Institut français des relations internationales

ifri

ramses 2018

Rapport annuel mondial sur le système économique et les stratégies

Sous la direction de Thierry de Montbrial et Dominique David

Avec 8 vidéos

DUNOD

Publié par Dunod pour l'Institut français des relations internationales

Comment l'information recompose les relations internationales

La faute à Internet ?

Internet renforce les incertitudes du monde contemporain. La surveillance défensive et offensive des communications privées, les attaques contre des entreprises et infrastructures, l'intoxication des fake news, et les soupçons de manipulation électorale, contribuent à défaire le vieux consensus sur le réel et la vérité.

Sous le grand ébranlement des démocraties qui a dominé l'année 2016 avec le Brexit et l'élection de Donald Trump aux États-Unis, pointe la révolution numérique, qui a changé de nature. Au départ principalement économique, bouleversant les chaînes de valeur et la hiérarchie des entreprises, la *disruption* est devenue politique et stratégique, avec la vague des populismes portée par la déstabilisation des classes moyennes et les réseaux sociaux. Il en est allé de même avec le retournement de la doctrine du *regime change* contre les démocraties, et avec l'interférence supposée de la Russie dans la campagne présidentielle américaine en faveur de Donald Trump.

Parallèlement à des transformations décisives (reconfiguration de la vie économique et sociale autour des objets connectés, avancées accomplies par l'intelligence artificielle), la révolution numérique charrie une face sombre, aux mutations tout aussi rapides. La cybercriminalité progresse fortement, avec un chiffre d'affaires estimé à 445 milliards de dollars par an[1]. La cyberguerre, expérimentée contre l'Estonie, la Géorgie et l'Ukraine, se révèle être une arme asymétrique redoutablement efficace entre les mains des régimes chinois et russe – qui l'utilisent pour compenser, sinon annuler, l'avantage technologique des armées occidentales –, ainsi que des puissances contestant l'ordre international (Iran ou Corée du Nord). Par ailleurs, le recours intensif des partis populistes aux réseaux sociaux contribue à déstabiliser les démocraties. Le piratage du site du Parti démocrate, orchestré par des hackers, aurait ainsi, *via* l'instrumentalisation de WikiLeaks, pesé sur le dénouement de l'élection présidentielle américaine.

Faute d'institutions et de règles, le cyberespace bascule du mythe libertaire de son autorégulation, de sa neutralité et de sa logique de partage altruiste, vers la balkanisation et le rapport de force. Le réseau se reconfigure autour de systèmes régionaux ou étatiques qui se superposent, mettant en péril l'infrastructure globale et les serveurs qui en assurent le fonctionnement. Des blocs de

1. Selon les données du spécialiste de la sécurité informatique McAfee.

régulation hétérogènes se juxtaposent, les États-Unis défendant l'oligopole GAFAM (Google, Apple, Facebook, Amazon, Microsoft), la Chine et la Russie le contrôle de l'État, tandis que l'Union européenne (UE) tente de préserver la liberté de ses citoyens à travers le *Privacy Shield* adopté en juillet 2016.

▸▸ Le monde de la post-vérité ?

▸ *La grande bascule : des faits aux données*

Omniprésente, la « post-vérité » s'est imposée comme l'une des clés de lecture principales pour expliquer deux des événements majeurs de l'année 2016 : le Brexit et l'élection de Donald Trump. Élu mot de l'année 2016 par l'*Oxford English Dictionary*, cette expression désigne « des circonstances dans lesquelles les faits objectifs ont moins d'influence pour modeler l'opinion publique que les appels à l'émotion et aux opinions personnelles ». L'essor fulgurant de la notion suscite plusieurs interrogations.

Premièrement, la post-vérité risque bien de représenter prochainement l'horizon indépassable de la vie publique. Un discours raisonnable n'a guère de puissance pour la mobilisation : pour faire vivre la démocratie, il faut mobiliser les passions, selon le linguiste Raffaele Simone. Le rêve nous installe dans la fiction, mais les citoyens des démocraties ont besoin de tenir pour vraies certaines fictions s'inscrivant dans une mythologie, laquelle constitue l'un des piliers fondamentaux de la démocratie.

Deuxièmement, la capacité de survie de la vérité dans la démocratie est un problème que découvrent depuis peu les journalistes. Les discours des populistes donnent de plus en plus de difficultés aux *fact checkers* qui vérifient la parole des hommes politiques. Ainsi le *Washington Post* a-t-il calculé que 70 % des déclarations de Donald Trump pendant sa campagne déformaient la réalité ou étaient fondées sur du pur mensonge.

