fausses informations et des théories conspirationnistes aux enfants : cela leur permet de les décristalliser (si eux sont capables de le faire, ils comprennent que les adultes aussi, et sans doute mieux). Leur apprendre également à utiliser Google images pour vérifier l'origine d'une image, par exemple. Et leur apprendre non seulement à décrypter mais aussi à débattre, et plus spécifiquement à débattre en ligne, par des ateliers, des simulations, etc.

c) L'éducation aux médias doit inclure un volet sur l'environnement médiatique, en particulier le modèle économique, le rôle de la publicité en

17. Normand Baillargeon, *Petit Cours d'autodéfense intellectuelle*, Montréal, Lux, 2005.

ligne, etc. L'éducation aux médias doit aussi inclure une dimension technologique pour faire comprendre comment les algorithmes des réseaux sociaux opèrent (personnalisation, bulles de filtrage). C'est un défi en soi d'expliquer aux enfants ce que la plupart des adultes ont déjà du mal à comprendre.

d) Ne pas se limiter aux salles de classe : pour accroître leur efficacité, les enseignements à la vérification d'information devraient utiliser tout un panel de diffuseurs, dont la télévision, qui continue malgré tout à toucher les jeunes publics. Ceci pourrait inclure des messages de sensibilisation précédant les vidéos sur YouTube, ou encore envoyés par les plateformes en messages privés, par exemple sur Snapchat ou Instagram.

e) Les adultes peuvent être touchés par des campagnes publiques, à l'occasion d'événements particuliers, et via des formations. On peut suivre l'exemple de l'ONG Baltic Centre for Media Excellence qui forme des journalistes et des enseignants dans toute la région. Dans la fonction publique, et notamment les ministères et services les plus concernés, former les agents pour renforcer l'« hygiène informatique » et se doter d'une expertise interne leur permettant d'agir de manière autonome ; cela passe par de nouveaux modes de recrutement, de formation, de partenariats public-privé et de mobilité de nos agents vers les entreprises innovantes permettant l'acquisition de ces nouveaux savoirs. Des structures similaires à l'Institut des hautes études de défense nationale (IHEDN) pourraient offrir des formations dédiées aux menaces informationnelles.

f) La dimension ludique est importante, car les manipulations de l'information sont souvent divertissantes et la réponse manquera une partie de sa cible si elle paraît ennuyeuse (voir recommandation n° 20). De ce point de vue, des jeux tels que celui développé sur Facebook par le centre d'excellence de l'OTAN sur la communication stratégique, peuvent être très utiles pour intéresser les jeunes (et les moins jeunes)[18]. Autre exemple : le site Buzzfeed fait chaque semaine un « Fake News Quiz » qui a beaucoup de succès.

18. Soutenir la recherche. Notre défense immunitaire contre l'infection informationnelle repose non seulement sur notre capacité de surveillance et d'analyse de l'espace informationnel – ce qui suppose d'y consacrer davantage de moyens en termes de renseignement – mais aussi sur notre capacité à comprendre les acteurs ayant recours à la manipulation

18. « The News Hero » (https://apps.facebook.com/thenewshero).

de l'information, à commencer par la Russie. Il faut donc soutenir la recherche sur la Russie et les espaces post-soviétiques. Il ne s'agit pas de ressusciter la soviétologie mais de se rendre à l'évidence qu'on ne peut répondre adéquatement qu'à ce que l'on connaît bien.

Concrètement, cela signifie que les États doivent accroître le financement de la recherche en lançant des appels d'offres pour des études sur des thèmes prédéterminés, voire en finançant des doctorats et/ou des postdoctorats, ainsi que des événements (colloques) et des publications. Le lien avec les manipulations de l'information peut être soit direct (lorsqu'il s'agit de l'objet de la recherche en question), soit indirect, puisqu'il peut être utile de soutenir des projets annexes en informatique, en psychologie sociale ou en science politique par exemple, qui apporteront des pièces au puzzle.

19. Marginaliser les organes de propagande étrangers. Il faut d'abord les appeler par leur nom. À peine élu, le président français l'a fait, à Versailles devant Vladimir Poutine, dans un passage remarqué dans le monde entier :

> Russia Today et Sputnik ont été des organes d'influence durant cette campagne qui ont, à plusieurs reprises, produit des contre-vérités sur ma personne et ma campagne. […] Il était grave que des organes de presse étrangers – sous quelque influence que ce soit, je ne le sais – aient interféré en répandant des contre-vérités graves dans le cadre d'une campagne démocratique. Et à cela je ne céderai rien, rien […] Russia Today et Sputnik ne se sont pas comportés comme des organes de presse et des journalistes, mais ils se sont comportés comme des organes d'influence, de propagande, et de propagande mensongère, ni plus, ni moins[19].

Ensuite, il faut en tirer les conséquences, c'est-à-dire ne pas les accréditer et ne pas les inviter à des conférences de presse réservées aux journalistes.

20. Utiliser l'humour et le divertissement. Il est souvent reproché aux contre-mesures de manquer leur cible faute d'être divertissantes – car les manipulations de l'information, elles, le sont généralement. Nombreux sont ceux qui consomment les *fake news* comme la *junk food* : en sachant que c'est mauvais mais pour se faire plaisir. RT et Sputnik pratiquent l'*infotainment*, un mélange d'information et de divertissement, à côté duquel les corrections apportées peuvent sembler bien austères. Or, ce que confirment quelques

19. Emmanuel Macron, dans une conférence de presse conjointe avec le président Vladimir Poutine, le 29 mai 2017 à Versailles.

années d'expérience en Europe et en Amérique du Nord est que l'humour, la satire, le canular, la moquerie, fonctionnent particulièrement bien contre les manipulations de l'information. La société civile l'a bien compris : il y a des émissions satiriques (« Derzites tam ! » en Lituanie), des prix satiriques (le Putin's Champion Award du think tank European Values), des comptes satiriques sur les réseaux sociaux (Darth Putin sur Twitter, qui donne des conseils du type « *Do not believe *anything* until the Kremlin denies it* »), etc. L'East StratCom Task Force fait aussi preuve d'humour sur son site EUvsDisinfo et sur les réseaux sociaux. Même si ce n'est pas leur registre naturel, les États ne doivent pas non plus exclure d'utiliser l'humour et le divertissement pour communiquer dans certains contextes (la Suède le fait très bien pour déminer certains clichés sur Sweden.ru, par exemple).

21. Être conscients de nos vulnérabilités. Les manipulations informationnelles exploitent les vulnérabilités de nos sociétés démocratiques. Il faut donc en faire la cartographie, les identifier, les comprendre, pour anticiper où porteront les coups et tâcher de les prévenir. La capacité à nous mettre à la place de nos adversaires est essentielle pour mieux anticiper leurs objectifs. À cette fin, nous devons non seulement davantage les étudier pour mieux les comprendre (recherche et renseignement) mais aussi tester nos procédures avec des *red teams*, des équipes jouant le rôle de l'adversaire et s'efforçant d'identifier et exploiter nos vulnérabilités.

22. Être conscients de ce pour quoi nous nous battons. Les manipulations informationnelles cherchent à installer un doute systématique quant aux valeurs et principes des communautés qu'elles ciblent. La meilleure façon de lutter contre ces manipulations consiste, en premier lieu, à savoir ce que nous souhaitons protéger.

23. Accepter l'inévitabilité du retournement et détournement de nos contre-mesures. Elles seront retournées par l'adversaire, parfois dans un effet miroir (RT a son FakeCheck en quatre langues, le site du ministère russe des Affaires étrangères a, depuis février 2017, une section intitulée « Published materials that contain false information about Russia », etc.), ou détournées par lui voire par des États tiers (les illibéraux profitant du sujet pour passer des lois liberticides). Il faut donc privilégier les approches positives de promotion d'une information de qualité qui puisse circuler librement, loin des logiques de fragmentation actuellement à l'œuvre sur internet.

24. Être attentifs aux signaux faibles en dehors du prisme russe (d'autres États, des acteurs non étatiques) ou contre nos intérêts en dehors de l'Europe (notamment en Afrique et au Moyen-Orient).

25. Écouter la société civile, et notamment les journalistes. Un dialogue régulier et libre entre journalistes et décideurs politiques peut aider à lutter contre les manipulations de l'information. En Suède, un Conseil des médias réunit régulièrement responsables médias et politiques pour identifier les enjeux, et, de façon cruciale, pour coordonner leurs actions de vérification des faits[20]. Le groupe d'experts belge recommande la création d'une « plateforme de concertation » réussissant tous les acteurs concernés (« universités, médias, journalistes et écoles de journalisme, ONG, plateformes[21] »). Cette excellente idée – qui sera toutefois plus facile à mettre en œuvre dans les petits pays, où ces acteurs sont moins nombreux – offrirait aussi un interlocuteur à l'État qui pourrait consulter cette plateforme de concertation.

