La démocratie française menacée :

Les actuelles cyberattaques russes en provenance du groupe spécialisé de la Direction générale (ex- GRU) de Moscou visant des citoyens français passifs

Depuis deux ans, quelques officiers francophones (choisis par les 175 personnes chargées de lancer des attaques dans le cyberespace), pour le moment une infime fraction des 12 000 agents de l'ex-GRU (Главное разведывательное управление Генерального штаба Вооружённых Сил Российской Федерации), agence recréée sous son nouveau nom en 1992 et commandée de janvier 2016 (après la mort par crise cardiaque d'Igor Sergoun) jusqu'à son décès d'un cancer le 22 novembre 2018 par le général Igor Korobov, lancent des campagnes d'essai en direction de la France en liaison avec les informations recueillies par l'antenne française de *Russia Today*.



Igor Korobov qui a créé le service de déstabilisation en direction de la France.

Avant les élections françaises de 2019 et 2020, il convient d'établir, avec l'ide des grouypes The Insider et Bellingcat pour les biographies des agents, les noms et adresses de chacun de ces personnels, à Moscou et dans sa banlieue, puisque leur lieu de travail est d'ores et déjà connu. Le vice-amiral Igor Kostioukov va sans doute succéder à Igor Korobov dans les jours à venir. Les agents du FSB sont également actifs, mais ils n'ont pas monté d'opération contre la France.



La « Tour » de Khimki à Moscou d'où sont lancées les cyberattaques contre les États étrangers (adresse : Moscou, chaussée Khoroshevskoe, 76).

L'accord avec le service étranger chargé d'analyser le contenu de ces messages (avec de nombreux indices, présents surtout dans les images, montrant qu'ils proviennent de Russie doit être mis en avant afin d'analyser provisoirement par l'outil Palantir l'origine et la diffusion de ces messages pour neutraliser les personnes relais en France même ou situées hors de France.
Ces informations seront données aux gouvernements alliés afin de les prémunir contre des attaques d'un type nouveau provenant de l'embryon d'une nouvelle armée s'ajoutant à l'armée de l'air créée en 1934. En effet, des cyberattaques russes ont visé récemment le siège de l'Organisation pour l'interdiction des armes chimiques [OIAC], à La Haye [Pays-Bas] ainsi que l'Agence mondiale antidopage [AMA], le Parti démocrate américain, les réseaux du Bundestag, la chaîne de télévision TV5 ou encore le ministère danois de la Défense.



Les agents russes impliqués dans l'opération des Pays-Bas.

Facebook a déjoué une campagne de propagande en français

Des comptes Facebook et Instagram, fermés le 4 novembre, postaient des messages liés à la politique et à la société françaises. Un rapport donne les détails de leur activité.

Par Martin Untersinger Publié le 28 novembre 2018 à 06h00 - Mis à jour le 29 novembre 2018 à 10h34



Saisie d'écran d'un des comptes ayant diffusé des messages problématiques en français sur Facebook et Instagram. DFR Lab / LE MONDE

Nous sommes au soir du 4 novembre. Chez Facebook, on se prépare à la soirée électorale des élections américaines de mi-mandat, qui doit se tenir dans moins de deux jours. Après le fiasco du scrutin présidentiel de 2016, où la Russie a pu mener, sans rencontrer de résistance, une opération de propagande sur le réseau social, ce dernier n'a pas le droit à l'erreur.

Des pages qui ne sont pas ce qu'elles prétendent être et pilotées de manière coordonnée

Arrive alors un message émanant de la police fédérale américaine (FBI). Celle-ci a repéré plusieurs comptes qu'elle juge suspects. Facebook les inspecte et confirme ces suspicions : il s'agit bien d'un réseau de pages et de comptes engagés dans ce que le réseau social appelle une *« activité inauthentique et coordonnée »*.

Pages fantômes

Autrement dit des pages qui ne sont pas ce qu'elles prétendent être (en mentant notamment sur leur identité) et pilotées de manière coordonnée, par exemple, par un seul administrateur, alors qu'elles semblent toutes différentes et séparées. Facebook fait la chasse à ce type de comportement, qui correspond aux méthodes d'ingérence par une puissance étrangère utilisées pendant la campagne électorale américaine de 2016.

Le réseau social décide donc, ce 4 novembre, de supprimer cette série de comptes Facebook et Instagram. Le lendemain, l'entreprise publie un premier communiqué, laconique. Un empressement justifié, selon elle, par l'imminence des élections de mi-mandat et la similarité de cette campagne de propagande avec d'autres.

Les experts du réseau social passent ensuite les pages et les comptes supprimés au peigne fin. Huit jours plus tard, le 13 novembre, ils publient un deuxième communiqué, évoquant quelques détails de l'opération ainsi déjouée.

Un élément passe alors relativement inaperçu dans le cadre des élections américaines de mi-mandat : parmi les quelques dizaines de pages et de comptes supprimés, certains sont en français. C'est pourtant la première fois que Facebook révèle avoir supprimé des pages fantômes francophones diffusant de la propagande.

Que postaient ces comptes ?

En parallèle, le réseau social a fourni la liste des comptes Facebook et Instagram supprimés à une équipe d'experts, le DFR Lab, financé par le think tank américainAtlantic Council, avec qui la société de Mark Zuckerberg a noué un partenariat pour analyser les opérations de propagande. Celui-ci a publié, mercredi 28 novembre, un rapport à ce sujet écrit par les analystes Ben Nimmo et Camille François, dont *Le Monde* a obtenu copie.

Le texte donne des informations plus précises sur l'étendue et l'activité des comptes ayant diffusé des messages problématiques en français sur Facebook et Instagram. Les deux auteurs du rapport du DFR Lab précisent toutefois d'emblée qu'ils n'ont pu récupérer qu'un *« aperçu »* de l'opération. Les comptes ayant été immédiatement supprimés par Facebook, les chercheurs se sont contentés d'analyser des « traces » gardées automatiquement en mémoire sur divers sites et sur des moteurs de recherche. Un travail « d'archéologue », forcément partiel.

« Aucun autre homme ou femme politique français n'a été autant mentionné dans les publications qu'Emmanuel Macron », selon les chercheurs

Au total, six pages Facebook et une dizaine de comptes Instagram postaient des messages ou des images en français. Tous formaient un seul et unique réseau, piloté par un ou plusieurs individus. Ils brassaient des thèmes variés, mais beaucoup abordaient, à intervalles réguliers, des questions sociales ou politiques. Trois se faisaient passer pour des femmes noires ; un autre postait des contenus liés aux femmes et à la mode musulmanes ; un compte était consacré au football ; d'autres prétendaient être un trotskiste, un militant nationaliste ou un citoyen engagé dans l'écologie. Les deux comptes Facebook semblaient, selon les éléments recueillis par le DFR Lab, aborder essentiellement des problématiques féministes.

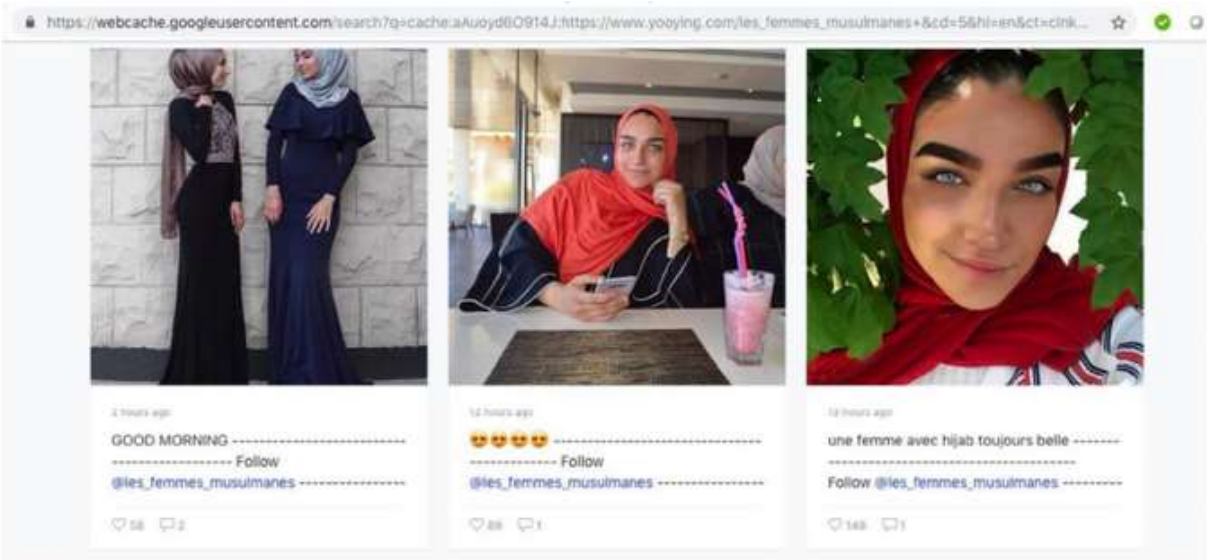
« Aucun autre homme ou femme politique français n'a été autant mentionné dans les publications qu'Emmanuel Macron », expliquent les deux chercheurs, qui ont pu retrouver des publications hostiles au président français sur cinq des onze comptes Instagram analysés.

On y retrouve des mots-clés critiques (#macrondegage) et beaucoup de mèmes, ces images virales et souvent humoristiques, sur lesquels on peut lire, par exemple : *« Si en France on marche la tête haute… c'est parce qu'avec*

Macron nous sommes dans la merde jusqu'au cou » ; *« Je préfère les migrants aux Français »* sur fond d'une photo d'Emmanuel Macron ; *« Les deux hantises des banquiers ? L'argent qui dort… et le peuple qui se réveille ! »* apposé sur le visage du président français. Même les comptes les moins « politiques » (@femme_combattante ou celui se disant écologiste) évoquaient, de temps à autre, Emmanuel Macron.

Le but : construire une audience auprès de catégories bien spécifiques de la population

Outre la politique, de nombreux comptes ont partagé des images et des textes plus neutres, voire positifs, très vraisemblablement pour construire leur audience auprès de catégories bien spécifiques de la population, expliquent les chercheurs, à la manière de l'Internet Research Agency (IRA), l'officine russe responsable des campagnes de manipulation sur les réseaux sociaux lors des élections américaines. C'est le cas du compte le plus important en termes d'abonnés, qui postait des photographies de femmes musulmanes *« glamours »*, notamment des images de femmes en hidjab, et des slogans positifs.



DFR Lab / Le Monde

Parallèlement, trois comptes publiaient des photos positives et encourageantes au sujet des femmes noires, en utilisant des mots-clés comme #beauty #blackbeauty ou #blackisbeautiful. Sur d'autres, notamment les deux pages Facebook, étaient postés des images et slogans féministes – *« J'ai souvent pensé qu'il était injuste que les femmes restent chez elles lorsqu'il faut se battre. Si une femme a la force de porter un enfant, elle peut brandir une épée aussi bien que n'importe quel homme. »*

Certains comptes, sans poster d'images ou de textes ouvertement politiques, abordaient des thèmes sociétaux, comme les discriminations, l'exploitation de l'Afrique par l'Occident ou l'écologie. Sur une des photographies partagées par le compte écologiste, représentant une toile d'araignée, on peut voir dans le coin supérieur gauche le mot *« toile d'araignée »* écrit en russe. *« Cela peut être totalement fortuit, mais n'en demeure pas moins notable dans le contexte des soupçons que ce réseau était piloté par la Russie »*, écrivent les chercheurs.

Une campagne d'ampleur modeste

Le DFR Lab note cependant la portée limitée de cette opération de propagande : selon eux, les pages Facebook et les comptes Instagram en français ont réuni au total 141 000 abonnés. Le plus suivi,@les_femmes_musulmanes, disposait d'un peu plus de 10 000 followers, quand les autres comptes Instagram en comptaient autour de 2 000.

Selon les chiffres fournis par Facebook, ces 141 000 abonnés se répartissaient à peu près équitablement entre Instagram et Facebook. Le réseau social indique aussi que 12 400 utilisateurs localisés en France suivaient l'un des comptes Instagram en français.

Il est très probable que cette opération de propagande ait été interrompue par Facebook à ses débuts

Sollicité, Facebook n'a pas été en mesure de donner, au-delà du nombre d'abonnés, le nombre de ses utilisateurs ayant été en contact avec les contenus postés par les pages incriminées. Selon les chercheurs du DFR Lab, il est très probable que cette opération de propagande ait été interrompue par le réseau social à ses débuts, au moment où les comptes concernés tentaient de se *« construire activement une communauté »*. Ainsi, de nombreux comptes Instagram incitaient sans cesse ceux qui consultaient leur page à s'abonner et faisaient un usage intensif de mots-clés que l'on trouve fréquemment sur les comptes cherchant à acquérir rapidement une audience importante.

« Les questions demeurent quant à la taille de l'opération, la durée de son activité, quels autres contenus postaient ces comptes et s'ils étaient actifs sur d'autres plates-formes », explique aussi le rapport du DFR Lab.

Des soupçons visant la Russie

Deux éléments saillants ont retenu l'attention des chercheurs. D'abord, la stratégie déployée par ces comptes pour attirer des abonnés, notamment auprès de segments bien précis de la population. Ensuite, la prégnance des thématiques sinon politiques, du moins sociales, qui parfois sont loin de faire consensus dans la société française.

La combinaison de ces deux facteurs fait penser *« aux opérations de manipulation de la Russie, qui utilisaient des inquiétudes et des tensions sociales pour promouvoir la division et attaquer des hommes et femmes politiques dans différents pays »*, écrivent-ils. Ils ajoutent cependant qu'il *« n'y a pas suffisamment de preuve pour attribuer avec certitude* [ce réseau de comptes] *à l'Internet Research Agency ».* D'autant que les éléments rassemblés par le DFR Lab sont fragmentaires et que Facebook n'est pas en mesure de fournir davantage d'éléments.