Troisièmement, le numérique a sans doute contribué à diffuser la démagogie – sans que celle-ci soit pour autant nouvelle. Dès l'Antiquité, Cléon d'Athènes était conspué par Aristote pour avoir été « le premier à crier à la tribune, à y employer des injures, et à parler débraillé, alors que les autres orateurs gardaient une attitude correcte ». La nouveauté n'est pas que la vérité soit falsifiée ou contestée, mais qu'elle soit devenue secondaire. Avec les réseaux sociaux, le relativisme et l'horizontalité des sources remplacent le monopole journalistique de l'information. La fragmentation des nouvelles sources d'information a créé un monde atomisé où le mensonge, la rumeur et les ragots se répandent quasi instantanément. Au XXIe siècle, le problème est la surabondance des informations – trop de sources, aux méthodes de crédibilité variables –, qui dessine un espace opaque, transitionnel, entre une « société des faits » et une « société des données ». À cela s'ajoute le danger que la prolifération de fausses informations décrédibilise le concept même d'information…

Chasser les fake news

La vaste prise de conscience concernant les fausses informations doit cependant se garder de toute simplification. La mesure du phénomène est ardue, la corrélation avec l'issue de la présidentielle américaine ne peut être établie, et le concept même de fausse information recoupe d'autres réalités, comme l'intoxication à visée politique, le canular, la « réinformation », etc.

Reste toutefois un constat général : celui d'une expansion du phénomène, portée par l'industrialisation de la fabrication de *fake news*, la fragilisation de l'espace public par les communications mensongères, le complotisme et les tenants de la post-vérité, enfin l'essor spectaculaire des moteurs de recherche, et désormais des réseaux sociaux, comme *moyens* d'information. Les *fake news* se diffusent désormais beaucoup plus vite et efficacement qu'auparavant – la faute, en partie, aux plateformes qui privilégient l'« engagement » de leurs utilisateurs, c'est-à-dire le fait qu'ils partagent, commentent, « aiment » des contenus, donnant une prime aux publications qui émeuvent, choquent ou font réagir. C'est ce parti pris qui est aujourd'hui mis en cause, après que de fausses informations, telle celle du soutien du pape François à Donald Trump, ont été plus largement lues et partagées que leurs contrepoints véridiques.

La responsabilité des plateformes

Les géants du Web sont désormais incités à agir pour maîtriser les comportements de leurs utilisateurs. La Grande-Bretagne a ouvert une enquête parlementaire sur le sujet début 2017. La France souhaite ouvrir des discussions avec Facebook et Google, tandis qu'en Allemagne les réseaux sociaux sont menacés d'une loi sanctionnant la diffusion de fausses informations. La Commission européenne réclame, elle aussi, une action plus déterminée des grandes plateformes. Les pressions commencent également à venir de l'intérieur. Au sein de Twitter, de Facebook ou de Google, des voix s'élèvent pour leur demander de faire plus, et mieux, contre les internautes qui abusent de leur outil pour répandre des mensonges, de la propagande ou des idéologies haineuses. Ces demandes vont néanmoins à l'encontre de la posture de plateformes qui se considèrent, par essence, neutres. Les États voudraient que Facebook ou Google agissent comme des régulateurs, trouvent les moyens de filtrer les contenus. Ces derniers considèrent que leur rôle est, au mieux, de fournir à des tiers des outils de régulation – ainsi que Facebook le fait, depuis plusieurs années, sur des sujets comme la prévention du suicide. Sous la pression de l'opinion, ces entreprises ont toutefois engagé des actions, en partie pour des raisons d'image : label *fact check* sur Google News aux États-Unis, projet de vérification collective *First Draft* de Google en partenariat avec plusieurs médias, système d'alerte aux fausses informations en test chez Facebook…

La recette de l'autorégulation pour éviter la régulation est connue – mais pour quelle efficacité ? L'impression que laissent ces initiatives est plutôt celle de plateformes souhaitant montrer qu'elles ne restent pas inactives, mais hésitant à s'emparer du problème. Pour des raisons économiques d'abord : embaucher ou financer une armée de modérateurs et de *fact checkers* compromettrait leur modèle, comme de réduire le volume de contenus en circulation ou de brider les utilisateurs. En juin, pour refuser un rapport sur les fausses informations, les actionnaires de Facebook et de Google ont certainement été mus par cette

préoccupation. Pour des raisons culturelles ensuite : fondés sur une idéologie libertaire, les géants du numérique considèrent que tout ce qui limite la liberté d'expression – dans son acception américaine – est dangereux.