26. Lutter contre les autres formes d'influence. Les manipulations de l'information ne sont qu'une partie d'un système complexe, elles se nourrissent d'autres types d'influence. Dans le cas russe, par exemple, les États visés devraient aussi réduire leur dépendance énergétique vis-à-vis de la Russie et lutter contre la corruption et l'argent russe qui contribuent à financer les opérations d'influence.

27. En opération militaire extérieure, soigner les relations avec les populations locales. Ne jamais oublier que « chaque action projette une image, génère une perception auprès de l'adversaire, des populations locales mais également aujourd'hui des audiences domestiques et internationales. Une troupe en opération est donc le premier acteur de l'influence et celle-ci ne se résume pas aux actions non létales[22] ». Dans le cadre de la présence avancée de l'OTAN dans les États baltes, des soldats américains en Lettonie ont rendu des services aux communautés russophones

20. Erik Brattberg et Tim Maurer, « Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks », Carnegie Endowment for International Peace, 23 mai 2018.

21. Alexandre Alaphilippe *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, *op. cit.*, p. 12.

22. Bertrand Boyer, « Les opérations sur l'environnement : la nouvelle guerre de l'information », in Stéphane Taillat, Amaël Cattaruzza et Didier Danet (dir.), *La Cyberdéfense. Politique de l'espace numérique*, *op. cit.*, p. 212.

(par exemple couper du bois), ce qui a augmenté leur cote de popularité et contribué à affaiblir la propagande anti-américaine véhiculée par les médias russes que ces communautés consomment[23].

28. Sanctionner les responsables en cas d'ingérence grave, notamment dans un processus électoral, si l'attribution le permet – par des sanctions économiques, par exemple, et des poursuites judiciaires (le procureur spécial américain Robert Mueller a inculpé 13 Russes et 3 entités russes en février 2018 puis 12 officiers du GRU en juillet 2018).

III. Recommandations à la société civile

29. Comprendre et renforcer les mécanismes de confiance numérique. Les manipulations de l'information sont à la fois une cause et un symptôme de la crise de confiance dans l'espace numérique. Lutter efficacement contre ces manipulations devrait donc contribuer, à terme, à augmenter le niveau de confiance mais, en même temps, cela exige de comprendre les mécanismes psychologiques de la confiance, en se plaçant du point de vue des utilisateurs, et de promouvoir les bonnes pratiques la renforçant. Les coopérations permettant d'établir des indices de fiabilité des contenus sont utiles de ce point de vue.

30. Développer la vérification des faits tout en ayant conscience de ses limites. Puisque nous avons tendance à ne pas tenir compte de la correction, surtout si elle remet en cause une croyance profonde, la vérification des faits peut être efficace sur une personne donnée à deux conditions : d'une part, si la correction n'est pas une remise en cause directe de sa vision du monde (sans quoi elle peut même avoir l'effet pervers de la renforcer – on l'a vu dans le cas des armes de destruction massive en Irak, du changement climatique ou encore des vaccinations) et, d'autre part, la correction doit expliquer pourquoi et comment la désinformation a été disséminée[24].

31. Développer les outils simples permettant aux citoyens de démasquer eux-mêmes les manipulations de l'information, comme

23. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 89.

24. Stephan Lewandowsky, Ullrich Ecker et John Cook, « Beyond Misinformation », *op. cit.*, p. 355.

savoir qui se cache derrière une publicité (whotargets.me) ou détecter des vidéos trafiquées (projet InVID de l'AFP), par exemple.

32. Développer les initiatives normatives (classements, index, labels) tout en ayant conscience qu'une multiplicité de normes concurrentes nuira à l'ensemble de l'effort. L'objectif doit donc être de faire émerger quelques outils de référence, autour d'ONG reconnues. L'initiative de RSF a du potentiel de ce point de vue.

33. Adopter une charte d'éthique journalistique internationale de façon collaborative (par association des grands médias traditionnels et en ligne). La plupart des grands médias ont des chartes de bonnes pratiques éditoriales et déontologiques[25] qui pourraient converger. La charte de Munich de 1971 peut servir de base mais elle doit être adaptée au paysage médiatique actuel, notamment numérique.

34. Mieux former les journalistes aux risques des manipulations de l'information, dans les écoles de journalisme et tout au long de leur carrière. Comment couvrir une fuite massive de données (*leak*), détecter un faux profil ou réagir aux contenus extrémistes ? Il existe des réponses concrètes[26], qui peuvent faire l'objet d'enseignements et de formations.

35. Renforcer la confiance à l'égard du journalisme en développant la transparence. The Trust Project[27], un consortium réunissant notamment *The Economist*, *The Globe and Mail*, *La Repubblica* ou *The Washington Post*, recommande de révéler les financements (de la même manière, le site *The Conversation* exige des chercheurs qui y publient qu'ils révèlent d'éventuels conflits d'intérêts, une pratique courante dans les revues scientifiques), les profils des journalistes, la justification de leur expertise, la distinction entre une opinion, une analyse ou un contenu sponsorisé, comment s'est fait l'accès aux sources, pourquoi le journaliste a préféré poursuivre telle hypothèse plutôt qu'une autre, etc. L'idée est que les lecteurs veulent savoir comment les journalistes travaillent, comment ils savent ce qu'ils savent : cette transparence sur les pratiques, les méthodes et les procédures journalistiques peut contribuer à renforcer la confiance.

25. Voir notamment celle de l'AFP du 22 juin 2016.

26. Voir par exemple Heidi Tworek, « Responsible Reporting in an Age of Irresponsible Information », Alliance for Securing Democracy (GMF) Brief 2018, n° 009, mars 2018, p. 4.

27. Thetrustproject.org

36. Développer des outils de lutte contre le *trolling*, comme Perspective de Jigsaw, qui en utilisant l'auto-apprentissage identifie des commentaires incendiaires, qui peuvent ensuite être isolés, suspendus avant leur publication, puis soumis à des modérateurs. Le *New York Times* utilise cet outil sur son site. Une autre méthode est de publier des listes de comptes identifiés comme étant des trolls.

37. Utiliser l'intelligence artificielle et le traitement automatique du langage dans la détection des manipulations et la vérification des faits. La profusion de nouvelles fausses ou biaisées est telle que les journalistes, les analystes et les chercheurs ne seront jamais assez nombreux pour les repérer et les traiter. Les logiciels de détection, tels que Storyzy, sont sans cesse plus perfectionnés et plus nombreux. Quant à la vérification des faits, les logiciels peuvent automatiquement comparer la nouvelle incriminée avec toutes celles qui ont déjà été « démythifiées », pour ne pas refaire le travail pour rien, mais cela suppose d'avoir accès à des bases de données communes – d'où l'importance des réseaux de vérificateurs. La vérification automatisée permet de gagner du temps, mais requiert toujours, pour l'instant, un humain à la fin du processus pour valider.

38. Développer les enquêtes et sondages visant à évaluer la sensibilité du public aux manipulations de l'information. Des données précises et régulières permettraient d'améliorer l'efficacité des contre-mesures qui les prendraient en compte.

39. Développer le pluralisme par des outils promouvant la diversité de l'information, afin de contourner le phénomène des « bulles filtrantes » : plusieurs projets, dont le NewsDNA de l'université de Gand, devraient permettre aux citoyens de régler le degré de diversité des nouvelles qu'ils consomment[28].

40. Repenser le modèle économique du journalisme afin de concilier préservation de la liberté d'expression, libre concurrence du marché et lutte contre les manipulations de l'information.

28. Alexandre Alaphilippe *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, *op. cit.*, p. 9.

41. Inciter les chercheurs à intervenir dans le débat public. La pseudo-science prolifère parce qu'elle occupe un terrain trop souvent laissé vacant par les véritables scientifiques : celui de la diffusion du savoir scientifique (ou vulgarisation). Trop de chercheurs délaissent cette activité, considérant que l'exposition médiatique constitue un dévoiement éthique et un frein dans leur carrière. Cependant, dans ce contexte de brouillage et de confusion, la reponsabilité sociale des universitaires n'a jamais été aussi grande : ils se doivent de rendre accessibles aux non-spécialistes le résultat de leurs travaux et ainsi occuper le débat public. Les établissements d'enseignement supérieur doivent ainsi organiser des formations de type *media training* à cet exercice de diffusion de la recherche, qui répond à des « codes » spécifiques. De plus, la diffusion de la recherche doit être davantage valorisée dans la carrière et constituer un critère d'évaluation majeur, afin d'inciter les universitaires à pratiquer l'exercice.

IV. Recommandations aux acteurs privés

42. Repenser le statut des plateformes : prendre les plateformes au mot et exercer une pression politique forte afin que ces dernières s'engagent, dans des codes de conduite exigeants, à ce que leurs missions affichées s'incarnent au niveau opérationnel (algorithmes, modération, effort de police sur les réseaux, etc.). Au-delà, il convient de réfléchir à un statut hybride entre média et hébergeur, permettant de prendre en compte les missions de service public dont les plateformes digitales ont *de facto* assumé la charge (agora digitale, principal portail d'accès à l'information). La question d'une régulation anti-trust évoquée dans le cadre du groupe d'experts établi par la Commission européenne (voir *supra*) doit être posée.