Selon nos informations, le réseau social devrait contacter les autorités françaises pour leur donner les éléments rassemblés sur ce réseau de faux comptes avant leur suppression.

PIXELS

Désinformation : le Sénat français va, lui aussi, demander des comptes à Facebook

Une commission du Sénat vient de se joindre à neuf Parlements de différents pays, qui demandent à Mark Zuckerberg de venir s'expliquer devant eux.

Par Morgane Tual Publié le 26 novembre 2018 à 18h15 - Mis à jour le 26 novembre 2018 à 18h26

Facebook a décliné à plusieurs reprises l'invitation de cette commission internationale sur les fausses informations. SAUL LOEB / AFP

Royaume-Uni, Canada, Brésil, Australie, Irlande, Argentine, Lettonie, Singapour…Et maintenant la France et la Belgique. Lundi 26 novembre, la commission culture, éducation et communication du Sénat a rejoint la grande commission internationale réclamant une audition de Mark Zuckerberg, le patron de Facebook. Une parlementaire belge, Karine Lalieux, y participera également.

Une initiative rare : des parlementaires de ces dix pays doivent se réunir mardi 27 novembre à Londres, où ils ont invité, à plusieurs reprises, le fondateur de Facebook pour qu'il s'explique sur les problèmes liés aux contenus de désinformation circulant sur sa plate-forme. La sénatrice Catherine Morin-Desailly, présidente de la commission culture au Sénat, participera à cette audition, a-t-elle indiqué au *Monde*.

Mais Facebook a déjà prévenu : l'entreprise enverra Richard Allan, l'un des responsables de la politique publique de Facebook, M. Zuckerberg ayant plusieurs fois décliné l'invitation.

« Les fake news sont une menace pour la démocratie »

Les parlementaires des pays concernées veulent que Facebook s'explique sur la question des fausses informations. Celles-ci ont notamment circulé massivement pendant la campagne présidentielle américaine de 2016, parfois à des fins de manipulation politique, et inquiètent les législateurs de différents pays. L'affaire Cambridge Analytica pourrait aussi donner lieu à plusieurs questions. Facebook est ainsi accusé d'avoir laissé cette entreprise spécialisée dans l'influence politique indirectement siphonner les données de 87 millions d'utilisateurs de Facebook.

En s'associant à cette commission internationale hors du commun, la commission culture du Sénat *« rappelle ainsi son attachement à la défense des données personnelles et à la responsabilisation des plates-formes dans la lutte contre la manipulation des opinions »*, peut-on lire dans un communiqué sur le site du Sénat. *« Les "fake news" sont une menace pour la démocratie »*, souligne, dans ce même document, la sénatrice Catherine Morin-Desailly : *« Il est donc légitime que Facebook rende compte aux représentants du peuple. »* Et malgré les multiples refus de M. Zuckerberg de se présenter devant cette commission internationale, le Sénat français réitère son souhait d'entendre, dans ce cadre, le patron de Facebook.

Adoption des propositions de loi en France

Avec plus de 2 milliards d'utilisateurs actifs, Facebook est le réseau social le plus populaire au monde. Devenu un important canal de diffusion de fausses informations, le réseau social est de plus en plus scruté par les Etats, dans le cadre, notamment, d'une volonté de lutter contre la désinformation en période électorale. En France, l'Assemblée nationale a ainsi adopté les propositions de loi contre la désinformation, mardi 20 novembre, obligeant notamment les plates-formes comme Facebook à davantage de transparence sur les contenus diffusés de manière payante.

Pour Facebook, la pression s'est accentuée au printemps, avec le scandale Cambridge Analytica. M. Zuckerberg avait fini par s'expliquer devant le Congrès des Etats-Unis en avril, au cours de deux éprouvantes audiences de plusieurs heures. Il avait également été entendu en mai par des parlementaires européensdans une audience d'une heure et demie seulement, essentiellement occupée par les questions des eurodéputés – un format contesté par plusieurs d'entre eux.

Morgane Tual

Les révélations des hackeurs Fancy Bears ébranlent la lutte antidopage

Le groupe de pirates, probablement russes, voulait dénoncer les pratiques de stars américaines. Il a mis au jour surtout les faiblesses du système des autorisations d'usage à des fins thérapeutiques de produits interdits dans le sport.

Par Clément Guillou Publié le 30 septembre 2016 à 10h46 - Mis à jour le 06 octobre 2016 à 14h45

Le 16 septembre, les Fancy Bears ont publié un deuxième volet des données piratées de l'Agence mondiale antidopage. RAMIL SITDIKOV/ SPUTNIK / ICON SPORT

Pendant que le monde du sport vivait son moment de gloire quadriennal sous le soleil de Rio, une bande d'ours mal léchés a mis la main sur un énorme pot de miel et l'a renversé par terre. Le problème avec le miel : c'est alléchant, mais très poisseux. Et beaucoup se sont trouvés les mains sales et collantes, englués dans des centaines d'autorisations d'usage à des fins thérapeutiques (AUT).

Les « Fancy Bears », qui ne sont ni des ours ni extravagants, mais probablement russes, disaient vouloir dénoncer un dopage autorisé par les instances de lutte contre le dopage, au profit d'athlètes américains. En réalité, ils ont discrédité 107 sportifs n'ayant rien à se reprocher, mais ont surtout secoué le système antidopage et jeté le doute sur les méthodes du vainqueur du Tour de France 2012, Bradley Wiggins.

. Le système des autorisations d'usage à des fins thérapeutiques doit-il être revu ?

Les premières fuites ont généré des cris d'orfraie sur un prétendu dopage légal, les commentateurs tombant ainsi dans le piège des pirates et celui de Vladimir Poutine, heureux de mettre sur le même plan des sportifs *« pouvant légalement prendre des médicaments interdits aux autres »* et les accusations de dopage d'Etat visant la Russie. En réalité, cette fuite n'est pas accablante, ni pour le système des AUT ni pour la quasi-totalité des athlètes montrés du doigt.

Certains cas permettent toutefois d'identifier deux faiblesses : des AUT sont accordées par certains pays ou fédérations, et pas par d'autres ; au moins une fédération, l'Union cycliste internationale (UCI), a validé des AUT dans des conditions discutables, sans que l'Agence mondiale antidopage (AMA) y trouve à redire.

La star de la gymnastique Simone Biles, qui souffre de troubles de l'attention, bénéficie d'une AUT pour de la Ritaline, proche des amphétamines par sa composition. La Fédération internationale de gymnastique lui a accordé d'utiliser ce produit interdit – qui peut être précieux dans son sport –, abondamment prescrit aux Etats-Unis. Dans la Ligue américaine de base-ball, près de 10 % des joueurs bénéficient d'autorisations thérapeutiques pour des médicaments censés soigner les troubles de l'attention.

Si Simone Biles avait soumis cette demande à l'Agence française de lutte contre le dopage (AFLD), elle ne l'aurait probablement pas obtenue. Un jeune footballeur français s'est ainsi vu refuser plusieurs demandes d'AUT pour ce même médicament. Plus de la moitié des demandes faites à l'agence sont retoquées par son groupe d'experts, qui n'a pas le pouvoir de contester l'authenticité de la pathologie mais peut refuser le traitement demandé.

Président de la commission médicale de la Fédération internationale d'aviron, le docteur Alain Lacoste affirme rejeter lui aussi beaucoup de demandes d'AUT :

« Si l'athlète ne fournit pas la totalité du dossier médical, n'a pas démontré qu'il n'avait pas tout essayé, qu'il n'y avait pas d'alternative, on rejette. »

Le scandale provoqué par les Fancy Bears est l'occasion d'un audit général sur les demandes d'AUT, estime cet autre agent de la lutte antidopage :

« Le principe de l'AUT, c'est que ça ne doit conférer aucun avantage par rapport aux autres. Si un produit est accepté sur un continent et pas sur un autre, c'est un échec total. Quand on regarde ce qui se passe avec les corticoïdes, on voit que ça ne fonctionne pas. L'AMA est prise en flagrant délit de n'avoir pas réussi à assurer une harmonisation. »

L'autre échec de l'AMA réside dans son incapacité à contrôler les AUT délivrées, comme le démontre l'époque – révolue – où le médecin de l'UCI, Mario Zorzoli, tamponnait seul les demandes, là où trois avis sont requis en principe. Les conditions dans lesquelles Christopher Froome et Bradley Wiggins ont bénéficié d'autorisations pour la prise de corticoïdes auraient au moins dû éveiller les soupçons de l'agence mondiale.

Cela n'a pas été le cas, admet son directeur général, Olivier Niggli, qui argue d'un manque évident de moyens humains : *« A l'avenir, on pourrait renforcer les moyens de l'AMA pour pouvoir vérifier de façon plus fréquente les AUT délivrées, voire imaginer un organe centralisé qui délivre des AUT. »*

. Secret médical des sportifs : le dernier rempart peut-il sauter ?

« Vous voulez une solution pour les AUT ? Rendez leur publication obligatoire. N'importe quel athlète y réfléchira à deux fois, à moins d'en avoir vraiment besoin. » Manageur de l'équipe cycliste Cannondale, Jonathan Vaughters n'est pas seul à prescrire cette solution radicale contre les AUT abusives. La triathlète Jodie Swallow l'avait devancé en estimant qu'*« après tout il n'y a pas de honte à avoir une maladie dont on souffre vraiment… »*.

IMO Athlete TUES should be public @wada_ama . After all there is no shame in taking a medication for a condition you truly suffer from…

— jodieswallow (@Jodie Swallow)

Publier sur un site Internet toutes les autorisations thérapeutiques, et donc indiquer de quelle pathologie souffre chaque sportif ? C'est comme si certains sportifs avaient intégré le fait que, pour prouver leur bonne foi, ils devaient accepter d'être des citoyens de seconde zone. Obligés d'indiquer en permanence où ils sont, pour satisfaire aux contrôles inopinés, et de donner leur accord à l'intrusion de préleveurs à leur domicile la nuit, depuis l'an dernier, les voilà qui accepteraient de voir leurs maladies étalées sur la place publique.

« La forme qu'a prise la lutte contre le dopage est discutable car elle nuit à ma liberté. Mais c'est le seul système pour coincer les tricheurs », accepte, de guerre lasse, Gauthier Grumier. Le champion olympique d'épée par équipe à Rio a pourtant vu son nom associé à la rubrique dopage dans certains médias, et subi des commentaires diffamants sur les réseaux sociaux après la publication d'une AUT, remontant à 2009, pour un traitement en urgence à la suite d'une violente réaction allergique.

« On devrait avoir le droit de refuser certaines choses, mais alors on est jugé coupable. C'est toute l'ambiguïté de la lutte antidopage. Alors allez-y, imprimez mon carnet de santé en quatre par trois, je n'ai rien à cacher ! »

C'est plus ou moins ce qu'a fait le pistard britannique Callum Skinner, qui, depuis la révélation de ses AUT, a appelé ses médecins et les hôpitaux l'ayant accueilli lors de crises d'asthme pour réunir un dossier médical et le publier dans la presse.

« Bien sûr, pour un asthme [qui peut nécessiter la prise de corticoïdes]*, ce ne serait pas un problème, mais il y a derrière certaines AUT des maladies génétiques, des maladies graves »*, s'inquiète l'ex-ministre des sports Valérie Fourneyron, présidente du comité santé de l'AMA et fidèle au serment médical qu'elle a prêté jadis.

Surtout, met en garde Olivier Niggli, chaque AUT serait sujette à de multiples interprétations du grand public. *« Ce ne serait pas raisonnable ni proportionné »*, résume le juriste, qui connaît trop bien les risques pour l'AMA de s'en prendre au secret médical. La dernière révision du code mondial antidopage a été

surveillée, rappelle-t-il, par Jean-Paul Costa, ancien président de la Cour européenne des droits de l'homme (CEDH), pour *« nous dire jusqu'où on pouvait aller »*. Surtout, l'épisode donnera du poids à la campagne de dénigrement menée par le CIO contre l'AMA dont il souhaite redéfinir les prérogatives.

. Quelles conséquences pour l'Agence mondiale antidopage ?

Elle est sans doute la principale victime des Fancy Bears : en centralisant dans son système d'administration et de gestion antidopage (Adams) la localisation, les valeurs sanguines et les certificats médicaux des athlètes, elle a passé avec eux un contrat moral. Celui-ci s'est rompu par ce piratage, réalisé de manière très simple.*« Cette attaque fragilise vraiment la confiance dans la chaîne de la lutte antidopage »*, admet Valérie Fourneyron, qui a tout de suite *« ressenti beaucoup d'inquiétude et de regrets vis-à-vis des sportifs »*.

La championne olympique britannique de hockey sur gazon Sam Quek a publié sur Facebook un texte remarqué, dans lequel elle dit se sentir *« violée »* par la publication de ses données médicales, et craint que certains sportifs renoncent désormais à demander des AUT par peur de voir leur nom sali.

L'AMA peut clamer tant et plus que personne n'a cassé la sécurité du système Adams, reste que les pirates ont obtenu l'accès à une partie de son contenu ; que, pendant les Jeux olympiques, le compte de Ioulia Stepanova, la lanceuse d'alerte sur le dopage dans l'athlétisme russe, avait aussi été piraté ; et que, en 2014, des médias s'étaient procuré les données du passeport biologique de centaines d'athlètes.

Et ce alors que plusieurs plaintes contestant l'obligation de localisation sont en attente de jugement par la CEDH. La fuite de données personnelles pourrait peser dans la décision des juges, et toute restriction au système de localisation signifierait un recul majeur de la lutte contre le dopage.

L'AMA va donc devoir s'attacher à retrouver la confiance d'athlètes qui, après les scandales de la Fédération internationale d'athlétisme et du sport russe, trouveront dans cet épisode une raison supplémentaire de douter de l'utilité d'un système qui leur demande beaucoup.