S'ils doivent assumer une plus grande part de responsabilité, les réseaux sociaux et grands opérateurs du Web font aussi figure de commodes boucs émissaires. Le succès viral d'informations outrageusement fausses ne s'appuie pas seulement sur la puissance des plateformes de Facebook ou Google, mais aussi sur l'envie d'y croire. Durant la campagne présidentielle américaine, des millions d'électeurs ont partagé ces messages parce qu'ils n'accordaient aucune confiance aux médias toujours suspects de parti pris, ni aux candidats considérés comme corrompus (*crooked*). La propagande et la désinformation se nourrissent donc d'abord et surtout de cette crise de confiance.

▸▸ Mythes et réalités de la cyberguerre

La guerre de l'information qui se fait jour est de plus en plus mêlée à la cyberguerre, à laquelle se livrent pêle-mêle grandes puissances, pays en marge de l'ordre international, acteurs privés, et individus seuls ou coalisés. Si les menaces cyber et informationnelles sont souvent analysées séparément, le contexte international a évolué et suggère d'adopter une approche plus intégrale, ne serait-ce que pour appréhender plus finement les stratégies d'États comme la Chine, et surtout la Russie, pour qui les cyberopérations sont subordonnées aux opérations informationnelles (propagande, désinformation, subversion, etc.).

▸ *L'information, nerf de la guerre*

Une cyberattaque émanant d'un État, au-delà du résultat destructeur, a pour objectif principal de produire de l'incertitude politique. La Conférence sur la sécurité de Munich, en février 2017, a précisément abordé ce point, postulant que la cyberconflictualité ne visait plus seulement les infrastructures dites critiques (opérateurs énergétiques, de télécommunications et de défense), mais aussi notre système politique et les valeurs sur lequel ce système est fondé. N'a-t-on pas entendu certains responsables politiques occidentaux suggérer que la démocratie et ses attributs devaient désormais être traités comme une infrastructure critique face aux attaques informatiques et aux manipulations d'internet ?

Dans une vie politique internationale qui voit depuis quelques années un certain retour de la géopolitique, la rivalité pour le récit, pour les idées, pèse fortement dans la balance stratégique. Post-vérité aidant, sommes-nous entrés dans un monde en voie accélérée de désoccidentalisation, dans lequel la prééminence de l'Occident s'effriterait, exponentiellement remise en question par le biais des outils numériques ? Il est aujourd'hui en effet très facile, et peu coûteux, de diffuser un discours et de discréditer le narratif adverse en recourant au numérique.

Aux *fake news* déjà mentionnées, aux fameux *trolls* s'attaquant aux débats en ligne, s'ajoutent dorénavant les *mèmes* – ces phénomènes repris en masse sur internet : hyperlien, image, *hashtag*, phrase, personnage récurrent… telle la mascotte de l'ultra-droite américaine, Pepe the Frog. Outils éminemment asymétriques, parfois comparés aux engins explosifs improvisés, les *mèmes*, par leur nature intrinsèque, affaiblissent les monopoles en matière de récits et défient les

autorités politiques centralisées[2]. Le sujet fait l'objet de réflexions stratégiques et doctrinales très sérieuses, en particulier dans les états-majors américains et de l'OTAN : on s'y intéresse de près tant pour contrer la propagande djihadiste que pour réagir aux campagnes informationnelles de la Russie.

La responsabilité des États dans la course aux cyberarmes

La multiplication d'attaques informatiques de plus en plus sophistiquées et désormais à portée globale ne peut être totalement dissociée du versant informationnel et requiert l'élaboration de nouvelles régulations. La question du contrôle des cyberarmes d'État est également posée avec acuité depuis la révélation du fait que le virus informatique *WannaCry*, qui a frappé plus de 250 000 ordinateurs en un week-end en mai 2017, a été subtilisé par des cybercriminels à la National Security Agency (NSA). Dans le monde entier, des hackers s'affairent pour débusquer des failles de sécurité logicielle (*zero day*) pour le compte d'agences de renseignement. Ces arsenaux servent à pénétrer dans les systèmes informatiques de leurs adversaires, qu'il s'agisse de gouvernements ou d'organisations terroristes.