43. Exiger un nouveau contrat avec les usagers, fondé sur de nouveaux droits digitaux. Les termes de référence doivent être repensés afin de les rendre intelligibles pour tous et explicites sur l'accès et l'usage des données personnelles. Il est important de restituer aux internautes un pouvoir de contrôle accru sur le devenir de leurs données (on peut imaginer un système d'*opt-in*, un régime payant assurant une ou plusieurs des fonctions suivantes : confidentialité des données, blocage des publicités, traçabilité des données personnelles).

44. Imposer un niveau élevé de transparence. Après le scandale Cambridge Analytica, les appels génériques à davantage de transparence ne suffisent plus. Les usagers doivent être informés des campagnes dont ils

sont la cible, et les raisons de ce ciblage. Les publicités politiques associées à l'exploitation des *big data* doivent faire l'objet d'une régulation spécifique compte tenu des enjeux qu'elles représentent pour nos démocraties. L'idée d'un médiateur public qui aurait accès aux algorithmes sous couvert d'une obligation de stricte confidentialité a dans ce contexte été évoquée.

45. Élever le coût des manipulations de l'information tout en protégeant les mouvements et individus vulnérables. Une lutte plus systématique doit être engagée contre les agents de la manipulation, à partir du concept de *threat actor* issu du champ de la cybersécurité. Cette notion permet d'identifier une chaîne de commandement et des infrastructures communes à différentes opérations. Plutôt que de censurer des contenus problématiques un à un (*whack-a-mole approach*), les plateformes procèdent à une investigation permettant d'identifier un acteur hostile et d'en censurer l'ensemble des manifestations, sur le modèle de la fermeture de toutes les pages Facebook liées à l'IRA. Les lanceurs d'alerte et organisations visés par une campagne de manipulation de l'information doivent à l'inverse être alertés en amont grâce à des systèmes de détection dédiés, et bénéficier de procédures de protection (*hotline*) pour leur permettre de se défendre.

46. Valoriser et mieux rétribuer un journalisme de qualité. Le système actuel n'est plus tenable, les plateformes digitales ayant accaparé l'essentiel des revenus publicitaires autrefois alloués au financement des médias tout en aspirant leurs contenus primaires sans les rétribuer. Il est nécessaire de réfléchir à de nouvelles modalités de redistribution de la valeur ajoutée informationnelle des plateformes vers les médias de qualité.

47. Faire contribuer financièrement les plateformes au journalisme de qualité, en leur faisant financer des outils de vérification des faits, par exemple.

48. Faire contribuer les plateformes au financement d'une recherche indépendante : les experts s'accordent sur la nécessité d'accéder aux données des plateformes pour pouvoir mesurer l'impact des campagnes de manipulation de l'information, comprendre les modalités de leur viralité et évaluer l'effet des mesures de lutte contre les fausses informations. Les plateformes doivent contribuer au financement de ces efforts de recherche sans imposer des conditionnalités cachées sur l'orientation de la recherche ou le positionnement politique des chercheurs vis-à-vis des sponsors.

49. Réfléchir à la mise en place de *safe zones* : compte tenu de l'asymétrie d'information, les défis posés aux démocraties par la désinformation en ligne ne sauraient être relevés sans la coopération des plateformes digitales, ce qui suppose de recréer les conditions d'un dialogue constructif. Il convient donc d'imaginer la création de lieux d'échange où seraient garantis les droits de propriété intellectuelle des plateformes en échange d'un accès facilité à leurs données, logiciels et algorithmes. Ces lieux doivent permettre de favoriser la collaboration entre chercheurs, société civile et plateformes numériques. Cela suppose, notamment suite à l'affaire Cambridge Analytica, l'établissement préalable d'un cadre pour une recherche éthique sur le modèle des protocoles d'accès des médecins aux dossiers des patients.

50. Explorer les méthodes de redirection pour que ceux qui cherchent une fausse nouvelle tombent sur de la démystification (*debunking*). Google Redirect, par exemple, aurait fait ses preuves pour réduire l'attrait de Daech, en identifiant de potentielles recrues (d'après leur historique de recherche) et en les exposant à des vidéos sur YouTube démythifiant Daech. L'idée est d'appliquer cette méthode à d'autres manipulations de l'information[29].

V. Réponses aux objections

Les réponses aux manipulations de l'information suscitent dans de nombreux pays des inquiétudes parfois sincères, d'autres fois feintes et instrumentalisées, des polémiques politiciennes, mais dans tous les cas des débats légitimes en démocratie. Dans les pages suivantes, nous recensons les principales critiques et tâchons d'y apporter quelques éléments de réponse.

On peut distinguer quatre catégories de critiques vis-à-vis des réponses aux manipulations de l'information : 1) le combat ne serait pas pertinent, les vrais problèmes seraient ailleurs ; 2) les solutions proposées ne seraient pas efficaces ; 3) elles seraient contre-productives, voire dangereuses ; 4) d'autres arguments plus polémiques que sérieux mais néanmoins courants.

29. Todd C. Helmus *et al.*, *Russian Social Media Influence*, *op. cit.*, p. 77.

A. Une cause non pertinente ?

« Rien de nouveau sous le soleil » : l'utilisation politique de l'information est une pratique ancestrale. Ce qui se passe aujourd'hui n'a rien de nouveau par rapport à la guerre froide.

→ La situation actuelle présente au moins trois différences essentielles par rapport au passé et en particulier à l'époque de la guerre froide :

– les réseaux sociaux démultiplient les effets des manipulations de l'information (vitesse de circulation, ampleur et diversité des publics touchés, impact élevé pour un coût nul) ;

– l'objectif n'est plus aujourd'hui la défense des vertus d'une idéologie ou d'un modèle (l'URSS), mais de dénigrer les États occidentaux et de polariser les sociétés ;

– les acteurs non étatiques jouent un rôle majeur dans la phase présente, ils interagissent entre eux et avec les puissances étatiques d'une façon à la fois plus systématique et plus diluée (cf. les déclarations de Vladimir Poutine sur les « patriotes russes » en ligne).

Le rôle de la désinformation dans les crises récentes (Brexit, élection américaine) est surévalué. Il n'existe d'ailleurs aucune recherche concluante permettant de démontrer que les fausses nouvelles ont un impact réel et direct sur les internautes. À l'inverse, y répondre de façon ostensible revient à leur accorder trop d'importance.

→ Les expériences récentes démontrent au contraire qu'il convient de ne pas sous-estimer la gravité des manipulations informationnelles. L'affaire Lisa en Allemagne a eu des conséquences bien réelles en termes de montée des sentiments anti-migrants, et ces effets sont le plus souvent irréversibles, quels que soient les efforts de rétablissement de la vérité *a posteriori*.

L'administration Obama a fait le choix, pour différentes raisons, de ne pas alerter l'opinion sur la campagne de manipulation de l'information dont le pays était alors victime, facilitant ainsi le déroulement de l'entreprise de déstabilisation démocratique alors en cours. À l'inverse, la Chancelière allemande a publiquement évoqué les risques de manipulations à la suite de l'attaque sur le Bundestag en 2015. C'est ce dernier modèle que la France a suivi avec les « Macron Leaks », modèle qui a prouvé son efficacité.

Les plateformes numériques sont les coupables idéaux que vous blâmez de tous les maux de vos sociétés. Or, la technologie est neutre, ces plateformes ne sont que des espaces sans préférences où s'expriment librement les internautes.

→ Pour reprendre les termes du lanceur d'alerte qui a révélé le scandale Cambridge Analytica, « le couteau est neutre, mais il peut être utilisé pour cuisiner ou pour tuer quelqu'un ». Cette neutralité *a priori* des plateformes impose justement des principes forts et des règles claires pour éviter qu'elles ne soient détournées à des fins néfastes ou pour servir des projets hostiles à nos démocraties et au bien-être de nos citoyens. Il est temps que les plateformes prennent la mesure de la responsabilité qui est la leur et que les États tirent toutes les conséquences de ce dernier scandale en termes de législation.

B. Des solutions inefficaces ?

Les solutions proposées (éducation aux médias, mise en avant de contenus de qualité) ne serviront qu'à convaincre ceux qui le sont déjà et n'auront aucun effet sur les publics les plus exposés à la désinformation (complotistes, groupes radicaux, etc.).

→ Les campagnes actuelles de manipulation de l'information parviennent à semer le doute et la confusion parmi un vaste public qui dépasse largement les communautés complotistes, alternatives et radicales. Les efforts d'éducation aux médias, de vérification des faits et de soutien à un journalisme de qualité visent à renforcer la résilience et l'immunité du public en général face à ces tentatives de manipulation. Nous sommes conscients du fait que les opinions les plus conspirationnistes ou radicales ne seront pas modifiées, mais elles sont minoritaires et doivent le rester.