Clément Guillou

A Londres, Facebook sous le feu d'une commission internationale de parlementaires

Les représentants de dix pays, dont la France, attendaient Mark Zuckerberg pour qu'il s'explique sur la responsabilité de Facebook dans la circulation de la désinformation sur Internet. Leurs questions, vives et dérangeantes, ont été posées à un vice-président du réseau social.

Le Monde avec AFP et AP Publié le 27 novembre 2018 à 19h43

Comme prévu, l'invité d'honneur a manqué à l'appel. Mark Zuckerberg, le président de Facebook, ne s'est pas rendu à Londres, mardi 27 novembre, malgré les convocations répétées des parlementaires de dix

pays, dont la France. Le numéro 1 de Facebook était pourtant depuis plusieurs mois dans le viseur de la Commission britannique sur le numérique, la culture et les médias (DCMSC) de la Chambre des communes et de son président, Damian Collins, dans le cadre d'une enquête sur le phénomène des « fake news ». Ces dernières semaines, plusieurs pays se sont joints à l'initiative britannique pour réclamer à Mark Zuckerberg des explications sur la circulation des fausses informations permise par son réseau social.

A la place du numéro 1 de Facebook, lors de l'audition tenue à la chambre basse du Parlement britannique, mardi : Richard Allan, vice-président de Facebook et responsable de la politique publique, qui a répondu aux questions des députés. Il y a défendu la décision de son PDG de ne pas témoigner dans le cadre de la Commission britannique, en expliquant que Mark Zuckerberg s'était déjà exprimé, plus tôt dans l'année, devant des parlementaires américains eteuropéens. Des auditions tendues, qui avaient eu lieu après le scandale généré par l'affaire Cambridge Analytica, et les questions posées dans le monde entier face à l'utilisation de Facebook par des organisations ou des pays étrangers souhaitant influer sur l'élection d'un pays, notamment à travers des campagnes de désinformation.

« Injustice fondamentale »

A Londres, à côté de Richard Allan, la commission internationale de parlementaires a cependant conservé un siège vide, avec un petit carton signifiant à la fois l'absence du principal responsable du réseau social et leur souhait d'en entendre davantage de sa part.

Lors de l'audition de Facebook à la chambre basse du Parlement britannique, mardi 27 novembre. Gabriel Sainhas / AP

« Je ne vais pas vous contredire : nous avons mis à mal la confiance que le monde pouvait avoir en Facebook, en raison de certaines actions de notre part », a justifié Richard Allan lors de l'audition, en réponse à un parlementaire canadien, Charlie Angus, qui a déclaré que Facebook avait *« perdu la confiance de la communauté internationale quant à sa capacité à se réguler soi-même »*.

« Pendant que nous jouions avec nos téléphones et nos applications, nos institutions démocratiques (...) semblent avoir été bouleversées par le club des milliardaires de Californie », a lancé Charlie Angus à Richard Allan. La sénatrice française Catherine Morin-Desailly a, de son côté, qualifié de *« scandale »*l'approche de Facebook en matière de protection de données. Le parlementaire irlandais Eamon Ryan a, lui, parlé d'*« injustice fondamentale »* en ce qui concerne l'accès à des données d'utilisateurs de Facebook par des tiers.

Des documents internes révélés

Lors de l'audition, Damian Collins a également demandé à Richard Alland de commenter le contenu de documents internes de Facebook saisis par l'intermédiaire de l'entreprise américaine Six4Three et provenant, à l'origine, d'une procédure juridique aux Etats-Unis. Des documents dont le contenu exact, de même que les dates d'écriture, et les dates de réception par Facebook ou d'envoi à Facebook restent flous, mais que Damian Collins avaient présenté comme cruciaux, la veille de l'audition.

Selon le discours tenu par le député britannique, l'un des e-mails contenus dans ces documents affirme qu'un ingénieur de Facebook avait averti son entreprise dès octobre 2014 que des personnes, potentiellement situées en Russie, avaient réussi à siphonner un nombre considérable de données d'utilisateurs Facebook.

Damian Collins a ainsi évoqué *« trois milliards »* de *« data points »* (des éléments de données utilisateurs) extraites chaque jour du réseau social par des *« adresses IP en provenance de Russie »*. Ce qui contredirait les affirmations publiques de Facebook, selon lesquelles des activités suspicieuses en provenance de Russie

n'ont commencé à être signalées et examinées qu'en 2016, dans le cadre de la campagne électorale américaine.

« Si les adresses IP russes extrayaient d'énormes quantités de données de la plate-forme, (…) *était-ce signalé ou juste caché sous le tapis ? »*, a demandé Damien Collins à Richard Allan. *« Toute information que vous pouvez avoir vue* (…) *est au mieux partielle, au pire potentiellement trompeuse »*, a répondu ce dernier, ajoutant que les e-mails évoqués par Damian Collins comportaient des informations *« partielles »* et *« non vérifiées »*. Peu après l'audition, Facebook a envoyé un communiqué à l'agence Bloomberg, précisant ce démenti : *« Les ingénieurs qui ont signalé ces problèmes ont ensuite examiné plus en détails les élements concernés et n'ont pas trouvé de preuve qu'il s'agissait bien d'activités suspectes en provenance de Russie. »*

Des réponses qui ne sont peut-être qu'un premier tour de chauffe pour Facebook. Selon Bloomberg, Damian Collins a également indiqué, lors de l'audition, qu'il souhaitait publier l'intégralité des documents en sa possession *« dans le courant de la semaine »*, afin de presser davantage Facebook à s'expliquer sur son manque potentiel de vigilance face aux utilisations problématiques de sa plateforme.

Comment les plates-formes du Web s'organisent pour éviter un « hack » des élections

Par Damien Leloup et Martin Untersinger
Publié le 17 octobre 2018 à 20h27 - Mis à jour le 26 novembre 2018 à 15h08

Deux ans après Donald Trump, et à l'approche des élections législatives aux Etats-Unis, la Silicon Valley veut éviter que les réseaux sociaux redeviennent un terrain d'influence pour des puissances étrangères.

Nous sommes le 2 novembre 2016 et Donald Trump sillonne la Floride. A moins d'une semaine de l'élection présidentielle américaine, le candidat républicain bataille pour arracher cet Etat clé à sa rivale, Hillary Clinton. Le même jour, le compte Twitter de la section du Tennessee du Parti républicain alerte ses 130 000 abonnés : une *« fraude électorale »* est en cours. *« Des dizaines de milliers de votes invalides parmi les voix d'Hillary sont repérées dans le comté de Broward, en Floride »,* affirme-t-il.

Cette information était totalement fausse. Tout comme le prétendu compte du Tennessee, en réalité piloté à Saint-Pétersbourg par une officine russe chargée de la propagande sur Internet. Pendant plusieurs mois, la campagne électorale américaine a été accompagnée par une opération de manipulation des réseaux sociaux, fomentée par le Kremlin et dont le faux compte des républicains du Tennessee n'était qu'un des nombreux avatars. Cette opération, mêlant fausses et vraies informations, dont la diffusion était parfois accélérée grâce à l'achat de publicité, était

destinée à attiser les divisions politiques, à semer la confusion et à décourager certains électeurs de se déplacer.

Quelques jours plus tard, Donald Trump est élu. Alors que la Silicon Valley, très majoritairement démocrate, déplore la victoire du candidat républicain, une partie des Etats-Unis accuse les réseaux sociaux d'avoir directement contribué à sa victoire. C'est dans ce contexte que le patron de Facebook, Mark Zuckerberg, prend la parole. *« Il faut avoir un profond manque d'empathie pour affirmer que la seule raison qui fait qu'une personne ait pu voter comme elle l'a fait est qu'elle a vu une fausse information »*, dit-il, dans une tentative maladroite d'explication. Puis, dans un message posté directement sur Facebook le 12 novembre 2016, il affirme, citant des études internes sur le sujet, que, *« sur l'ensemble de Facebook, plus de 99 % de ce que voient les utilisateurs est authentique. Seule une très faible partie du contenu publié est composée de fausses informations et de* hoax [canulars] *»*.

Une campagne visant avant tout à démobiliser

Pourtant, les employés de l'agence de propagande russe Internet Research Agency (IRA), avaient parfaitement compris en 2016 tout le bénéfice qu'ils pouvaient tirer des outils de Facebook, de Twitter et d'autres réseaux sociaux comme Tumblr ou Reddit. D'après les relevés fournis par Facebook aux parlementaires américains enquêtant sur les campagnes d'influence russes durant l'élection, 116 millions de personnes ont été exposées à des messages publiés par l'IRA durant la campagne, et 10 millions de personnes ont vu les publicités ciblées financées par cette même agence sur Facebook.

Quels étaient ces messages ? A quelle fin étaient-ils publiés ? L'analyse des publications sur Facebook concernées montre que la campagne russe avait plusieurs objectifs complémentaires. Leur but premier n'était pas de convaincre, mais plutôt de mobiliser ou de démobiliser des électorats. Une partie importante des messages s'adressait ainsi aux Afro-Américains, qui votent historiquement démocrate à une écrasante majorité, et aux soutiens de Bernie Sanders, le candidat à l'investiture de la gauche du Parti démocrate, battu par Hillary Clinton à l'issue des primaires.

Ce groupe Facebook géré par l'IRA publiait de très nombreux messages incitant les afro-américains à ne pas voter.

De très nombreux messages de la propagande de l'IRA affirmaient ainsi que Hillary Clinton était raciste et soutenait les violences policières contre les communautés noires. Ils s'accompagnaient parfois de messages très explicites appelant les Afro-Américains à rester chez eux le jour de l'élection. Les sympathisants de Bernie Sanders ont eux eu droit à des messages les incitant à voter pour Jill Stein, la candidate écologiste appréciée d'une partie de la gauche de la gauche américaine, plutôt que de voter pour Hillary Clinton.

Grâce aux outils de publicité ciblée de Facebook ou de Twitter, les agents russes ont pu précisément cibler leurs messages, pour parler à des publics très précis, par exemple les personnes qui « aimaient » les pages de Black Lives Matter dans le premier cas, ou de Bernie Sanders dans le second.

A ces publicités ciblées s'ajoutaient des comptes se présentant comme ceux d'Américains engagés, mais qui étaient en réalité administrés en Russie. Ces comptes publiaient de très nombreux messages, le plus souvent sur des sujets de société clivants, dans le double but d'acquérir rapidement un grand nombre d'abonnés, et de miner la confiance des Américains dans leurs institutions et dans leurs élus.

Une campagne efficace et peu coûteuse

Ces messages ont-ils été efficaces ? C'est la thèse défendue notamment par la chercheuse Kathleen Hall Jamieson dans un livre sorti à la fin de septembre, *Cyberwar, how Russian hackers and trolls helped elect a president* (« Cyberwar, comment les pirates et les trolls russes ont aidé à élire un président », Presses universitaires d'Oxford, en anglais). Elle y détaille la manière dont ces messages publiés sur les réseaux sociaux ont pu avoir un impact notable, notamment en parvenant à imposer un agenda politique et médiatique favorable à Donald Trump.

Message d'un site anti-immigration géré par l'IRA russe. Facebook

« Lorsque les discussions sur l'immigration dominent le fil d'information d'une personne au détriment d'autres sujets, ce sujet devient plus important pour l'utilisateur, et a plus de chance de jouer un rôle important dans son évaluation d'un candidat », écrit-elle. En « poussant » des sujets coïncidant avec le programme de Donald Trump,

comme l'immigration, le port d'arme, le traitement des vétérans, mais aussi le contenu des e-mails du Parti démocrate rendus publics par WikiLeaks, l'IRA est parvenue à influer sur la campagne, estime-t-elle.

Sans aller jusqu'à affirmer que la campagne d'influence russe a fait élire Donald Trump, Kathleen Hall Jamieson note que plusieurs facteurs distincts ont permis, en 2016, à cette opération d'obtenir des résultats remarquables : un nombre plus important que d'ordinaire d'électeurs indécis — et donc plus sensibles aux messages politiques — ou encore le faible taux de popularité des deux principaux candidats.

Les détails d'organisation de la campagne montrent également que les agents russes ont fait preuve d'un certain degré de sophistication dans leur utilisation des réseaux sociaux, par exemple en ciblant plus particulièrement les électeurs des Etats les plus disputés, ou en adaptant de manière astucieuse leurs messages en fonction des cibles. Sans être, non plus, particulièrement brillants en la matière : la plupart des techniques utilisées relevaient des outils de marketing classiques. Et les agents de l'IRA ont aussi commis un certain nombre d'impairs, en publiant notamment de nombreux messages écrits dans un anglais approximatif, voire en essayant d'organiser une *« manifestation de mineurs »* à Philadelphie… ville dans laquelle aucune mine n'a jamais existé.

Publicité financée par l'IRA - les campagnes russes de 2016 étaient parfois subtiles, et parfois beaucoup moins.

Myopie initiale des réseaux sociaux… et des autorités

Comment une opération menée par une grande puissance a-t-elle pu échapper à une entreprise comme Facebook, censée être à la pointe de la technologie ? Cette myopie est d'autant plus surprenante que l'existence de l'IRA, et son activité visant les Etats-Unis, est connue et documentée depuis 2013.

« Elles utilisaient encore une définition de la cyberguerre centrée sur les techniques de piratage traditionnelles. Elles n'étaient pas préparées à détecter ni à endiguer les campagnes de propagande », écrit Alex Stamos. Il est bien placé pour le savoir, il occupait le poste de responsable de la sécurité de Facebook pendant l'élection de 2016. *« Les gens connaissaient l'existence de l'usine à trolls, mais personne ne se doutait*

de l'ampleur réelle de l'opération », soutient Ben Nimmo, expert à l'Atlantic Council et l'un des meilleurs connaisseurs du sujet. D'autant que dans les cercles progressistes, dans la Silicon Valley comme à Washington, Hillary Clinton était donnée gagnante.