En mars, WikiLeaks avait révélé que la CIA disposait de dizaines de failles pour pirater des iPhone et des smartphones Android, des ordinateurs équipés de Windows, et même des téléviseurs Samsung. Cette course à l'armement, préoccupante, n'est aujourd'hui l'objet que d'un contrôle minimal. Les Nations unies réfléchissent à des moyens supplémentaires de limiter la prolifération des cyberarmes, comme elles le font pour les armes classiques – mais le droit international du cyberespace en reste à un stade embryonnaire. En février, le président de Microsoft a appelé à la signature d'une « convention de Genève du numérique », avec l'introduction de normes qui obligeraient les États à révéler aux éditeurs les failles de sécurité en leur possession. Un nouveau cadre mondial devrait aussi permettre de définir la manière dont un État, ou ses entreprises, a le droit de riposter à une cyberattaque.

Pour qu'il soit efficace, cet indispensable contrôle des cyberarmes supposerait, en parallèle, que ne soient pas systématiquement recherchés les moyens d'affaiblir la sécurité des logiciels à des fins de surveillance. Après les attentats qui ont frappé la France, certains responsables politiques avaient appelé à la création de « portes dérobées » (*backdoors*) dans les applications de messagerie, afin d'espionner les conversations des terroristes. En 2016, Apple s'était publiquement opposé au FBI, en refusant de casser le chiffrement de l'iPhone du tueur de San Bernardino. Cette affaire avait confirmé la centralité de l'enjeu du chiffrement, sur lequel se cristallise la tension entre intérêt supérieur des États et exigences des opinions en matière de respect de la confidentialité des échanges.

2. J. Siegel, « Is America Prepared for Meme Warfare? », Vice.com, 31 janvier 2017.

▸▸ Qui remportera la bataille de l'information ?

Dans l'ensemble de ces luttes informationnelles, verra-t-on l'un ou l'autre acteur (États démocratiques, régimes autoritaires, plateformes du Net) prendre le dessus ? La puissance inédite des géants du Web ne peut qu'interpeller. Ceux-ci prennent désormais position sur des sujets politiques plus larges, portés par certains PDG médiatiques comme Mark Zuckerberg. Le patron de Facebook se montre de plus en plus politisé, au point d'être suspect d'ambitions politiques nationales. Dans un discours remarqué à Harvard en mai 2017, le jeune milliardaire soulignait l'importance de la lutte contre le réchauffement climatique et prônait un revenu universel et une couverture de la santé étendue.

Voici beau temps que la Silicon Valley impose une vision du monde, son fantasme d'un univers connecté et ouvert. Mais jusqu'ici, les GAFAM s'en tenaient à un discours du ressort de l'utopie, dans laquelle les technologies devaient occuper une place déterminante, sans pour autant adopter de positions fermes et tranchées – quitte à s'arranger avec les pratiques de censure des régimes autoritaires.

Aujourd'hui, leurs propos deviennent plus concrets et concernent des sujets d'actualité majeurs (éducation, emploi, etc.) dans lesquels la technologie n'a pas de rôle direct à jouer. Ce positionnement permet à ces « États-plateformes » de se façonner une image d'organisations quasi philanthropiques aux prises de position progressistes, d'affirmer leur puissance, et de faire oublier que leur pouvoir repose sur l'exploitation des données personnelles des trois milliards d'internautes dans le monde[3]. Avec ses liquidités, Apple pourrait distribuer près de 35 dollars à chaque habitant de la planète…

Depuis l'époque des utopies, les règles du jeu ont changé : ces multinationales ont aujourd'hui la possibilité d'agir financièrement et politiquement, tant elles pèsent lourd, économiquement, médiatiquement, mais aussi sur les esprits. En frôlant les deux milliards d'utilisateurs actifs, Facebook réunit près d'un humain sur trois ; cet humain en faisant l'une de ses principales sources d'information sur le monde.

J. N.

POUR EN SAVOIR PLUS

T. Berners-Lee, « Trois défis pour le Web », Fondation World Wide Web, 12 mars 2017.

R. Darnton, « The True History of Fake News », *The New York Review of Books*, 13 février 2017.

R. Simone, *Si la démocratie fait faillite*, Paris, Gallimard, 2016.

« Post-Truth, Post-West, Post-Order? », *Munich Security Report*, 2017.

Voir également la carte « Le numérique comme facteur de puissance », p. 311.

3. « The World's Most Valuable Resource Is No Longer Oil, but Data », *The Economist*, 6 mai 2017.