L'effet contre-productif : les projets de classement et d'index des sources d'information fiables (notamment celui de RSF) risquent d'avoir l'effet inverse : la méfiance de l'opinion vis-à-vis de l'establishment pourrait inciter de nombreux internautes à aller chercher leur information partout sauf via les médias classés fiables.

→ Dans le chaos informationnel actuel, il est important que le public puisse disposer de références objectives permettant de juger de la fiabilité des sources d'information. Les efforts d'organisations non gouvernementales et indépendantes telles que RSF visant à créer un consensus de la profession sur les critères objectifs d'un journalisme de qualité (méthode

de travail, recoupement des informations, procédure de rectification en cas d'erreur, gouvernance du média etc.) sont, dans ce contexte, très utiles. Afin d'éviter un effet contre-productif, les efforts de classification ou de labélisation des médias doivent offrir des garanties en termes de transparence du processus, de qualité des critères et du caractère inclusif et divers des juges de ces critères.

L'argument de la diversion : ce sujet qui fait la une des médias détourne l'attention des vrais sujets de fond, en particulier la question de la concentration du contrôle des médias dans les mains d'intérêts privés.

→ La prise en compte des problèmes sérieux posés par les manipulations de l'information n'exclut pas les autres dimensions de ce qui ressemble à une crise profonde de la communication politique au XXIe siècle. Le président de la République, dans ses vœux à la presse le 3 janvier dernier, avait d'ailleurs évoqué la question des conflits d'intérêts entre actionnaires et rédactions et proposé des pistes d'action pour garantir la pleine indépendance rédactionnelle des médias.

C. Un danger pour les libertés ?

L'argument liberticide : sous couvert de lutte contre les fausses nouvelles, on assiste à une reprise en main par les États du champ informationnel avec des risques très réels pour la liberté d'expression. En Égypte, le régime a exigé la fermeture de 21 sites d'informations accusés de diffuser des fake news. *Parmi les sites censurés figurait entre autres le journal* MadaMisr*, indépendant, progressiste et opposé au pouvoir en place*[30]*. Le remède est ainsi pire que le mal.*

→ En France, la proposition de loi contre les manipulations de l'information actuellement débattue présente de nombreuses garanties : il s'agit d'un dispositif limité dans le temps puisqu'il ne s'applique qu'aux campagnes électorales, il repose par ailleurs sur le renforcement des pouvoirs du juge judiciaire, gardien des libertés, et du CSA, autorité publique indépendante chargée de veiller à la liberté d'expression audiovisuelle. L'objectif essentiel de ce projet est simplement de faire respecter l'honnêteté et la sincérité du scrutin, afin qu'il reflète fidèlement l'expression

30. Tourya Guaaybess, « *Fake news :* de l'instrumentalisation d'un terme à la mode ou les nouveaux visages du "Schmilblick" », *The Conversation*, 11 février 2018.

de la volonté populaire. Il ne s'agit donc pas d'établir un « ministère de la vérité ».

→ Les acteurs des médias et de la société civile sont précisément impliqués dans le processus d'élaboration de la loi, ce qui offre une garantie contre les risques que l'État ne porte atteinte à des libertés fondamentales en voulant lutter contre les manipulations de l'information.

Le risque de retournement : la dénonciation des fausses nouvelles se retourne partout contre les journalistes eux-mêmes. L'anathème de fake news *est devenu un instrument commode de justification de la censure aux mains des dictateurs et des régimes illibéraux.*

→ C'est un risque réel que nous prenons très au sérieux. Nous avons fait le choix résolu de répondre aux manipulations informationnelles de manière transparente et démocratique, en collaboration avec les acteurs de la société civile et les médias. Ces réponses, qui s'appuient sur les piliers de notre État de droit et le caractère ouvert de nos sociétés, sont par nature plus difficiles à « retourner » en contexte autoritaire. Lorsque nous luttons contre les manipulations de l'information, nous nous tournons soit vers le juge judiciaire protecteur des libertés, soit vers le CSA, autorité publique de régulation indépendante qui a pour mission de garantir la liberté de communication audiovisuelle. La France veillera, à chaque étape de la formulation de solutions, à ce que les conséquences potentielles pour la liberté d'expression en contexte illibéral et autoritaire soient dûment prises en compte. À l'instar du MSB suédois, « nous recommandons la vigilance, pas la paranoïa[31] ».

L'inquiétude pour la diversité informationnelle. À trop vouloir définir ce qu'est la « bonne information » et mettre en avant les contenus « de qualité », on risque de réduire la diversité des sources et de les homogénéiser.

→ C'est un faux procès : les principes fondamentaux de la liberté d'expression et d'opinion, ainsi que notre attachement démocratique à la diversité de l'information, demeurent inchangés. Les différentes initiatives évoquées dans ce rapport visent à valoriser des contenus de qualité, non pas à censurer les contenus faux ou biaisés.

31. James Pamment *et al.*, *Countering Information Influence Activities*, *op. cit.* p. 9.

D. La polémique

La fausse équivalence : vous accusez RT et Sputnik de propagande. Or, Al-Jazeera, CNN, la BBC ou encore France 24 font exactement la même chose.

→ Nous ne parlons pas de propagande mais de manipulations de l'information. Al-Jazeera, CNN, la BBC ou France 24 contribuent certes à l'influence du Qatar, des États-Unis, du Royaume-Uni ou de la France, mais ces médias conservent leur indépendance éditoriale et respectent les standards journalistiques professionnels. En outre, ils ne recourent pas à des procédés fréquemment constatés chez RT et Sputnik tels que l'invention de faits et la falsification de documents, de traductions et d'interviews. Ce sont ces manipulations de l'information et elles seules que nous dénonçons, pas le fait de défendre un point de vue.

L'argument du bouc émissaire : vous accusez Moscou d'être à l'origine de tous les maux de l'Occident.

→ Ceux qui sont derrière les campagnes de désinformation, et qui sont souvent facilement identifiables, ne sont pas la cause des maux de nos sociétés, ils n'en sont que les amplificateurs. Il s'agit d'une stratégie délibérée d'identification des failles propres à chaque société (minorités religieuses, linguistiques, enjeux de mémoire, inégalités, séparatismes, tensions raciales…), puis de polarisation des opinions autour de ces enjeux.

→ La lutte contre les manipulations informationnelles doit en outre prendre en compte les autres acteurs, potentiels ou connus, susceptibles de se livrer à des campagnes de manipulation de l'information.

Cette initiative démontre que vous prenez vos citoyens pour des idiots que ne savent pas « penser correctement ».

→ Notre démarche ne comporte aucun jugement de valeur : nos citoyens sont entièrement libres de leurs choix et de leurs opinions, nous sommes une société ouverte et plurielle, c'est bien là notre force. Notre devoir est toutefois de protéger nos institutions démocratiques et les intérêts essentiels de la nation des manipulations informationnelles à visées hostiles, d'une part, et de favoriser le développement, par des acteurs de la société civile et des institutions publiques, de programmes permettant aux

citoyens, en particulier aux jeunes, d'exercer pleinement et entièrement leur esprit critique dans le domaine informationnel.

Vous n'êtes pas innocents : les nations occidentales, dont la France, n'ont pas hésité à recourir à la propagande d'État, notamment dans le contexte colonial.

→ Comme toutes les démocraties, la France est ouverte à toute discussion sur le passé sur la base de la rigueur scientifique. C'est là le domaine des historiens, qui étudient et continueront d'étudier tous les épisodes de notre histoire. Nous avons aujourd'hui affaire à un défi précis, spécifique, auquel nous devons faire face en tirant toutes les leçons du passé, mais aussi en nous tournant vers l'avenir.

BIBLIOGRAPHIE

Cette liste, non exhaustive, est donnée à titre indicatif.

Sources écrites

AALTOLA Mika, *Democracy's Eleventh Hour: Safeguarding Democratic Elections Against Cyber-Enabled Aurocratic Meddling*, FIIA Briefing Paper 226, novembre 2017.

ADEMSKY Dima, *Cross-Domain Coercion*, Institut français des relations internationales, novembre 2015.

AIELLO Luca Maria *et al.*, « People Are Strange When You're a Stranger: Impact and Influence of Bots on Social Networks », *Proceedings of the Sixth International AAAI Conference on Weblogs and Social Media* 697, 2012, p. 10-17.

ALAPHILIPPE Alexandre *et al.*, *Disinformation detection system: 2018 Italian elections. Case report,* EU Disinfo Lab, 1er juin 2018.

— *et al.*, *Rapport du Groupe d'experts belge sur les fausses informations et la désinformation*, juillet 2018.

ALBERT Jean-Marie, *La Désinformation* (t. 1 et 2), Triomphe, 2015.

ALLCOTT Hunt et GENTZKOW Matthew, « Social Media and Fake News in the 2016 Election », *Journal of Economic Perspectives*, 31:2, 2017, p. 211-236.