Les pouvoirs publics américains ont aussi une responsabilité dans l'affaire. Depuis la fin de la guerre froide, la contre-propagande, a fortiori intérieure, n'est plus une priorité de l'appareil de renseignement américain. Les services ont ainsi commis une erreur d'analyse enpensant que la Russie n'oserait pas porter le glaive de la propagande directement contre les Etats-Unis.

Prise de conscience des géants du Web

Deux ans après, les grandes plateformes du Web ont opéré un demi-tour complet. Ceux qui jugeaient fantaisiste l'idée que des *« fake news »* aient pu altérer l'élection se sont désormais investis de la mission de*« protéger l'intégrité des élections »*.

Chez Facebook, on martèle que cet effort, qui mobilise selon l'entreprise plusieurs milliers de salariés, est de même ampleur que son basculement massif vers les technologies mobiles. Incarnation de cette nouvelle priorité, largement mise en avant dans les médias, la création d'une*« salle de crise »* durant l'été 2018, censée réunir les principaux responsables de cet effort. Elle a été inaugurée par Facebook mercredi 17 octobre, trois semaines avant les élections américaines de mi-mandat.

Dans l'ensemble, les efforts des principales entreprises de la Silicon Valley pour lutter contre l'ingérence lors de ce scrutin, premier test de grande ampleur à haute valeur symbolique, ont pris quatre directions.

- **La modération des contenus**

Les plateformes américaines ont d'abord annoncé étoffer les rangs des équipes chargées de modérer ce que leurs utilisateurs publient, une question qui dépasse largement la question de l'ingérence étrangère. Chez Google, YouTube a promis d'augmenter d'un quart ses effectifs spécialisés dans cette question. Twitter l'a fait de 15 %, et Facebook les a presque multipliés par deux.

Les entreprises ont également supprimé des millions de comptes fallacieux : Facebook en a retiré de son réseau 583 millions au premier trimestre 2018, et continue de le faire, tandis que Twitter bloque quotidiennement plus de 500 000 connexions de robot.

- **La transparence publicitaire**

Facebook comme Twitter ont fait un effort de transparence quant aux publicités politiques circulant sur leurs réseaux et visibles par les utilisateurs, en appliquant les mêmes règles que celles appliquées aux publicités politiques télévisées, qui doivent obligatoirement indiquer qui les ont financées.

- **La lutte contre les fausses informations**

Plus globalement, les réseaux sociaux tentent de purger leurs réseaux des fausses informations. Un projet ambitieux, d'autant que la propagande n'emprunte pas toujours la voie des *fake news* et que les producteurs de fausses informations n'ont pas toujours pour objectif de pourrir le débat politique. Les réseaux sociaux, et particulièrement Facebook, tentent de limiter l'audience des sites producteurs de fausses nouvelles. Facebook met ainsi souvent en avant son partenariat noué en 2017 avec des médias internationaux spécialistes de la vérification des faits (dont *Le Monde*).

- **L'intelligence artificielle**

Les plateformes abattent aussi la carte à la mode de l'intelligence artificielle. Facebook affirme ainsi avoir supprimé 30 000 faux comptespeu avant l'élection présidentielle française de 2017 (sans que ces derniers aient trempé dans une opération de manipulation), et d'avoir supprimé un nombre non précisé de comptes similairement louches lors de l'élection en Alabama.

Prise de conscience bien réelle

Mark Zuckerberg le 10 avril, lors de son audition parlementaire sur l'usage de Facebook durant l'électin présidentielle. Andrew Harnik / AP

Toutes ces mesures sont-elles efficaces ? Depuis deux ans, elles ont donné de premiers résultats, encore à confirmer, note une étude de l'université Stanford. Et au sein des états-majors des grandes entreprises du Web, la prise de conscience est bien réelle, juge Eli Pariser, interrogé par *Le Monde* en septembre. « *Aujourd'hui, depuis Mark Zuckerberg jusqu'aux employés du bas de l'échelle, tout Facebook se pose sérieusement la question de savoir quelles sont les dynamiques sociales à l'œuvre sur la plateforme* », analyse-t-il.

« Les plateformes reviennent de loin, et se débrouillent bien mieux. En 2016, elles étaient dans le déni. Elles ne le sont plus », veut croire Ben Nimmo, expert à l'Atlantic Council. Les principales plateformes en ligne*« se sont*

améliorées » reconnaît également le sénateur américain Mark Warner. Ce démocrate, vice-président de la puissante commission sur le renseignement, était l'une des voix les plus critiques sur le rôle des grandes plateformes de la Silicon Valley lors de l'élection de 2016. Lors d'une audition au Sénat, au début de septembre, il s'est même dit*« impressionné »* par les efforts déployés par certaines d'entre elles.

Toutes ne trouvent pas grâce à ses yeux cependant.*« Google, pendant un peu plus d'un an et demi*[après l'élection de 2016] *a été plutôt mauvais. La plupart des experts disent que YouTube est utilisé pour radicaliser les gens : Google doit mettre en place les mêmes protocoles que les autres entreprises »,* estime le sénateur. Moins mis sous pression que Facebook pour son rôle dans la diffusion de propagande, Google a tout de même reconnu, en 2017, avoir découvert 50 000 dollars de publicités, vraisemblablement payées par des agents russes, sur ses différentes plateformes pendant la campagne électorale.

Des tentatives moins nombreuses et plus discrètes

Cela étant, la plupart des experts notent que jusqu'à présent la campagne des élections américaines de mi-mandat n'a pas été autant polluée que l'élection de 2016. *« Nous n'avons rien vu qui se rapproche de ce que la Russie a réalisé en 2016 »,* reconnaissait, en juin, auprès du*Washington Post*, Christopher Krebs, un cadre du ministère de l'intérieur, à l'issue d'une réunion au siège de Facebook consacrée aux élections de mi-mandat.

Chez Facebook, principal concerné, on martèle qu'il s'agit d'une *« course à l'armement »* permanente. De fait, le réseau social a annoncé, à plusieurs reprises ces derniers mois, des suppressions de comptes liés, selon l'entreprise, à des opérations d'influence étrangères. Ces dernières sont-elles moins nombreuses, ou les barrières mises en place par les réseaux sociaux jouent-elles leur rôle ?

En septembre, une ONG a prouvé qu'il était encore possible d'acheter des publicités sur Google en reprenant de nombreux éléments (adresse, informations fiscales, etc.) de l'IRA. Des internautes et des chercheurs ont également trouvé des correspondances entre des messages publiés récemment sur le forum Reddit et l'infrastructure technique de l'IRA. Sur Twitter, des chercheurs ont identifié 6,6 millions de messages pointant vers de fausses informations ou des théories du complot un mois avant l'élection de 2016. Ils étaient encore 4 millions à le faire six mois après l'élection.

Désormais, les acteurs de la désinformation en ligne ont recours à des méthodes pour dissimuler leur provenance et leurs activités, qui contrastent avec le culot et le peu de précaution de l'IRA lors de l'élection de 2016. *« Ils ont appris de leurs erreurs.* (…) *L'opération de 2016 était amatrice, primitive. Mais là, ils utilisaient des VPN, des numéros de téléphone sur Internet… Ils essayaient de s'incruster parmi la population américaine, en essayant même de recruter des gens en chair et en os »,*détaille Ben Nimmo. Ce dernier explique aussi que les propagandistes utilisent davantage d'images et moins de texte, une méthode qui rend la détection de leur origine, basée sur la langue, beaucoup plus ardue.

« La stratégie [russe]*, qui a fait ses preuves, est à présent à la disposition de qui veut s'en servir. Et l'histoire récente indique qu'une fois qu'un puissant Etat a démontré l'efficacité d'une technique de nombreux autres groupes se précipitent pour en élaborer des versions moins chères, souvent plus rapides et légères »,* écrivait Alex Stamos cet été. Le manuel écrit par les trolls du Kremlin est même suivi à la lettre par des Américains : Facebook a tout récemment retiré de sa plateforme 559 pages et 251 comptes,opérés essentiellement aux Etats-Unis.

Mais déterminer ce qui relève de la propagande politique étrangère et ce qui constitue une expression politique légale dans un pays comme les Etats-Unis, où les divisions internes confinent à l'hystérie, s'avère particulièrement difficile. *« L'un des plus gros dangers, ce sont les faux positifs. Les gens sont tellement déterminés à trouver des opérations russes ou iraniennes, qu'il y a un risque de dire "j'ai trouvé une usine à trolls" quand ce ne sont que des activistes »,* rappelle Ben Nimmo.

Manquements du gouvernement fédéral

Le problème d'une éventuelle ingérence étrangère dans les élections de mi-mandat n'est pas la seule responsabilité des réseaux sociaux. Problème : l'appareil d'Etat américain tarde à se mettre en ordre de bataille. Il n'existe aucun organe spécialisé, et la responsabilité de la contre-ingérence numérique est éclatée entre plusieurs ministères et agences. *« A cette date, aucun plan coordonné et consolidé pour répondre à l'ingérence russe n'a été dévoilé au public.* (…) *L'exécutif est paralysé »*,écrivait en début d'année Clint Watts, ancien agent du FBI et auteur d'un livre sur le sujet.

L'un des principaux blocages n'est pas à chercher plus loin qu'à la Maison Blanche. Donald Trump est *« le problème dont personne n'ose parler »*, lâche Peter Singer, expert au think tank New America Foundation et auteur de *Like War, the Weaponization of Social Media. « Tout le monde dans les services de renseignement a conscience que la Russie est une énorme menace. Mais le président refuse encore d'accepter cette vérité. Dans une Maison Blanche normale, face à une menace comme celle-là, il y aurait un responsable spécialement désigné. Mais il n'y a pas de leadership à la Maison Blanche, chaque agence doit travailler dans son coin »,* juge, pour sa part, le sénateur Mark Warner.

Problèmes structurels et enjeux sociaux

L'efficacité de la lutte contre la désinformation d'origine étrangère reste aussi sujette à caution de manière structurelle. Notamment parce que les principes même de fonctionnement des réseaux sociaux comme Facebook et Twitter peuvent faciliter la diffusion de fausses informations ou la viralité de contenus ultrapartisans. En accordant une gigantesque importance à « l'engagement », c'est-à-dire au fait qu'un contenu suscite des commentaires, des partages ou des « j'aime », ces plateformes donnent mécaniquement une grande visibilité aux contenus émotionnels, qui font peur, choquent ou amusent.

Pour trois universitaires de l'université de New York, auteurs d'un rapport sur la lutte contre les opérations de propagande russe, les grandes plateformes ne sont pas allées assez loin, *« car s'attaquer en profondeur à la désinformation requerrait de reconsidérer leur modèle d'affaire basé sur la publicité, qui sous-tend toute l'industrie numérique ».*Ces plateformes *« sont conçues pour assurer le succès de la publicité. Les campagnes de désinformation ne sont pas très différentes de n'importe quelle campagne publicitaire »,* cinglait, en janvier, un rapport de la New America Foundation.

Mais au-delà des réseaux sociaux, le principal terreau qui a fait le jeu de la désinformation en 2016 est bien connu : c'est l'état d'extrême inflammabilité et de profonde division du paysage politique américain,rappelle la sociologue Zeynep Tufekci, l'une des meilleures observatrices des grandes plateformes, dans les colonnes du *New York Times : « L'ingérence étrangère est à notre paysage politique ce que la fièvre est à la tuberculose : un simple symptôme d'un mal plus profond. »*

Damien Leloup
Martin Untersinger

Facebook durcit sa modération contre les « infox » liées à un jour de vote

Le réseau social a expliqué, lundi, qu'il cherche à limiter la portée de messages pouvant décourager les électeurs à se rendre aux urnes, quelques semaines avant la tenue des élections de mi-mandat aux Etats-Unis.

Publié le 16 octobre 2018 à 12h52 - Mis à jour le 16 octobre 2018 à 15h56

Alors que les élections de mi-mandat se rapprochent aux Etats-Unis (elles doivent avoir lieu le 6 novembre), Facebook a annoncé l'extension de certaines règles de modération pour limiter au maximum la visibilité sur son réseau des fausses informations sur le scrutin.

Tomberont sous le coup de ces nouvelles règles les messages expliquant qu'il est possible de voter par texto (ce n'est pas le cas) ou mettant en doute l'impact réel d'un bulletin (par exemple : un message Facebook qui dirait *« votre voix ne sera pas comptée si vous avez déjà voté aux primaires »*). Facebook avait depuis 2016 des règles en la matière, mais elles étaient cantonnées, selon le réseau social, aux fausses informations concernant les *« dates, lieu, horaires et prérequis pour voter »*.

L'ensemble de ces messages, une fois portés à la connaissance de Facebook, ne seront pas nécessairement supprimés. En cas de doute, Facebook sollicitera les organismes de vérification des faits avec lesquelles il travaille. S'ils estiment que l'information est mensongère, la visibilité des contenus sera réduite.

« Canaux dédiés »

Afin de limiter ce type de messages, les utilisateurs de Facebook aux Etats-Unis pourront directement signaler un message qu'ils estiment problématique, avec l'apparition d'une option « Signaler une information incorrecte concernant le vote ». Les autorités électorales américaines disposent également désormais de*« canaux dédiés »* au signalement de telles fausses informations, précise Facebook dans son communiqué. Les équipes de modération de Facebook pourront ensuite décider de supprimer les messages litigieux, ou d'en réduire la visibilité.

Les nouvelles options de signalement de Facebook.

Autant d'exemples qui rappellent des messages qui ont été diffusés sur Facebook lors de l'élection présidentielle américaine de 2016. La justice américaine avait par exemple établi que des faux profils Facebook, dont certains contrôlés par l'IRA (l'agence russe de propagande sur Internet, sise à Saint-Pétersbourg), avaient diffusé des messages quelques jours avant le vote appelant au « boycott du scrutin » par certaines catégories de population. Des publicités diffusées sur Facebook par des comptes russes ont été épinglées comme ayant servi de support d'influence pour favoriser Donald Trump pendant l'élection.