ALLEN T. S. et MOORE A. J., « Victory without casualties: Russia's information operations », *Parameters,* 48:1, printemps 2018.

ARO Jessikka, « The Cyberspace War: Propaganda and Trolling as Warfare Tools », *European View*, 10 mai 2016.

ASSOCIATION DES ANCIENS DE L'ÉCOLE DE GUERRE ÉCONOMIQUE, *Désinformation et révolution technologique*, 2006.

AUDINET Maxime, « Soft power russe : l'information au cœur », *in* MONTBRIAL Thierry de et DAVID Dominique (dir.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017.

BADOUARD Romain, *Le Désenchantement de l'internet. Désinformation, rumeur et propagande*, FYP éditions, 2017.

BAUMARD Philippe, *Le Vide stratégique,* CNRS éd., 2015.

— et col. BENVENUTI J. A., *Compétitivité et systèmes d'information,* InterÉditions, 1998.

BAZZELL Michael, *Open Source Intelligence Techniques: Resources for Searching and Analyzing Online Information,* CreateSpace Independent Publishing Platform, 2016.

BENASAYAG Miguel et AUBENAS Florence, *La Fabrication de l'information,* La Découverte, 2007.

BERNAYS Edward, *Propaganda,* ed. H. Liveright, 1928.

BERTOLIN Giorgio (dir.), *Digital Hydra: Security Implications of False Information Online,* NATO Strategic Communications Centre of Excellence, novembre 2017.

BLOCH Marc, « Réflexions d'un historien sur les fausses nouvelles de la guerre », *Revue de synthèse historique*, n° 33, 1921, p. 13-35.

BOGHARDT Thomas, « Operation Infektion: Soviet Bloc Intelligence and Its AIDS Disinformation Campaign », *Studies in Intelligence*, 53:4, 2009, p. 1-24.

BOYER, Bertrand, *Cybertactique : conduire la guerre numérique*, Nuvis, 2014.

—, « Les opérations sur l'environnement : la nouvelle guerre de l'information », *in* TAILLAT Stéphane, CATTARUZZA Amaël et DANET Didier (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018, p. 209-218.

BRADSHAW Samantha et HOWARD Philip N., *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*, Computational Propaganda Research Project, Working paper n° 2017.12, University of Oxford, juillet 2017.

BRATTBERG Erik et MAURER Tim, « Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks », *Carnegie Endowment for International Peace*, 23 mai 2018.

BRONNER Gérald, *La Démocratie des crédules*, PUF, 2013.

BULINGE Franck, *Maîtriser l'information stratégique : Méthodes et techniques d'analyse,* De Boeck, 2014.

CADIER David, « L'Europe centrale et la désinformation russe », *in* MONTBRIAL Thierry de et DAVID Dominique (dir.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017, p. 172-178.

— et LIGHT Margot (dir.), *Russia's Foreign Policy: Ideas, Domestic Politics and External Relations,* Palgrave Mcmillan, 2015.

CENTRE DE LA SÉCURITÉ DES TÉLÉCOMMUNICATIONS, *Cybermenaces contre le processus démocratique du Canada,* Gouvernement du Canada, 2017.

CENTRE FOR INTERNATIONAL RELATIONS, *Information Warfare in the Internet. Countering Pro-Kremlin Disinformation in the CEE Countries,* juin 2017.

CHEKINOV Sergei et BOGDANOV Sergei, « Asymmetrical Actions to Maintain Russia's Military Security », *Military Thought*, vol. 1, 2010.

CHOMSKY Noam et HERMAN Edward, *La Fabrication du consentement : de la propagande médiatique en démocratie* (1988), Agone, 2008.

CHOMSKY Noam et MCCHESNEY Robert W., *Propagande, médias et démocratie,* Écosociété, 2005.

CHOMSKY Noam et BARSAMIAN David, *De la propagande*, 10/18, 2003.

COLLECTIF, « L'Ère de la désinformation », *Courrier international*, Hors-série n° 63, octobre 2017.
CONNELL Mary Ellen et EVANS Ryan, « Russia's Ambiguous Warfare and Implications for the U.S. Marine Corps », *MCU Journal*, vol. 7, 2016.
CONSEIL NATIONAL DU NUMÉRIQUE, *Neutralité des plateformes. Réunir les conditions d'un environnement numérique ouvert et soutenable,* mai 2014.
COOK John et LEWANDOWSKY Stephan, *The Debunking Handbook*, University of Queensland, 2012.
CORDIER Anne*, Grandir connectés, les adolescents et la recherche d'information*, C&F éditions, 2015.
CORKER Bob *et al.*, *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, United States Senate, 10 janvier 2018.
CRAWFORD Krysten, « Stanford study examines fake news and the 2016 presidential election », *Stanford News*, 2017.
D'ALMEIDA Fabrice, *La Manipulation* (4e éd.), PUF, coll. « Que sais-je », 2017.
DAMARAD Volha et YELISEYEU Andrei, *Disinformation Resilience in Central and Eastern Europe*, Disinformation Resilience Index (DRI), 2018.
D'ANCONA Matthew, *Post-Truth: The New War on Truth and How to Fight Back,* Ebury Press, 2017.
DARCZEWSKA Jolanta, « The Devil is in the Details. Information Warfare in the light of Russia's Military Doctrine », *Point of View*, n° 50, OSW (Centre for Eastern Studies), mai 2015.
DARNTON Robert, « On retrouve tout au long de l'histoire l'équivalent de l'épidémie actuelle de "fake news" », *Le Monde*, 20 février 2017.
—, « The True History of Fake News », *The New York Review of Books*, 13 février 2017.
DEPREZ Fabrice, *« Fact-Checking » et « vérification », quel rôle et quels outils pour le veilleur ?,* Netsources, 2015.
DIEGUEZ Sebastian, *Total Bullshit ! Au cœur de la post-vérité*, PUF, 2018.
DOMENACH Jean-Marie, *La Propagande politique*, PUF, 1965.
DUPAQUIER Jean-François, *Politiques, militaires et mercenaires français au Rwanda, chronique d'une désinformation*, Khartala, 2014.
DURANDIN Guy, *L'Information, la désinformation et la réalité,* PUF, 1993.
ELKJER NISSEN Thomas, *Social Media's Role in « Hybrid Strategies »*, Riga NATO Strategic Communications Centre of Excellence, 2016.
ELLUL Jacques, *Propagandes*, Armand Colin, 1962.
EL-OIFI Mohammed, « Désinformation à l'israélienne », *Le Monde diplomatique*, 2005.
EUROPEAN COMMISSION, *A Multi-Dimensional Approach to Disinformation, Report of the Independent High Level Group on Fake News and Online Disinformation*, mars 2018.
EUROPEAN VALUES, *The Prague Manual. How to tailor national strategy using lessons learned from countering Kremlin's hostile subversive operations in Central and Eastern Europe,* Kremlin Watch Report, 30 avril 2018.
EUvsDISINFO, « The Strategy and Tactics of the Pro-Kremlin Disinformation Campaign », 27 juin 2018.
FARWELL James P., « Countering Russian Meddling in US Political Processes », *Parameters,* 48:1, printemps 2018.
FINNISH GOVERNMENT, *Security Strategy for Society. Government Resolution*, The Security Committee, 2 novembre 2017.

FRANKE Ulrik, *War by non-military means. Understanding Russian Information Warfare,* Swedish Defense Research Agency (FOI), mars 2015.
—, *Information Operations on the Internet: A Catalog of Modi Operandi*, FOI Totalförsvarets forskningsinstitut, mars 2013.
FRAU-MEIGS Divina, « *Fake news* : engager enfin un débat public confisqué… », *The Conversation,* 8 janvier 2018.
—, « Développer l'esprit critique contre les "infaux" », *Courrier de l'UNESCO,* juillet-septembre 2017.
FREEDOM HOUSE, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*, novembre 2017.
FRIED Daniel et POLYAKOVA Alina, *Democratic Defense Against Disinformation,* Atlantic Council, Eurasia Center, 2018.
GAGLIANO Giuseppe, *Désinformation, désobéissance civile et guerre cognitive*, VA Press, 2016.
GALEOTTI Mark, « An Unusual Friendship: Bikers and the Kremlin (Op-Ed) », *The Moscow Times*, 19 mai 2015.
—, « The Gerasimov Doctrine and Russian Non Linear War », *Blog in Moscow's Shadows*, juillet 2014.
GARRIGOU Alain, « Ce que nous apprennent les "fake news" », *Le Monde diplomatique*, février 2018.
GASTINEAU Pierre et VASSET Philippe, *Armes de déstabilisation massive. Enquête sur le business des fuites de données*, Fayard, 2017.
GÉRÉ François, *Dictionnaire de la désinformation*, Armand Colin, 2011.
GILES Keir, *Handbook of Russian Information Warfare*, Fellowship Monograph 9, NATO Defense College Research Division, novembre 2016.
—, *The Next Phase of Russian Information Warfare*, NATO Strategic Communications Centre of Excellence, 2016.
GU Lion, KROPOTOV Vladimir et YAROCHKIN Fyodor, *The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public*, A Trendlabs Research Paper, Trend Micro, 2017.
GUEHAM Farid, *Le Fact-Checking : une réponse à la crise de l'information et de la démocratie,* Fondapol, 2017.
HARBULOT Christian, *Les Fabricants d'intox, La guerre mondialisée des propagandes*, Lemieux, 2016.
—, *La France peut-elle vaincre Daech sur le terrain de la guerre de l'information ?* École de guerre économique, 2015.
— et LUCAS Didier, *La Guerre cognitive,* Lavauzelle, 2002.
HARREL Yannick, *La Cyberstratégie russe,* Phebe, 2013.
HARSIN Jayson, « Un guide critique des *Fake News* : de la comédie à la tragédie », *Pouvoirs*, n° 164, janvier 2018, p. 99-119.
HELLMAN Maria et WAGNSSON Charlotte, « How can European states respond to Russian information warfare? An analytical framework? », *European Security*, 26:2, 1er mars 2017, p. 153-170.
HELMUS Todd C. *et al.*, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, 2018.
HENIN Nicolas, *La France russe*, Fayard, 2016.
HENROTIN Joseph, *Techno-guérilla et guerre hybride : le pire des deux mondes*, Nuvis, 2014.