Un contexte qui explique les nombreuses mesures annoncées actuellement par Facebook, pour éviter que sa plateforme soit utilisée à des fins de manipulation électorale pendant les élections de mi-mandat de 2018. Facebook a ainsi annoncé,il y a quelques jours, la suppression de centaines de pages et de comptes suspectés d'être d'avoir des *« comportements inauthentiques »*. Nombre de ces pages et comptes étaient connus pour leur activisme politique.

Facebook met en scène sa « salle de crise » pour contrer d'éventuelles manipulations électorales

Le réseau social est mis en cause depuis deux ans pour ne pas avoir su combattre des campagnes de désinformation, en particulier pendant la présidentielle américaine de 2016.

Le Monde avec AFP Publié le 20 septembre 2018 à 10h11 - Mis à jour le 20 septembre 2018 à 10h11

À quelques semaines des élections de mi-mandat aux États-Unis, le 6 novembre, Facebook met les bouchées doubles en terme de communication. Objectif : convaincre les utilisateurs et les pouvoirs publics que l'entreprise met tous les moyens en œuvre pour éviter de réitérer le fiasco de 2016 – le réseau social avait été exploité par un organisme de propagande proche du Kremlin afin d'influencer l'opinion publique avant l'élection américaine.

Depuis, Facebook enchaîne les annonces, savamment égrainées au fil des mois – (chasse aux faux comptes, contrôle renforcé des publicités politiques, dévalorisation des fausses informations, ETC). La dernière en date se veut spectaculaire : mercredi 19 septembre, le réseau social a annoncé la mise en place d'une « salle de crise » au cœur de son « campus » à Menlo Park, en Californie. Objectif affiché : déjouer *« en temps réel »* les tentatives de manipulation des élections. Elle devrait être opérationnelle pour l'élection présidentielle au Brésil, dont le premier tour est prévu pour le 7 octobre, et servira également à détecter les activités suspectes sur le réseau social autour des élections de mi-mandat aux Etats-Unis.

seven weeks from the U.S. midterm elections, Facebook is on a sprint to prepare against bad actors and foreign infl… https://t.co/XKwiz9aaIx

— MikeIsaac (@rat king)

Ce *« centre de commandement »* sera en mesure *« de prendre des décisions en temps réel »* en cas de *« pire des scénarios »,* comme des afflux de messages trompeurs à l'approche des élections ou le jour même du scrutin, a expliqué Samidh Chakrabarti, responsable « élections et engagement civique » lors d'une conférence téléphonique destinée à la presse mercredi. Il a cité comme exemple des messages erronés indiquant que l'on pouvait voter par SMS, comme cela s'est produit lors de scrutins précédents.

Un vocabulaire militaire

Seulement voilà : à part la création d'une pièce consacrée, qu'apporte cette annonce de nouveau ? Pas grand-chose. Le terme « salle de crise » (« war room » ou « salle de guerre » en traduction littérale, un vocabulaire militaire) est soigneusement choisi pour afficher une mobilisation générale de Facebook sur le front de la guerre contre les manipulations de sa plateforme. Mais l'entreprise américaine n'a annoncé à cette occasion aucun nouveau changement dans son fonctionnement.

Dans un long texte sur les tentatives de manipulation d'élections publié la semaine dernière, Mark Zuckerberg, le patron de Facebook, avait assuré que le réseau social était *« mieux préparé »*. Pour autant, avait-il poursuivi, *« nous faisons face à des adversaires sophistiqués et bien financés. Ils ne lâcheront pas et ils vont continuer à évoluer »*.

Pour l'ex-responsable de la sécurité informatique de Facebook Alex Stamos, qui a quitté l'entreprise cet été, *« il est bien trop tard pour réhabiliter de manière efficace la sécurité de nos élections pour les élections de mi-mandat de 2018, mais il y a* [des mesures] *qui peuvent être prises pour aider les Etats-Unis à empêcher des attaques en 2020* [année de la prochaine élection présidentielle] *»*, écrivait-il dans une tribune traduite fin août dans Le Monde.

Facebook remporte de premiers succès face aux fausses informations, note une étude de Stanford

Une étude menée par trois chercheurs de l'université Stanford montre que le succès de certaines publications mensongères sur Facebook s'étiole depuis la fin de 2016.

Publié le 17 septembre 2018 à 14h31 - Mis à jour le 17 septembre 2018 à 14h31

Les efforts entrepris par Facebook depuis deux ans pour tenter de limiter la propagation d'informations mensongères pourraient commencer à payer. C'est ce qui ressort d'une étude menée par trois scientifiques de l'université Stanford,publiée vendredi 14 septembre. Ces derniers ont identifié 570 sites *« producteurs de fausses informations »* et ont étudié le niveau d'activité engendré par leurs articles sur Twitter et sur Facebook entre janvier 2015 et juillet 2018.

L'étude montre que le nombre d'utilisateurs de Facebook *« likant »*, commentant ou partageant des articles publiés sur des sites connus pour leurs publications mensongères ou fortement biaisées a nettement baissé à partir de la fin de l'année 2016. Cette tendance semble propre à Facebook, puisque le nombre d'utilisateurs de Twitter partageant ces articles a continué sa hausse pendant la même période. Au début des mesures des chercheurs, le rapport entre un partage sur Twitter et une interaction sur Facebook était de 1 pour 40 (1 partage Twitter pour 40 interactions sur Facebook). En juillet 2018, il n'était plus que de 1 pour 15.

Une étude réalisée par trois chercheurs à l'université de Stanford montre que le succès de certaines publications mensongères sur Facebook s'étiole depuis fin-2016. Allcott, Gentzkow, Yu / Stanford / Capture d'écran

Pour réaliser ces mesures, les chercheurs ont créé une liste de 570 sites, quasi exclusivement anglophones, en combinant plusieurs listes préexistantes établies par des médias spécialistes du *« fact-checking »* (« la vérification de faits ») ou par des universitaires pour de précédentes études. Ils n'ont conservé que des sites apparaissant dans plusieurs de ces listes. Certains sites appartiennent à des médias (comme celui du tabloïd britannique *Daily Express* ou un site appartenant au *Times of India*), d'autres ne contiennent que des articles purement mensongers sans but précis et beaucoup le font à des fins politiques, principalement pour la droite dure américaine. Les données de partage (sur Twitter) et d'engagement (sur Facebook) sont quant à elles issues d'une entreprise commerciale spécialisée dans la mesure d'audience sur les réseaux sociaux.

Les chercheurs ont aussi créé plusieurs listes de sites dits *« de contrôle »*, notamment des grands et petits sites d'actualité. La tendance est totalement différente des sites mensongers : les interactions sur Facebook et les partages sur Twitter des articles issus de ces sites continuent d'augmenter même après la fin de 2016. Cela a permis aux chercheurs de prendre en compte le changement d'algorithme annoncé en début d'année par Facebook visant à réduire la part des contenus issus des médias par rapport à ceux postés par les proches dans le fil d'actualité des visiteurs.

Les efforts de Facebook commenceraient à payer

La rupture claire détectée par les chercheurs, à la fin de 2016, survient peu après l'élection américaine de novembre et correspond au moment où Facebook, sous pression, a commencé à prendre des mesures pour combattre la désinformation en ligne. Le réseau social a, entre autres, commencé à travailler avec des médias spécialistes de la vérification des faits, a mis en place une signalétique pour certains médias problématiques, a diminué la diffusion des articles mensongers lorsqu'ils sont partagés par les utilisateurs et a asséché le financement par la publicité de certains sites propageant des informations mensongères.

« L'ampleur du problème de la désinformation a semble-t-il décliné, du moins temporairement, et les efforts fournis par Facebook après l'élection de 2016 pour limiter la diffusion de la désinformation pourraient avoir eu un impact important », écrivent les chercheurs.

Des chercheurs très prudents

« Nos preuves comportent de nombreuses limites importantes, et doivent être interprétées avec précaution » préviennent toutefois d'emblée les chercheurs.

D'abord, expliquent-ils, la durée de vie des sites produisant de fausses informations est très courte, aussi n'excluent-ils pas ne pas avoir pris en compte certains sites, notamment de petite taille, apparus récemment. Le moindre succès des informations mensongères sur Facebook se vérifie cependant lorsque les chercheurs se concentrent sur des sites créés après l'élection de 2016.

Ensuite, les chercheurs estiment qu'il est possible que la présence des élections ait produit un biais dans leurs résultats : les contenus politiques clivants ont plus de succès pendant cette période. Mais, notent-ils, le fait que leur diffusion augmente sur Twitter après les élections tend à nuancer ce constat.

Enfin, certains sites mensongers sont issus de listes créées par des médias partenaires de Facebook dans la lutte contre la désinformation. Aussi, notent les chercheurs, s'agit-il de sites dont Facebook connaît le caractère mensonger ou trompeur, et donc plus susceptible d'en limiter la portée.

Les chercheurs ne veulent surtout pas que leurs travaux sonnent la fin de la lutte contre la désinformation. *« Il est important de souligner que la quantité absolue de fausses informations sur les deux plates-formes demeure importante et que Facebook joue encore un rôle important dans leur diffusion »,* écrivent-ils.

Eli Pariser : « Il est vital de résoudre les problèmes de l'information en ligne »

Par Damien Leloup

MÉGA-PIXELS

Publié le 12 septembre 2018 à 09h52 - Mis à jour le 12 septembre 2018 à 10h07

Le militant et entrepreneur américain, théoricien du concept de « bulles de filtres », travaille pour Reporters sans frontières sur l'information et la démocratie. Il explique au « Monde » les enjeux qu'il souhaite y aborder.

Eli Pariser est le directeur général du média en ligne Upworthy, et président du conseil de l'association progressiste MoveOn. Ce militant et entrepreneur américain est aussi le théoricien du concept de « bulles de filtres », détaillé dans un livre publié en 2011, selon lequel les réseaux sociaux nous enferment dans des « bulles » de pensée en nous présentant en permanence des idées avec lesquelles nous sommes déjà d'accord.

A l'occasion de son passage à Paris, dans le cadre du lancement par Reporters sans frontières (RSF) d'une commission – dont il est membre – pour définir un pacte international pour l'information et la démocratie, Eli Pariser explique au *Monde* les enjeux qu'il souhaite y aborder : le rôle des réseaux sociaux dans la diffusion de l'information.

Pourquoi avez-vous rejoint ce projet lancé par RSF ?

Eli Pariser : Parce que c'est important. Cela fait un moment que je réfléchis à la question fondamentale : comment pouvons-nous réparer les grands principes qui sous-tendent l'information ? Ce pacte est une excellente opportunité de le faire. Il y a beaucoup de concepts et de mots que l'on utilise couramment, et qui ont des sens très différents en fonction de qui les utilise.

Vous faites allusion à l'expression « fake news », souvent galvaudée ?

Oui, il y a cette expression. Mais aussi des questions beaucoup plus fondamentales, comme ce que veut dire *« être bien informé »*. Il y a des formats, des manières de s'exprimer, qui aident ou, au contraire, gênent la construction d'une sphère de débat public. Par exemple, je pense qu'il faut porter une grande attention à ce que fait Facebook. Que ça soit bien ou mal, ils sont confrontés à beaucoup de questions importantes : comment définit-on le fait d'être informé ?

Comment définit-on la confiance ? La pertinence ? Les réponses de Facebook définissent la manière dont s'informent des milliards de personnes.

Aux Etats-Unis, Facebook cherche à savoir ce que vous savez déjà, et quels types de contenus amélioreront vos connaissances. Cela part d'une bonne intention. Mais je ne pense pas que la connaissance des faits suffise pour être bien informé. La recherche l'a démontré. Cela ne veut pas dire que les faits ne sont pas importants, mais qu'il y a d'autres facteurs tout aussi importants pour la bonne information de citoyens actifs et réfléchis.

Vous écriviez en 2011 que nous étions « sur le point de développer l'équivalent psychologique de l'obésité » dans notre rapport à l'information en ligne. Sommes-nous devenus « infobèses » ?

Ce qui est fascinant, pour filer la métaphore, c'est que, pendant très longtemps, les restaurants de fast-food se sont développés à une vitesse incroyable. Mais à un moment, les consommateurs ont compris que manger des hamburgers tous les jours créait des problèmes de santé, et ils ont cherché d'autres options. Nous voyons aujourd'hui toute une gamme de fast-foods qui proposent de la nourriture plus saine, ou issue de l'agriculture raisonnée.

En termes d'information, nous avons atteint ce point de bascule. Il y a aujourd'hui suffisamment de personnes qui s'interrogent sur leur propre utilisation des réseaux sociaux pour inciter à l'invention d'alternatives.

L'élection présidentielle américaine de 2016 a-t-elle eu un rôle dans ce processus ?

Ce n'est pas l'unique raison. Un exemple personnel : j'ai deux enfants, nés en 2014 et 2017. Entre les deux naissances, ma relation avec mon smartphone a changé. Cette technologie trouve des manières très subtiles de nous attirer, et je pense que je ne suis pas le seul à m'être demandé récemment pourquoi je regardais Twitter alors que j'avais un bébé avec moi ! Ces deux phénomènes se sont combinés : l'élection de Trump a été un électrochoc pour beaucoup, mais il y a aussi eu le sentiment grandissant que nous n'utilisions pas notre temps de la meilleure manière.

C'est aussi une tendance dans les rédactions, avec une part grandissante de journalistes qui abandonnent ou limitent leur usage des réseaux sociaux, principalement Twitter. Est-ce un indicateur d'une tendance générale ?

Je ne pense pas que cela soit vrai. Le comportement des journalistes et des personnes qui sont plongées dans le bain de l'actualité est extrêmement différent de celui des personnes qui en sont les plus éloignées. Twitter est par bien des aspects un phénomène des élites surdiplômées.

Mais les réseaux sociaux restent encore un outil important pour s'informer. Si Facebook cessait subitement de diffuser des informations, cela ne serait pas une bonne chose. Cela couperait complètement une partie de la population de l'information, des personnes qui ne sont pas habituellement en recherche d'actualités.

Les patrons de presse eux aussi sont de plus en plus méfiants vis-à-vis des réseaux sociaux…

Il y a eu une forme de surcorrection. Au début, les patrons de presse n'y prêtaient aucune attention, puis soudainement ils s'y sont beaucoup intéressés. Mais je suis aussi très méfiant vis-à-vis des idées « à la mode » dans les rédactions. Par exemple, en ce moment, il y a tout cet enthousiasme pour les modèles sur abonnement. Il est parfaitement compréhensible : par bien des aspects, il vaut mieux dépendre de vos lecteurs que d'annonceurs ou de réseaux sociaux. Mais ce n'est pas une solution parfaite, du point de vue du rôle démocratique des médias. Les lecteurs qui sont prêts à payer ne sont qu'une toute petite partie de la population. Tous les modèles économiques ont leurs biais.

Facebook, qui a longtemps affirmé que les « bulles de filtres » n'étaient pas une réalité tangible, réfléchit désormais à la manière de présenter plusieurs points de vue sur un même sujet.

Aujourd'hui, depuis Mark Zuckerberg jusqu'aux employés du bas de l'échelle, tout Facebook se pose sérieusement la question de savoir quelles sont les dynamiques sociales à l'œuvre sur sa plate-forme, et quelle y est la sociologie de l'information.

Eli Pariser. Knight Foundation CC by-sa 2.0 via Wikimedia Commons

Dans le détail, le simple fait de présenter une variété de points de vue peut avoir des conséquences négatives. Nous en avons tous fait l'expérience : si vous lisez un média qui est à l'opposé complet de vos convictions, tout ce que vous en retirez est une déduction que le camp d'en face est composé d'abrutis. Les médias très partisans, comme Fox News aux Etats-Unis, prennent depuis longtemps une apparence d'équité tout en présentant des opinions qui renforcent vos idées préconçues : ils présentent une version caricaturale de la position adverse, avant de la démonter. C'est très divertissant, mais cela n'incite aucunement à la réflexion.

Nous n'en sommes qu'au début de notre compréhension de ces phénomènes. Je pense qu'on peut mettre les gens dans un environnement qui favorise une réelle conversation. Savoir comment on crée ces espaces est l'une des grandes questions pour l'avenir. Restera à savoir si un modèle économique qui repose sur la publicité, et donc une forme de manipulation, est compatible avec ces aspirations.

Que pensez-vous de la solution évoquée par Jack Dorsey, le PDG de Twitter, qui a parlé d'un projet pour afficher des messages de personnes que vous ne suivez pas, et avec qui vous n'êtes pas d'accord ?

Cela peut être bon ou mauvais, tout dépend de la manière dont c'est mis en place. Si vous m'affichez une liste d'articles provenant de sources que vous ne lisez jamais, mais partagées par des personnes à qui vous faites confiance, c'est un service extrêmement utile. Si vous vous contentez de m'agresser avec des messages que je trouve révoltants, j'ai plus de doutes sur la démarche.

L'autre discours que l'on entend beaucoup dans la bouche des créateurs de réseaux sociaux, c'est « faites-nous confiance »…

Peut-on leur faire confiance ? La réponse courte est non. Pas parce qu'ils ne sont pas sincères ou volontaristes, mais parce que c'est presque impossible de construire une structure sociale qui marche pour des milliards d'utilisateurs dans tous les pays du monde. Ce n'est pas une tâche qu'une poignée de personnes est capable d'accomplir. Il n'y a pas « un algorithme pour les diriger tous » qui fonctionne pour 192 pays, sans écraser tout ce qui fait la richesse et l'individualité des pays.

La polarisation de la société n'est, cependant, pas uniquement causée par les réseaux sociaux.

Non. Il y a un réseau d'interactions très complexes entre les citoyens, les médias et les plates-formes, qui n'est pas le même aux Etats-Unis qu'en Europe, où il y a beaucoup de bons médias publics et des dynamiques politiques différentes. Aux Etats-Unis, la polarisation est aussi géographique, et c'est le cas depuis cinquante ans.

Par ailleurs, les médias sont tout à fait capables de polariser le débat sans l'aide des réseaux sociaux. Lorsque vous passez beaucoup de temps sur Internet, il est facile de croire que tout l'écosystème politique et médiatique est dominé par ce qui se passe en ligne. Mais nous n'en sommes pas là. La plupart des gens s'informent à la télévision. C'est un média en déclin, mais qui est toujours extrêmement puissant. Il faudra encore dix ans environ avant que ce qui se passe en ligne soit vraiment le moteur de la politique et des médias.

Il y a beaucoup de gens qui pensent que Trump a utilisé les réseaux sociaux pour influencer le vote des citoyens, et que c'est comme ça qu'il a gagné. Je n'y crois pas du tout. Trump et l'extrême droite se sont servis des réseaux sociaux pour peser, de manière très forte, sur les sujets abordés par les grands médias, ce qui a eu une influence sur le vote. Ce qui devrait concentrer notre attention, c'est ce double jeu qui permet à des théories conspirationnistes de passer dans l'espace public médiatique.

Vous semblez, malgré tout, optimiste sur l'avenir de l'information en ligne ?

Comme le disait Gramsci, j'ai le pessimisme de la raison et l'optimisme de la volonté. Je ne sais pas comment nous allons résoudre tous ces problèmes, mais je sais qu'il est vital d'essayer. Nous parlons de phénomènes qui sont encore très jeunes – tant de choses ont changé en dix ans. Je ne pense pas que les plates-formes peuvent tout résoudre seules. Mais on voit de plus en plus de chercheurs, d'ingénieurs et de journalistes qui y travaillent ensemble.

Damien Leloup

La propagande numérique de la Russie « a coûté moins cher qu'un avion F-35 »

Dans un entretien au « Monde », le sénateur américain Mark Warner explique son combat contre les campagnes d'influence de puissances étrangères .

Propos recueillis par Martin Untersinger Publié le 18 octobre 2018 à 10h48 - Mis à jour le 18 octobre 2018 à 12h49

Mark Warner, à gauche, avec le président du comité du renseignement du Sénat, le républicain Richard Burr, le 25 juillet. NICHOLAS KAMM / AFP

Le **sénateur de Virginie Mark Warner,** vice-président du groupe démocrate au Sénat américain, siège au comité du Sénat sur le renseignement, qui mène l'enquête sur les opérations d'ingérence russe dans l'élection américaine de 2016.

Il s'est fait remarquer par ses appels réguliers à un meilleur encadrement des publicités politiques en ligne et ses interventions très critiques de la manière dont Facebook, Twitter et Google ont géré les opérations de propagande. *Le Monde* l'a interviewé.

Martin Untersinger : Comment expliquez-vous que les grands réseaux sociaux n'aient pas vu venir la campagne d'influence, menée par l'organisation russe Internet Research Agency (IRA), et ses milliers de publications de contenus de propagande ? Ses activités étaient pourtant connues et documentées depuis environ 2013.

Mark Warner : Je pense que les activités de l'IRA étaient connues, mais qu'aux Etats-Unis les entreprises ne l'ont pas vue venir. Elles n'étaient pas organisées pour le faire. Mais le gouvernement américain non plus n'en était pas conscient et a été pris par surprise. Les réseaux sociaux ont rapidement appris de leurs erreurs car, au moment de l'élection présidentielle de 2017, elles ont dit travailler activement avec le gouvernement français.

Les réseaux sociaux ont changé de posture depuis 2016, après avoir initialement nié l'impact des campagnes de désinformation. Ont-ils fait assez pour protéger les élections de mi-mandat ?

Ils se sont améliorés. Aux Etats-Unis, j'essaie de faire voter une loi qui obligerait à plus de transparence sur les publicités politiques en ligne, qui leur impose les mêmes règles que nous avons pour la télévision et la radio. Je n'ai pas encore pu défendre le texte, mais Facebook a pris les devants dans ce domaine, et c'est une bonne chose. Ils arrivent bien à identifier les faux comptes et disent en supprimer des milliers régulièrement.

Même chose du côté de Twitter. Google, pendant un peu plus d'un an et demi [après l'élection de 2016], a été plutôt mauvais. La plupart des experts disent que Youtube est utilisé pour radicaliser les gens : Google doit mettre en place les mêmes protocoles que les autres entreprises.

Dans quel domaine souhaitez-vous que les réseaux sociaux fassent plus d'efforts ?

On devrait avoir le droit de savoir, sur les réseaux sociaux, quand on interagit avec un robot ou un humain, par exemple. Et puis il y a le problème de la localisation : si vous dites que vous postez de Paris mais qu'en fait vous êtes connecté à Saint-Pétersbourg, il pourrait y avoir une fenêtre qui vous dit que ce message ne provient pas de là où la personne prétend poster.

Est-ce que les Etats-Unis ont repéré, durant la campagne actuelle pour les élections de mi-mandat, une activité de propagande étrangère semblable à celle de 2016 ?

Il y a encore de l'activité. Cela n'est pas forcément pour appeler directement à voter pour le candidat X ou le candidat Y, mais ils essaient encore de diviser les Américains sur les questions sociales, de race… parce que ça marche, et cela ne coûte pas cher : si vous additionnez tout ce qu'ils ont dépensé pour interférer dans l'élection américaine et en Europe, cela coûte moins qu'un avion de combat F-35. C'est un sujet dont l'Occident doit prendre conscience.

Est-ce que le gouvernement américain travaille suffisamment avec les réseaux sociaux pour limiter l'interférence étrangère ?

Le gouvernement américain, en 2018, s'est concentré sur l'infrastructure du vote : les machines à voter, les listes électorales… C'est là qu'il y a eu plus d'efforts. Nous nous améliorons, mais nous ne sommes pas encore au niveau. Les Etats-unis et l'Occident ont considéré les campagnes de désinformation et les attaques informatiques comme deux champs distincts.

Les pays comme la Chine et la Russie voient cela comme un seul. Par exemple, si la Russie était à l'origine du piratage d'Equifax, ils auraient pu utiliser cette information pour faire des e-mails d'hameçonnage, ou pour cibler un post sur Facebook… Cette combinaison de désinformation et de cyberattaques est très puissante, et je ne pense pas que le gouvernement américain soit assez préparé.

Le fait que le président Donald Trump ne veuille pas entendre parler d'une « menace russe » limite-t-il la capacité des Etats-Unis à faire face au problème ?

Oui, absolument. Tout le monde dans les services de renseignement réalise que la Russie est une énorme menace. Mais le président refuse encore d'accepter cette vérité. Dans une Maison Blanche normale, face à une menace comme celle-là, il y aurait un responsable spécialement désigné. Mais il n'y a pas de leadership à la Maison Blanche, chaque agence doit travailler dans son coin.

J'ai assisté à une réunion en juillet avec des représentants de nombreux pays, des Suédois, des Canadiens, des Ukrainiens... Le jour où nous étions rassemblés pour s'attaquer à cette nouvelle menace, c'était le jour de la piètre performance de Donald Trump face à Vladimir Poutine : nous nous sommes interrompus pour voir Trump s'incliner devant le président russe et nier le problème. Il devrait y avoir un leadership américain fort, mais pour l'instant, il n'existe pas.

Pensez-vous que l'élection présidentielle de 2020 sera protégée contre le type d'ingérence qui a eu lieu en 2016 ?

Non. Nous verrons lors des élections de mi-mandat : nous ne connaissons pas encore le nombre de faux comptes qui seront actifs. Cela peut encore se produire.

Martin Untersinger

Les Occidentaux se coordonnent pour accuser la Russie de cyberattaques

Par Michaël Szadkowski et Martin Untersinger
FACTUEL
Publié le 04 octobre 2018 à 19h15 - Mis à jour le 09 octobre 2018 à 12h05
Chose inédite, les Etats-Unis, le Royaume-Uni, les Pays-Bas et le Canada ont accusé la Russie d'être responsable de cyberattaques majeures.

Dans un mouvement d'une ampleur inédite, plusieurs pays occidentaux – parmi lesquels les Etats-Unis, le Royaume-Uni, les Pays-Bas et le Canada – ont accusé, jeudi 4 octobre, la Russie d'être responsable de cyberattaques majeures survenues ces dernières années.

Les annonces concertées ont eu lieu alors que les ministres de la défense des pays de l'OTAN sont réunis à Bruxelles pour un sommet, où la question des attaques informatiques russes était au menu. Les Etats-Unis ont officialisé, à cette occasion, la mise à disposition de ses capacités en matière de cyberdéfense, qui pourront être directement utilisées par l'OTAN.

La Russie doit *« cesser son comportement irresponsable »*, a averti, en marge de ce sommet, le secrétaire général de l'OTAN, Jens Stoltenberg. Moscou doit mettre un terme à *« l'usage de la force contre ses voisins,*[aux] *tentatives d'immixtion dans des processus électoraux et* [aux]*campagnes massives de désinformation »*, a martelé le chef de l'Alliance atlantique.

Le GRU, le service de renseignement militaire russe et bras armé du Kremlin sur Internet, est au centre de cette cascade d'attributions d'attaques informatiques. Il a été récemment accusé par les autorités américaines d'être impliqué, peu avant l'élection américaine de 2016, dans le piratage du Parti démocrate, préambule à une plus vaste opération d'ingérence numérique de la Russie.

. Pays-Bas : l'OIAC espionnée par des Russes à La Haye

Les autorités néerlandaises ont annoncé avoir déjoué, en avril, une cyberattaque contre l'Organisation pour l'interdiction des armes chimiques (OIAC), basée à La Haye. Cette organisation, impliquée dans les enquêtes sur l'empoisonnement de Sergueï Skripal et les attaques chimiques en Syrie, s'est attiré à de nombreuses reprises les foudres du Kremlin.