HOLIDAY Ryan, *Croyez-moi, je vous mens : Confessions d'un manipulateur des médias*, Globe, 2015.

HUYGHE François-Bernard, « Que changent les *fake news* ? », *La Revue internationale et stratégique*, n° 110, février 2018, p. 79-87.

—, *Fake news : la grande peur*, VA Press, 2018.

—, *DAECH : l'arme de la communication dévoilée*, VA Press, 2017.

—, *La Désinformation : les armes du faux*, Armand Colin, 2016.

—, « Désinformation : armes du faux, lutte et chaos dans la société de l'information », *Sécurité globale*, 2:6, 2016, p. 63-72.

—, KEMPF Olivier et MAZZUCHI Nicolas, *Gagner les cyberconflits : au-delà du technique*, Economica, 2015.

IRELAND (Government of), *First Report of the Interdepartmental Group on Security of Ireland's Electoral Process and Disinformation*, prepared by the Department of the Taoiseach, juin 2018.

ISSUE (Institute for Security Studies – European Union), *Strategic Communications. East and South,* Rapport n° 30, juillet 2016.

JACK Caroline, *Lexicon of Lies: Terms for Problematic Information*, Data & Society Research Institute, 2017.

JANDA Jakub, « Why the West is Failing to Counter Kremlin Disinformation Campaigns », *The Observer*, 30 décembre 2016.

JEANGÈNE VILMER Jean-Baptiste, « La lutte contre la désinformation russe : contrer la propagande sans faire de contre-propagande ? », *Revue Défense Nationale*, n° 801, juin 2017, p. 93-105.

—, *The Macron Leaks: A Post-Mortem Analysis*, CSIS Europe Program, Washington D.C., automne 2018.

—, *Successfully Countering Russian Electoral Interference: 15 Lessons Learned from the Macron Leaks*, CSIS Briefs, juin 2018.

JULIEN Claude (dir.), « L'art de la désinformation », *Le Monde diplomatique*, dossier de 13 articles, mai 1987.

KAJIMOTO Masato et STANLEY Samantha (dir.), *Information disorder in Asia – Overview of misinformation ecosystem in India, Indonesia, Japan, the Philippines, Singapore and South Korea,* Journalism & Media Studies Centre of the University of Hong Kong, 12 avril 2018.

KIRSCH Hervé (col.), « Guerre de l'information et opérations militaires », *Conflits*, n° 18, juillet-août-septembre 2018, p. 58-61.

KREKÓ Péter *et al.*, *The Weaponization of Culture: Kremlin's traditional agenda and the export of values to Central Europe,* Political Capital Institute, 4 août 2016.

KRÓL Aleksander, « Russian Information Warfare in the Baltic States – Resources and Aims », *The Warsaw Institute Review*, 3/2017.

KOYRÉ Alexandre, *Réflexions sur le mensonge*, Allia, 2004.

LANGE-IONATAMISVILI Elina (dir.), *Russia's Footprint in the Nordic-Baltic Information Environment,* NATO Strategic Communications Centre of Excellence, 2016-2017.

LAZER David *et al.*, *Combating Fake News: An Agenda for Research and Action*, Harvard University, 2017.

LE DRIAN Jean-Yves, ministre de l'Europe et des Affaires étrangères, *Discours de clôture de la conférence internationale « Sociétés civiles, médias et pouvoirs publics : les démocraties face aux manipulations de l'information »,* Paris, 4 avril 2018.

LENOIR Théophile, *Désinformation : la faute (seulement) aux réseaux sociaux ?,* Institut Montaigne, 2018.
LEWANDOWSKY Stephan, ECKER Ullrich K. H. et COOK John, « Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era », *Journal of Applied Research in Memory and Cognition*, 6:4, 2017, p. 353-369.
LEWANDOWSKY Stephan *et al.*, « Misinformation and Its Correction: Continued Influence and Successful Debiasing », *Psychological Science in the Public Interest,* 13:3, décembre 2012, p. 106-31.
LIMONIER Kevin, « Internet russe, l'exception qui vient de loin », *Le Monde diplomatique*, août 2017, p. 22-23.
—, « La Russie dans le cyberespace : représentations et enjeux », *Hérodote*, n° 152-153, 1er et 2e trimestres 2014, p. 140-160.
LIPPMAN Walter, *Public opinion*, Greenbook Publications, 1922.
LUCAS Edward et POMERANTSEV Peter, *Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe*, CEPA's Information Warfare Project/Legatum Institute, août 2016.
LUCAS Edward et NIMMO Ben, *Information Warfare: What Is It and How to Win It?*, CEPA Infowar Paper n° 1, novembre 2015.
LUTSEVYCH Orysia, *Agents of the Russian World: Proxy Groups in the Contested Neighbourhood,* Chatham House, avril 2016.
MACRON Emmanuel, président de la République, *Discours du président de la République Emmanuel Macron à l'occasion des vœux à la presse,* 3 janvier 2018.

MARANGÉ Céline, *Les Stratégies et les pratiques d'influence de la Russie,* Étude de l'IRSEM n° 49, mars 2017.
MARINI Lorenzo, « Fighting fake news: Caught between a rock and a hard place », *European Council on Foreign Relations*, mars 2018.
MATTIS James N. et HOFFMAN Frank, « Future Warfare: The Rise of Hybrid Wars », *Proceedings Magazine* (U.S. Naval Institute), 131:11, novembre 2005, p. 18-19.
MCGEEHAN Timothy P., « Countering Russian Disinformation », *Parameters,* 48:1, printemps 2018.
MCKELVEY Fenwick et DUBOIS Elizabeth, *Computational Propaganda in Canada: the Use of Political Bots,* Computational Propaganda Research Project, University of Oxford, Working Paper n° 2017.6, 2017.
MÉGRET Maurice, *La Guerre psychologique*, PUF, coll. « Que sais-je », 1963.
—, *L'Action psychologique,* Arthème Fayard, 1953.
MERCIER Arnaud (dir.), *Fake news et post-vérité : 20 textes pour comprendre la menace,* The Conversation France, 2018.
MILO Daniel et KLINGOVÁ Katarína, *Countering Information War Lessons Learned from NATO and Partner Countries: Recommendations and Conclusions*, Globsec, 2016.
MINISTÈRE DE L'ÉDUCATION NATIONALE, de l'Enseignement supérieur et de la Recherche, Direction du numérique pour l'éducation, *Infopollution : Hoax, rumeurs et désinformation*, vol. 1, 2016.
MOROZOV Evgeny, *Pour tout résoudre cliquez ici : l'aberration du solutionnisme technologique*, FYP, 2014.
—, « Les vrais responsables des fausses nouvelles », *Le Monde diplomatique,* 2017.
NATO STRATCOM COE & THE KING'S COLLEGE LONDON, *Fake News. A Roadmap,* février 2018.

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, *Internet Trolling as a tool of hybrid warfare: the case of Latvia. Results of the study*, 2016.

NGO INTERNEWS UKRAINE, *Words and Wars. Ukraine Facing Kremlin Propaganda,* 2017.

NIMMO Ben *et al.*, « Hashtag Campaign: #MacronLeaks. Alt-right attacks Macron in last ditch effort to sway French election, » *Atlantic Council's Digital Forensic Research Lab*, 6 mai 2017.

NOCETTI Julien, « Comment l'information recompose les relations internationales », *in* MONTBRIAL Thierry de et DAVID Dominique (dir.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017, p. 138-144.

—, « Internet renforce-t-il l'autoritarisme ? » *in* MONTBRIAL Thierry de et DAVID Dominique (dir.), *Ramses 2018. La guerre de l'information aura-t-elle lieu ?*, IFRI, Dunod, 2017, p. 162-166.