Les deux agents du GRU impliqués dans la tentative d'assassinat en Angleterre. À gauche le colonel Anatoly Chépiga, « héros de Russi »alias Ruslan Bochirov, à droite l'agent Alexandre Petrov

Quatre agents russes, expulsés depuis par les Pays-Bas, avaient positionné un véhicule truffé d'équipements électroniques sur le parking d'un hôtel proche du siège de l'OIAC, afin d'accéder à son réseau informatique interne.

« Le gouvernement néerlandais juge extrêmement inquiétante l'implication de ces agents de renseignement », a déclaré la ministre néerlandaise de la défense. L'Union européenne a dénoncé, après ces révélations, un *« acte agressif »* de la part du renseignement militaire russe. *« Ces actions portent atteinte au droit et aux institutions internationales »*, ont écrit, dans un communiqué, le président du Conseil européen, Donald Tusk, celui de la Commission, Jean-Claude Juncker, et la chef de la diplomatie européenne, Federica Mogherini.

Moscou a eu recours a son habituelle ironie, fustigeant *« l'ampleur »* de*« l'espionnite aiguë des Occidentaux »*, selon les termes du ministère russe des affaires étrangères.

. Le Royaume-Uni dénonce des actions « sans foi ni loi »

C'est le Royaume-Uni qui a ouvert le bal des dénonciations visant la Russie, jeudi. Le ministère britannique des affaires étrangères, Jeremy Hunt a dénoncé les actions *« sans foi ni loi »* du GRU, qui ont *« affecté des citoyens dans de nombreux pays et coûté des millions de livres »*. Les autorités britanniques évoquent ainsi à la fois l'attaque contre le Parti démocrate américain en 2016, mais aussi l'offensive contre l'Agence mondiale antidopage ou bien le virus informatique BadRabbit, qui avait touché l'Ukraine en 2017.

L'agence britannique chargée de la défense informatique a, par ailleurs, relié d'un trait plusieurs groupes que les experts en sécurité informatique rattachent depuis des années à la Russie. Pour les autorités britanniques, les groupes Fancy Bear, Sandworm, APT28 ou CyberCaliphate sont des alias derrière lesquels se cache le GRU.

. Etats-Unis : sept agents russes inculpés

La justice américaine a, elle, inculpé sept agents du GRU. Ils sont poursuivis pour avoir piraté des instances sportives internationales, parmi lesquelles l'Agence mondiale antidopage (AMA), le Comité international olympique (CIA) ou encore la FIFA. Les autorités les accusent aussi de blanchiment d'argent, de fraude bancaire et d'usurpation d'identité.

Parmi les Russes inculpés figurent les quatre agents expulsés par les Pays-Bas. Les trois autres font partie des douze responsables inculpés en juillet pour le piratage du Parti démocrate.

. Canada : l'Agence mondiale antidopage visée

Le Canada y est aussi allé de sa dénonciation. Selon les autorités d'Ottawa, le renseignement militaire russe se trouve *« fort probablement »* derrière l'attaque de l'Agence mondiale antidopage (AMA), basée à Montréal.

En 2016, des documents internes à l'AMA contenant des informations sur les traitements médicaux de nombreux athlètes avaient été publiés sur le Web. *« Le groupe avait obtenu illégalement ces renseignements en piratant le système d'administration et de gestion de l'AMA »,* précise le gouvernement canadien.

La même année, le Centre canadien pour l'éthique dans le sport, responsable de la lutte antidopage dans le pays, *« a été compromis par un logiciel malveillant »,* poursuit le ministère, pour qui la responsabilité du GRU dans ce piratage est également engagée.

. Des tensions croissantes avec la Russie, la France prudente

Cette volée d'accusations concertées confirme la stratégie agressive adoptée depuis plusieurs mois par Londres, Washington et leurs plus proches alliés sur la question des attaques informatiques russes.

L'attribution d'attaque informatique est très délicate sur le plan technique. La posture de ces pays occidentaux est davantage politique, dans l'espoir de décourager la Russie de mener des attaques informatiques.

La France n'a pas, à ce stade, rejoint le concert des accusations et, quitte à donner l'impression d'être isolée, campe sur sa stratégie : celle de ne pas formuler d'accusations publiques concernant les cyberattaques qui la visent et de gérer plus discrètement les différents qui l'opposent, en particulier, à la Russie. *« Nous ne sommes pas plus naïfs que les autres, mais la France n'a rien à gagner à se mettre à la remorque des autres pays »,* estimait, jeudi dans l'après-midi, une source gouvernementale française.

Michaël Szadkowski
Martin Untersinger

yberattaques d'instances sportives : les Etats-Unis inculpent des agents russes

Sept personnes sont poursuivies par le ministère de la justice américain pour avoir piraté, entre décembre 2014 et mai 2018, l'Agence mondiale antidopage, le Comité olympique international ou le Tribunal arbitral du sport.

Le Monde avec AFP Publié le 04 octobre 2018 à 18h55 - Mis à jour le 04 octobre 2018 à 19h28

La justice américaine a annoncé, jeudi 4 octobre, l'inculpation de sept agents supposés du renseignement militaire russe (GRU) dans le cadre d'une campagne mondiale de cyberattaques attribuée au Kremlin et dénoncée par plusieurs pays occidentaux.

Selon l'acte d'accusation, ces sept personnes sont poursuivies par les Etats-Unis pour des faits commis entre décembre 2014 et mai 2018 et qui visaient, pour une bonne partie, des instances sportives internationales.

Poursuivis pour blanchiment d'argent, fraude bancaire, fraude informatique et usurpation d'identité, les sept agents supposés du GRU sont accusés d'avoir piraté l'Agence mondiale antidopage (AMA), le Comité olympique international (CIO), les Fédérations internationales de football (FIFA) et d'athlétisme (IAAF) et le Tribunal arbitral du sport (TAS), ainsi que plus d'une trentaine d'instances nationales, dont les agences antidopage canadienne et américaine.

Les opérations *« concernaient des accès sophistiqués, continuels et non autorisés aux réseaux informatiques des victimes en vue de voler des informations d'ordre privé ou sensible »*, a expliqué John Demers, ministre adjoint de la justice pour la sécurité nationale.

Documents de l'AMA « modifiés » pour « soutenir les thèses du gouvernement russe »

Des codes d'accès de membres de différentes organisations sportives auraient ainsi été volés pour se procurer des documents concernant la lutte antidopage, des dossiers médicaux ou des informations sur les procédures antidopage.

Ces informations sensibles ont été communiquées au célèbre groupe de pirates informatiques Fancy Bear, considéré comme étant contrôlé par les services de renseignement russes. Les hackeurs ont ensuite diffusé ces documents à des journalistes dans le cadre d'une campagne de désinformation.

L'AMA avait suspendu en 2015 l'Agence russe antidopage (Rusada) en raison de son rôle moteur dans le système de dopage d'Etat qui régissait le sport russe entre 2011 et 2015. Certains documents de l'AMA fournis à la presse *« ont été modifiés »* pour *« soutenir les thèses du gouvernement russe »*, précise l'acte d'accusation.

Trois des sept Russes poursuivis font partie des douze responsables inculpés en juillet d'ingérence dans la présidentielle américaine de 2016 par le procureur spécial Robert Mueller. Les deux dossiers sont différents, mais ils se chevauchent, a souligné John Demers.

L'annonce américaine survient alors que les Pays-Bas, l'Australie, la Grande-Bretagne, l'OTAN et l'Union européenne accusent également Moscou de cyberattaques. Le gouvernement canadien a pour sa part annoncé , jeudi, que l'AMA, établie à Montréal, avait fait l'objet d'une cyberattaque, dont le GRU était *« fort probablement responsable »*.

La Grande-Bretagne accuse la Russie de cyberattaques « sans foi ni loi »

Ces opérations, menées par les services de renseignement militaire russes (GRU), auraient « affecté des citoyens dans de nombreux pays ».

Le Monde avec AFP Publié le 04 octobre 2018 à 02h14 - Mis à jour le 04 octobre 2018 à 12h07

Le ministre des affaires étrangères britannique, Jeremy Hunt, a accusé jeudi 4 octobre les services de renseignement militaire russes (GRU) d'avoir mené des cyberattaques contre des institutions politiques et sportives, des entreprises et des médias à travers le monde.

« Ce type de comportement démontre leur désir d'opérer sans tenir compte du droit international ou des normes établies, et d'agir avec un sentiment d'impunité et sans considérer les conséquences », a-t-il déclaré dans un communiqué. *« Avec nos alliés, nous révélerons et répondrons aux tentatives du GRU de saper la stabilité internationale. »* Ces opérations, menées *« au hasard et sans foi ni loi »*, ont*« affecté des citoyens dans de nombreux pays, dont la Russie, et coûté des millions de livres aux économies nationales »*, a-t-il poursuivi.

Attaque du Parti démocrate

Parmi les attaques identifiées par le Centre national de cybersécurité (NCSC, pour*National Cyber Security Centre*, en anglais) figure notamment celle du Parti démocrate aux Etats-Unis, prélude au scandale de l'ingérence russe dans l'élection présidentielle de 2016, et pour laquelle le GRU avait déjà été accusé par Washington. Sont également mises en avant des fuites de documents confidentiels consécutives au piratage de la base de données de l'Agence mondiale antidopage (AMA) ou encore l'attaque informatique contre l'aéroport d'Odessa en Ukraine.

Les autorités britanniques en profitent aussi pour associer le GRU à plusieurs groupes de pirates connus (Fancy Bear, Sandworm, Strontium, APT 28, CyberCaliphate…), imitant en cela les nombreuses entreprises spécialisées ayant étudié leurs activités depuis plusieurs années.

Entre les Etats-Unis et la Russie, des relents de guerre froide dans le cyberespace

Par Martin Untersinger
MÉGA-PIXELS
Publié le 14 octobre 2016 à 13h03 - Mis à jour le 03 juillet 2017 à 15h02
L'administration Obama vient d'incriminer officiellement la Russie dans la cyberattaque qui avait ciblé, en juin, le Parti démocrate. Une accusation qui a encore envenimé les relations russo-américaines.

La Russie tente *« d'interférer avec le processus électoral américain »*. Vendredi 7 octobre, après maintes tergiversations, l'administration Obama a officiellement confirmé, par la voix de son directeur du renseignement national (DNI) et de celle du département de la sécurité intérieure (DHS), l'implication de Moscou dans l'attaque informatique visant le Parti démocrate.

Cette accusation, au parfum de guerre froide et à un mois de l'élection présidentielle américaine, marque un tournant. Depuis des semaines, la Russie est suspectée d'orchestrer une série de piratages visant les Etats-Unis. Mais c'est la première fois que le gouvernement de Barack Obama incrimine directement Moscou dans *« la récente compromission de courriels de citoyens et d'institutions américains, y compris d'organisations politiques »*. Dans leur communiqué, le DNI et le DHS estiment que *« seuls les plus hauts responsables russes ont pu autoriser ces actions »*, sans pour autant en apporter la preuve. Le Kremlin a qualifié cette allégation de *« foutaise »*.

Deux groupes pirates déjà soupçonnés

Mi-juin, le Comité national démocrate (DNC), l'organe du parti chargé d'organiser les élections pour l'investiture, avait prévenu que deux groupes de pirates avaient pénétré son réseau. Un mois plus tard, WikiLeaks publiait sur son

site plusieurs milliers de courriels internes au parti, révélant que les caciques démocrates avaient pris fait et cause pour Hillary Clinton au détriment de son challenger Bernie Sanders.

Plusieurs incidents ont ensuite contribué à nourrir le climat de défiance vis-à-vis de Moscou. L'entreprise de sécurité informatique chargée de nettoyer les systèmes informatiques du DNC a indiqué que les pirates étaient liés aux services de renseignement russes. Le premier groupe, surnommé Cozy Bear (APT29), n'est pas un inconnu : il avait déjà été accusé au printemps 2015 d'avoir pénétré les réseaux de la Maison Blanche et du département d'Etat. Le second, appelé Fancy Bear (APT28), s'est lui aussi forgé une réputation : soupçonné depuis longtemps d'être lié au renseignement militaire russe, c'est vers lui que se dirigeait l'enquête sur le piratage, les 8 et 9 avril 2015, de la chaîne TV5Monde, selon une source judiciaire interrogée à l'époque par *Le Monde*. En juin de la même année, les services de renseignement allemands accusaient ce même groupe d'avoir espionné le Bundestag.

Plusieurs Etats américains ont également été victimes de piratages ou de tentatives d'intrusion visant leurs systèmes électoraux, en provenance, semble-t-il, de Russie. En juin 2016, le Federal Bureau of Investigation (FBI) avertissait l'Arizona d'une intrusion mineure visant sa base de données électorale. A l'approche des élections, la même police fédérale enjoignait l'ensemble des Etats à muscler leurs mesures de sécurité informatique, redoutant d'autres agressions. L'administration Obama est cependant moins affirmative quant à leurs commanditaires. *« Dans la plupart des cas,* [ces attaques] *provenaient de serveurs gérés par une entreprise russe. Nous ne sommes cependant pas en mesure d'attribuer cette activité au gouvernement »,* écrivent ainsi le DHS et le DNI dans leur communiqué.

« Les pirates de Fancy Bear ont comme cible numéro un l'Ukraine, puis les forces armées de l'Est et les pays de l'OTAN »

Autre signe, plus indirect, de l'atmosphère irrespirable qui règne entre Moscou et Washington dans le cyberespace, la publication sur le Web, mi-août, d'outils sophistiqués d'espionnage numérique appartenant à l'Agence nationale de la sécurité américaine (NSA), considérée comme la plus puissante du monde en la matière. Que des pirates se soient procuré une partie de son arsenal et décident d'en publier son contenu a surpris la plupart des observateurs. S'agissait-il d'une fuite émanant d'une agence rivale russe, désireuse de lancer un avertissement ? Les regards se sont tous tournés vers l'est, au moment où se précisaient les accusations d'une implication russe dans le piratage du Comité national démocrate.