—, « Contest or Conquest: Russia and Global Internet Governance », *International Affairs,* 91:1, 15 janvier 2015, p. 111-130.

NYSSEN Françoise, ministre de la Culture, *Discours prononcé à l'occasion des Assises internationales du journalisme,* Tours, 15 mars 2018.

NYST Carly et MONACO Nick, *State-Sponsored Trolling: How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns*, Institute for the Future, 2018.

O'CARROLL Eoin, « How information overload helps spread fake news », *The Christian Science Monitor,* 27 juin 2017.

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (ODNI), *Assessing Russian Activities and Intentions in Recent US Elections*, Washington DC, janvier 2017.

OH Sarah et ADKINS Travis L., *Disinformation Toolkit*, InterAction, juin 2018.

O'NEIL Cathy, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy,* Crown, 2016.

PACEPA Ion Mihai (général), *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books, 2013.

PALMERTZ Björn, *Theoretical Foundations of Influence Operations: A Review of Relevant Psychological Research*, Center for Asymmetric Threat Studies (CATS), Swedish National Defence College, n.d.

PAMMENT James *et al.*, *Countering Information Influence Activities: The State of the Art,* Department of Strategic Communication, Lund University, research report, version 1.4, 1er juillet 2018.

PARISER Eli, *The Filter Bubble: What The Internet Is Hiding From You*, Penguin, 2011.

PASQUALE Frank, *The Black Box Society: The Secret Algorithms That Control Money and Information,* Harvard University Press, 2015.

PAUL Christopher et MATTHEWS Miriam, *The Russian « Firehose of Falsehood » Propaganda Model – Why It Might Work and Options to Counter It*, Expert insights on a timely policy issue, RAND Corporation, 2016.

PÉTINIAUD Louis et LIMONIER Kevin, « Cartographier le cyberespace : le cas des actions informationnelles russes en France », *Les Champs de Mars*, n° 30, vol. 2 (supplément), 2018, p. 317-326.

POLYAKOVA Alina et BOYER Spencer P., *The Future of Political Warfare: Russia, The West, and the Coming Age of Global Digital Competition,* Brookings, mars 2018.

POMERANTSEV Peter, *Nothing is True and Everything is Possible: The Surreal Heart of the New Russia*, PublicAffairs, novembre 2015.

POMERANTSEV Peter et WEISS Michael, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, The Interpreter, a project of the Institute of Modern Russia, 2014.

POPPER Karl, *La Société ouverte et ses ennemis*, t. 2, *Hegel et Marx*, Éd. du Seuil, 1979 [1962-1966].

QUESSARD Maud, *La Diplomatie publique américaine et la désinformation russe : un retour des guerres de l'information ?*, Note de recherche de l'IRSEM, n° 54, 30 avril 2018.

REPORTERS WITHOUT BORDERS, *Online Harassment of Journalists: Attack of the trolls*, 2018.

RILEY Michael, ETTER Lauren et PRADHAN Bibhudatta, *A Global Guide to State-Sponsored Trolling*, Bloomberg, 19 juillet 2018.

RIOCREUX Ingrid, *La Langue des médias : destruction du langage et fabrication du consentement*, L'Artilleur, 2016.

ROBINSON Linda *et al.*, *Modern Political Warfare. Current Practices and Possible Responses,* RAND Corporation, 2018.

ROSENFELD Louis, MORVILLE Peter et ARANGO Jorge, *Information Architecture*, O'Reilly, 2015.

SALAÜN Jean-Michel et HABERT Benoît, *Architecture de l'information : Méthodes, outils, enjeux,* De Boeck, 2015.

SANOVICH Sergey, *Computational Propaganda in Russia – The Origins of Digital Misinformation*, Working Paper, Computational Propaganda Research Project, Oxford Internet Institute, 2017.

SCHMITT Olivier, *Pourquoi Poutine est notre allié. Anatomie d'une passion française,* Hikari Éditions, 2017.

—, « "Je ne fais que poser des questions". La crise épistémologique, le doute systématique et leurs conséquences politiques », *Temps présents,* 15 juin 2018.

SCHOEN Fletcher et LAMB Christopher J., *Deception, Disinformation, and Strategic Communications: How One Interagency Group Made a Major Difference*, Center for Strategic Research, Institute for National Strategic Studies National Defense University, juin 2012.

SÉNÉCAT Adrien, « Le Décodex, un premier pas vers la vérification de masse de l'information », *Le Monde*, 2017.

SERMONDADAZ Sarah, « Google et Facebook déclarent la guerre aux fausses informations. Avec quels moyens ? », *Sciences et Avenir*, 2016.

SERRES Alexandre, *Dans le labyrinthe : évaluer l'information sur internet,* C&F Éditions, 2012.

SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ (SCRS), *Qui dit quoi ? Défis sécuritaires découlant de la désinformation aujourd'hui*, série « Regards sur le monde : avis d'experts », n° 2018-02-01, février 2018.

SMYRNAIOS Nikos, *Les GAFAM contre l'internet : une économie politique du numérique,* Institut national de l'audiovisuel, 2017.

STIEGLER Bernard *et al.*, *La toile que nous voulons*, FYP éditions, 2017.

SUNSTEIN Cass R. et VERMEULE Adrian, « Conspiracy Theories: Causes and Cures », *The Journal of Political Philosophy*, 17:2, 13 avril 2009, p. 202-227.

SUN TZU, *L'Art de la guerre*, Mille et Une Nuits, 1972.

SZWED Robert, *Framing of the Ukraine-Russia Conflict in Online and Social Media*, NATO Strategic Communications Centre of Excellence, mai 2016.

TATHAM Steve, *The Solution to Russian Propaganda Is Not EU or NATO Propaganda but Advanced Social Science to Understand and Mitigate Its Effects in Targeted Populations*, Policy paper, National Defence Academy of Latvia, Center for Security and Strategic Research, juillet 2015.

TENENBAUM Élie, *Le Piège de la guerre hybride*, Focus stratégique n° 63, IFRI, octobre 2015.

THE INTEGRITY INITIATIVE, *Framing Russian meddling in the Catalan question*, octobre 2017.

THE HAGUE CENTRE FOR STRATEGIC STUDIES, *Inside the Kremlin House of Mirrors. How Liberal Democracies can Counter Russian Disinformaion and Societal Interference,* 2017.

THE WARSAW INSTITUTE REVIEW, *Report: Disinformation in CEE,* n° 3, édition spéciale, 2017.

THOM Françoise, « La désinformation », *Commentaire*, n° 40, hiver 1987-88, p. 675-680.

TOUCAS Boris, « Exploring the Information-Laundering Machinery: The Russian Case », Commentary, CSIS, 31 août 2017.

—, *« L'Affaire russe » : la démocratie américaine ébranlée*, Notes de l'IFRI, Potomac Papers, n° 32, décembre 2017.

TUFEKCI Zeynep, « YouTube, the Great Radicalizer »*, The New York Times*, 10 mars 2018.

TWOREK Heidi, « Responsible Reporting in an Age of Irresponsible Information », Alliance for Securing Democracy (GMF) Brief 2018, n° 009, mars 2018.

UK HOUSE OF COMMONS (Digital, Culture, Media and Sport Committee), *Disinformation and "fake news": Interim Report, Fifth Report of Session 2017-19*, 29 juillet 2018.

US DEPARTMENT OF JUSTICE, *Report of the Attorney General's Cyber Digital Task Force*, juillet 2018.

VAISSIÉ Cécile, *Les Réseaux du Kremlin en France*, Les Petits Matins, 2016.

VANDERBIEST Nicolas, « Les institutions démocratiques : l'influence des réseaux sociaux durant une élection présidentielle », *in* TAILLAT Stéphane, CATTARUZZA Amaël et DANET Didier (dir.), *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018, p. 181-188.

VENTRE Daniel (dir.), *Cyberwar and Information Warfare,* Wiley, 2011.

VICHOVA Veronika et JANDA Jakub (dir.), *The Prague Manual: How to Tailor National Strategy Using Lessons Learned from Countering Kremlin's Hostile Subversive Operations in Central and Eastern Europe*, European Values, Kremlin Watch Report, 30 avril 2018.

VOLKOFF Vladimir, *Désinformation, flagrant délit*, Éd. du Rocher, 1999.

—, *Petite Histoire de la désinformation*, *Du cheval de Troie à Internet*, Éd. du Rocher, 1999.

—, *La Désinformation vue de l'Est*, Éd. du Rocher, 2007.

VOSOUGHI Soroush, ROY Deb et ARAI Sinan, « The spread of true and false news online », *Science*, 359:6380, 9 mars 2018, p. 1146-1151.

VOLKOFF Vladimir, POLIN Claude et MUCCHIELLI Roger, *La Désinformation : arme de guerre,* L'Âge d'homme, 1986.

WALTZMAN Rand, *The Weaponization of Information – The Need for Cognitive Security*, RAND Corporation, 2017.

WARDLE Claire et DERAKHSHAN Hossein, *Information disorder: Toward an interdisciplinary framework for research and policy making*, Conseil de l'Europe, 2017.

WATZLAWICK Paul, *La Réalité de la réalité. Confusion, désinformation, communication*, Éd. du Seuil, coll. « Points », 1978.

Sources audiovisuelles francophones

2016 dans les médias : post-vérité, « fake news » et crise du « fact checking », France Culture, 31 décembre 2016.
« Fact-checking » : fondement du journalisme ou miroir aux alouettes ? France Culture, 10 novembre 2012.
Fake news : jeux de mains, jeux de vilains, 28 minutes, Arte, 2017.
Fake news : le vrai du faux de Frédéric Lordon, France Culture, 19 janvier 2018.
Guerre de l'info : au cœur de la machine russe, Paul Moreira, Arte thema, 2018.
La Désinformation et les fabricants d'intox, 5e conférence Puissance 21, École de guerre économique, mars 2016.
Mensonge ou vérité, comment repérer les « fake news » ?, Xenius, Arte, 2017.
Moscou : l'info dans la tourmente, Alexandra Sollogoub*,* Arte, 2017.
Poutine contre les USA (1 et 2), Michael Kirk, Arte thema, 2017.
Runet, la bataille de l'Internet russe, Arte, web série de 10 épisodes, 2018.

PRÉSENTATION DES AUTEURS

Jean-Baptiste Jeangène Vilmer est directeur de l'Institut de recherche stratégique de l'École militaire (IRSEM) du ministère des Armées, après avoir été chargé de mission « Affaires transversales et sécurité » au Centre d'analyse, de prévision et de stratégie (CAPS) du ministère des Affaires étrangères (2013-2016). Formé dans trois disciplines – la philosophie (licence, master, Ph.D.), le droit (licence, LL.M., postdoctorat) et la science politique (doctorat) –, il a été en poste à la faculté de droit de McGill University (2011-2013), au département de War Studies du King's College London (2010-2011), au MacMillan Center for International and Area Studies de Yale University (2008-2009), à l'ambassade de France au Turkménistan (2007-2008) et à l'Université de Montréal (2005-2007). Auditeur de la 68e session nationale « Politique de défense » de l'IHEDN, membre du conseil scientifique du Collège de Défense de l'OTAN, enseignant à Sciences Po et à l'ENS Ulm, il est l'auteur d'une centaine d'articles et d'une vingtaine de livres, et le récipiendaire de plusieurs distinctions (prix maréchal Foch de l'Académie française 2013, Munich Young Leader 2018). Sur les manipulations de l'information, il est également l'auteur d'un rapport du CSIS (*The Macron Leaks: A Post-Mortem Analysis*, automne 2018).

Contact : jbjv.com / jean-baptiste.jeangene-vilmer@irsem.fr / Twitter @jeangene_vilmer

Alexandre Escorcia, diplomate, est directeur adjoint du Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères. Précédemment conseiller du ministre des Affaires étrangères et du développement international Jean-Marc Ayrault (2016-2017), il a également été premier secrétaire à l'ambassade de France en Allemagne (2013-2016) et diplomate d'échange au ministère allemand des affaires étrangères (2012-2013). Affecté comme conseiller diplomatique du premier commandant suprême allié transformation de l'OTAN de nationalité française à Norfolk aux États-Unis (2009-2012), il avait auparavant été rédacteur à la direction des affaires stratégiques, de sécurité et du désarmement et à la direction politique (service de la politique étrangère et de sécurité commune) du Quai d'Orsay (2005-2009). Ancien élève de l'École normale supérieure, diplômé de l'Institut d'études politiques de Paris, il est l'auteur de publications sur les questions de politique étrangère et de défense européenne et sur l'OTAN.

Marine Guillaume est chargée de mission « Enjeux numériques et cybersécurité » au Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères et maître de conférences en science politique à l'École Polytechnique. Docteure en science politique de Columbia University et de Sciences Po, elle a précédemment été Lecturer à la School of International Public Affairs (SIPA) de Columbia University, et ATER à l'IEP de Paris. Elle a également été Associate Consultant chez Bain & Company (2015-2016).

Janaina Herrera, diplomate, était jusqu'à récemment chargée de mission « Affaires multilatérales, Amérique latine, droits de l'homme » au Centre d'analyse, de prévision et de stratégie (CAPS) du ministère de l'Europe et des Affaires étrangères (2015-2018). Elle est désormais consule générale de France à Alexandrie. Diplômée de Sciences Po et ancienne élève de l'ENA, elle a fondé à Beyrouth un think tank indépendant dédié aux printemps arabes (2011-2015), après avoir été première secrétaire à l'ambassade de France au Liban, en charge des questions régionales et multilatérales (2007-2010), et rédactrice au Service de la politique étrangère et de sécurité commune (PESC) et à la Direction des Nations unies sur les dossiers environnementaux.

Remerciements

Nous remercions chaleureusement l'ensemble de nos interlocuteurs, en France et à l'étranger, ainsi que les collègues qui ont bien voulu nous assister dans la préparation de ce rapport, par des contributions ciblées ou une relecture attentive (Jean-Pierre Bat, Emmanuel Bloch, Lucie Delzant, Emmanuel Dreyfus, Jean Dubosc, Émilien Legendre, Kevin Limonier, Benjamin Pajot, Maud Quessard, Marie Robin, Boris Toucas), ainsi que Élodie Ternaux pour la couverture, Chantal Dukers pour la maquette intérieure, et Mickaela Churchill, Aziliz Gouez et Diana Reisman pour la traduction en anglais.

Les manipulations de l'information ne sont pas nouvelles mais leur actualité récente est liée à la combinaison de deux facteurs : les capacités inédites de diffusion et de viralité offertes par internet et les réseaux sociaux, et la crise de confiance que vivent nos démocraties et qui dévalue la parole publique allant jusqu'à relativiser la notion même de vérité. Ce phénomène qui s'est illustré par plusieurs ingérences électorales ces dernières années menace la sécurité nationale. Le CAPS et l'IRSEM ont donc uni leurs forces pour l'étudier.

Ce rapport est le fruit d'une enquête de terrain (une centaine d'entretiens menés dans une vingtaine de pays) pour mieux saisir la nature du problème et identifier les bonnes pratiques mises en œuvre par les États et les sociétés civiles. Il s'appuie également sur l'abondante littérature scientifique disponible.

Écartant la notion vague et polémique de *fake news*, et d'autres (propagande, influence, désinformation, etc.) souvent trop étroites ou trop larges pour s'appliquer précisément au problème, il parle de « manipulations de l'information » pour désigner la diffusion intentionnelle et massive de nouvelles fausses ou biaisées à des fins politiques hostiles.

Il analyse d'abord les causes, qui sont à la fois individuelles, relevant de la psychologie et de l'épistémologie (des failles cognitives et une crise de la connaissance), et collectives, liées à la vie en société (une crise de confiance dans les institutions, une crise de la presse et une désillusion à l'égard du numérique), avant de voir qui en profite, c'est-à-dire qui sont les acteurs de ces manipulations – en se focalisant sur celles qui sont d'origine étatique et qui visent les populations d'autres États, constituant donc des ingérences.

Ce rapport examine ensuite les conséquences, en tâchant de dégager quelques caractéristiques communes des plus récentes campagnes, en termes de facteurs de vulnérabilités et de moyens mis en œuvre. Il explore également d'autres terrains – autres par rapport à l'espace post-soviétique, l'Europe et l'Amérique du Nord qui sont les plus connus – et notamment le Moyen-Orient, l'Afrique et l'Amérique latine.

Dans une troisième partie consacrée aux réponses, il fait la synthèse des contre-mesures adoptées par les différents acteurs – États, organisations internationales, société civile et acteurs privés –, en commençant par tirer les leçons de la tentative d'ingérence dans la dernière élection présidentielle française (« Macron Leaks »).

Pour finir, ce rapport tente d'anticiper les défis futurs – défis technologiques, tendances de la « guerre de l'information » russe, scénarios possibles – et formule 50 recommandations concrètes partant du principe que les manipulations de l'information constituent un défi de longue haleine pour nos démocraties, auquel elles devront apporter une réponse participative, libérale et respectueuse des droits fondamentaux.

Auteurs : Jean-Baptiste Jeangène Vilmer, chercheur, directeur de l'IRSEM ; Alexandre Escorcia, diplomate, directeur adjoint du CAPS ; Marine Guillaume, chercheuse, chargée de mission au CAPS et Janaina Herrera, diplomate, ancienne chargée de mission au CAPS.

Le CAPS est le Centre d'analyse, de prévision et de stratégie du ministère de l'Europe et des Affaires étrangères. L'IRSEM est l'Institut de recherche stratégique de l'École militaire du ministère des Armées.

Août 2018

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'EUROPE ET DES AFFAIRES ÉTRANGÈRES
MINISTÈRE DES ARMÉES