La Russie est l'un des pays les plus actifs et les plus compétents en matière d'espionnage informatique. Le conflit en Ukraine a été l'occasion de constater son savoir-faire. De nombreuses attaques – de la fuite de courriels jusqu'à la saturation de sites Web, et même une brève extinction d'une partie du réseau électrique ukrainien – avaient alors été attribuées à des pirates russes par plusieurs laboratoires de cybersécurité. La Russie est aussi classée par les autorités américaines, aux côtés de la Corée du Nord, de la Chine et de l'Iran, parmi les principaux adversaires des Etats-Unis dans le cyberespace.

Ces dernières années, au moins une demi-douzaine de groupes d'espionnage informatique, aux origines russes plus ou moins établies, ont été découverts par des experts basés en Allemagne, en Finlande, au Japon et aux Etats-Unis. Parmi les plus performants d'entre eux figurent ceux qui ont été identifiés dans les serveurs du Parti démocrate, notamment Fancy Bear. Ce dernier a été découvert à l'été 2014 par Feike Hacquebord, expert en sécurité informatique au sein de l'entreprise spécialisée Trend Micro, basée au Japon. M. Hacquebord assure aujourd'hui ne détenir *« aucune preuve »* de liens connectant Fancy Bear avec le Kremlin, précisant qu'il n'est pas *« sage »* de les voir nécessairement aux ordres de Moscou.

Mais leurs caractéristiques restent troublantes. Le groupe dispose, selon l'expert, *« de très grandes ressources d'argent et de main-d'œuvre »*, dont l'activité diminue *« pendant les vacances et pendant l'été »,* signe qu'il s'agirait d'un groupe étatique. Les pirates de Fancy Bear, parmi les plus compétents observés, visent avec une intensité particulière *« l'Ukraine, quasiment leur cible numéro un, les forces armées d'Europe de l'Est et les pays de l'OTAN »*. Si des Russes figurent aussi parmi leurs victimes, ce sont pour l'essentiel des *« activistes et opposants au régime »*.

Donna Brazille, présidente du Comité national démocrate américain, à l'université de Longwood à Farmville, en Virginie, le 4 octobre. JOE RAEDLE/REUTERS

Quel intérêt aurait le Kremlin à s'attaquer au système électoral américain ? Pour la Russie, *« les cyberattaques sont des outils intégrés dans un effort plus large de maintien de sa domination politique et militaire sur un théâtre donné et, plus largement, sur les opinions publiques mondiales »,*écrivait la chercheuse Jen Weedon dans un rapport de 2015 du Cooperative Cyber Defence Centre of Excellence (CCDCOE), un organisme de recherche consacré à la cyberdéfense patronné par l'OTAN.

« Instiller la confusion »

« Les cyberattaques font partie d'une campagne pour instiller le doute et la confusion aux populations occidentales envers leurs institutions, embarrasser leurs gouvernements, affaiblir l'OTAN, les Etats-Unis et tout ce qui peut être un obstacle à la Russie », estime de son côté Matthijs Veenendaal, également chercheur au CCDCOE. *« Il ne s'agit pas tant de déterminer l'issue des élections américaines que d'entretenir le relativisme des Américains sur leur propre pays, de propager l'image d'élites corrompues, de nourrir la remise en cause des institutions »,* précise Julien Nocetti, chercheur à l'Institut français des relations internationales (IFRI). Donald Trump, poursuit-il, *« est le candidat idéal pour alimenter cette dialectique et attiser le sentiment que la démocratie n'est pas idéale ».*

Les cyberattaques, discrètes et dont l'origine est difficile à déterminer, constituent les outils parfaits pour ce type de campagne de déstabilisation. Dans sa conception du cyberespace et de la sécurité informatique, Moscou attribue autant d'importance aux contenus (informations, opinions) circulant sur le Web qu'au fonctionnement technique des infrastructures d'Internet. Ainsi, ses attaques informatiques comportent volontiers ces deux dimensions : provoquer la fermeture de sites et faire « fuiter » des informations. *« Si les Américains se concentrent sur la sécurité des réseaux et des infrastructures, les Russes, eux, mettent l'accent sur le contenu »,* explique le chercheur Julien Nocetti. L'utilisation par le Kremlin de « fermes à trolls », où des commentateurs sont payés pour influencer le débat en ligne, en Russie et aux Etats-Unis, est un autre volet de l'activité parfois délétère de la Russie sur Internet.

Le communiqué attribuant à Moscou la cyberattaque contre le Parti démocrate, quelques semaines avant le scrutin du 8 novembre, constitue un net palier dans la dégradation des relationsrusso-américaines dans le domaine de la cybersécurité. Il est rare que les Etats-Unis attribuent officiellement une cyberattaque, et plus encore qu'une puissance rivale soit ainsi désignée.

La Corée du Nord avait été mise en cause par le FBI, en décembre 2014, pour son implication présumée dans le piratage des serveurs du studio Sony Pictures. La même année, cinq militaires chinois avaient été accusés par la justice américaine d'espionnage informatique et de vol de secrets économiques dont auraient été victimes, aux Etats-Unis, les entreprises Westinghouse, Alcoa et United States Steel.

L'accusation portée contre la Russie est cependant d'une tout autre nature : les attaques chinoises et nord-coréennes visaient l'économie américaine, tandis qu'en ciblant le DNC à la veille des élections les pirates ont touché au fonctionnement même de la démocratie américaine, dans un contextede tensions entre Moscou et Washington. *« Influencer le débat politique d'un pays, les Etats-Unis le font tout le temps – par la diplomatie, par exemple –,* observe Adam Segal, du think tank américain Council of Foreign Relations. *Mais attribuer l'attaque du DNC à la Russie est une manière de dire que ce pays a franchi une limite. »*

Les Etats-Unis vont-ils apporter une réponse plus musclée à ces cyberattaques que cette stratégie du *« name and shame »* (« nommer et couvrir de honte ») ? Cette dernière *« peut avoir un impact si deux nations ont intérêt à s'entendre*, explique Matthijs Veenendaal. *Mais, actuellement, la Russie ne montre aucun signe de volonté à améliorer sa relation avec les Etats-Unis ».*

Répondre par la force si besoin

D'autres options sont envisageables par le président Barack Obama. Il pourrait ainsi appliquer l'Executive Order, adopté à l'été 2015 : un outil législatif inédit lui permettant de prendre des sanctions financières contre des organisations ou des pirates soupçonnés d'avoir orchestré des cyberattaques. Reste que les sanctions économiques

occidentales à l'encontre de Moscou, déjà mises en place en réaction au conflit en Ukraine, n'ont visiblement pas découragé les Russes de s'en prendre aux Etats-Unis.

Une contre-attaque – les Etats-Unis disposent des moyens offensifs les plus aboutis du monde – peut également être organisée. Depuis 2011, la doctrine américaine établit que les Etats-Unis peuvent répondre, par la force si besoin, à toute cyberattaque dirigée contre leurs intérêts. Mais cette théorie se heurte à la perspective de nouvelles attaques contre le système électoral américain. A plus long terme, l'administration américaine n'aurait que peu d'intérêts à provoquer un affrontement incontrôlé dans le cyberespace, compte tenu de la dépendance de son économie et de son administration à Internet.

Cette option serait aussi contraire à l'objectif affiché des Américains en matière de diplomatie – la construction d'un « code de la route » pour le cyberespace –, alors même qu'ils ne donnent pas l'exemple en matière de surveillance et d'espionnage numériques. *« Notre but n'est pas de provoquer un cycle d'escalade auquel on a assisté dans le passé pour d'autres types d'armement, mais plutôt de construire des normes afin que tout le monde se comporte de manière responsable »,* a déclaré Barack Obama au sujet du piratage du DNC lors de sa conférence de presse au G20 de Hangzhou (Chine), le 5 septembre.

La Chine, ancien ennemi numéro un

L'accusation américaine portée à l'encontre de Moscou illustre le dilemme auquel est confronté Washington : circonscrire les cyberattaques sans déclencher de conflit ouvert. Cette problématique rappelle celle qui s'est posée quand le cyberespionnage économique chinois est devenu, au début des années 2010, un enjeu majeur des relations sino-américaines.

Après des négociations officieuses, les autorités américaines ont fini par hausser le ton, le chef de l'Agence nationale de la sécurité (NSA) qualifiant, en juin 2013, l'espionnage chinois de *« plus important transfert de richesses de l'histoire ».* La même année, la presse américaine évoquait la possibilité de sanctions contre la Chine. Les tentatives d'apaisement ont échoué après les révélations d'Edward Snowden, impliquant les Etats-Unis dans des affaires de cyberespionnage, y compris économique. La situation se corse quand, en 2014, cinq militaires chinois sont mis en accusation par la justice américaine : la Chine suspend les discussions.

En 2015, la Chine devient le suspect numéro un dans le piratage d'une base de données fédérale de l'Office of Personnel Management (OPM), contenant des informations sur plus de 20 millions d'Américains, dont certains étaient accrédités « secret défense ». Washington semblait alors prêt à répliquer, sans que cette exaspération soit finalement traduite en actes.

Accord surprise de 2015

C'est dans ce contexte tendu qu'en septembre 2015, les deux pays étaient pourtant parvenus à un accord surprise sur le cyberespionnage économique. Les mots sont soigneusement choisis : chaque pays s'engage à ne pas *« mener ni soutenir volontairement le vol électronique de propriété intellectuelle aux fins de fournir des avantages compétitifs à des entreprises ou à des secteurs commerciaux »*. C'est la première fois que deux pays s'accordent ainsi à tracer une ligne rouge dans le cyberespace : l'espionnage économique est officiellement condamné. La coopération s'enclenche alors : une réunion portant sur la traduction concrète de cet accord, la troisième du genre, devrait avoir lieu en décembre 2016.

Depuis, une certaine normalité semble prévaloir. *« L'activité chinoise a quelque peu diminué »,* affirmait en avril Mike Rogers, patron de la NSA. Un constat corroboré par des entreprises américaines spécialisées en sécurité informatique. L'une d'elles, FireEye, dans un rapport publié en juin, notait une *« menace moins grande mais plus ciblée, calculée, qui parvient encore à compromettre des réseaux d'entreprises »*.

Cette reconfiguration de la menace chinoise pourrait, outre l'accord de septembre 2015, être liée à d'autres facteurs tels que la réorganisation de l'armée chinoise entreprise par Xi Jinping, qui a permis de rationaliser et de

professionnaliser ses forces offensives dans le cyberespace. La lutte contre la corruption menée par Pékin pourrait aussi avoir remis de l'ordre et *« limité le travail "de free-lance" de fonctionnaires chinois utilisant les moyens de l'armée ou de l'Etat à des fins personnelles »,* explique Scott Harold, spécialiste de l'Asie à la Rand Corporation, un think tank basé en Californie.

Cet apaisement sur le front sino-américain doit être relativisé. Les experts ignorent s'il sera durable. *« Les Chinois ont tellement investi pour pénétrer dans les réseaux, mais aussi pour traiter l'information qu'ils récupèrent,* note Jon Lindsay, professeur en multimédia et relations internationales à l'université de Toronto. *Difficile de les imaginer renoncer à un tel investissement. »*

« Un important contentieux politique »

L'accord entre les Etats-Unis et la Chine prouve que deux pays aux intérêts contraires sur les réseaux peuvent toujours s'accorder sur quelques règles de principe. Difficile pourtant d'imaginer que les relations russo-américaines suivent le même chemin. *« La Russie n'a pas le même profil que la Chine : elle n'a pas de grandes entreprises aux Etats-Unis, ni d'investissements d'ampleur, le marché américain ne lui est pas crucial pour écouler ses biens et ses services,* résume Scott Harold, spécialiste de l'Asie à la Rand Corporation, un think tank établi en Californie. *En outre, il y a un important contentieux politique depuis la guerre entre la Russie et la Géorgie* [en 2008]. *Vladimir Poutine prospère grâce à l'idée que l'Occident est injuste avec la Russie. C'est un paradoxe, mais les sanctions pourraient le servir politiquement. »* Jon Lindsay, professeur de relations internationales à l'université de Toronto, abonde :*« La Chine piratait pour son développement économique, mais voulait garder les choses sous contrôle. La Russie, elle, veut voir davantage de friction, de bruit, d'agitation. »*

Manifestations ant-Poutine, à Moscou, en décembre 2011. SIME SIMON/CC BY 2.0

Au-delà de l'exemple russe, selon les experts, les escarmouches dans le cyberespace sont vouées à se multiplier. L'indécision américaine face à la Chine a-t-elle donné un blanc-seing à d'autres Etats pour intervenir dans le cyberespace ? Au bout d'une décennie de cyberattaques, faute de sanctions et malgré des progrès avec la Chine, les Etats-Unis ne sont pas parvenus à se montrer assez dissuasifs. *« Pékin ou Moscou n'iront pas jusqu'à des attaques destructrices, comme l'extinction du réseau électrique, par exemple*, estime Adam Segal. *Mais, à un autre niveau, la dissuasion est impossible*. *Nous allons assister à du harcèlement continuel entre Etats, avec une limite de plus en plus floue entre la guerre et la paix. »*

« C'est une nouvelle forme de conflit du XXIe siècle : *des attaques bon marché et difficiles à retracer »,* avance Pasha Sharikov, chercheur à l'Académie des sciences de Moscou. Est-il encore possible de pacifier le cyberespace ? Oui, estime Matthijs Veenendaal, à condition de *« travailler sur des normes internationales – l'approche la plus logique et la plus réaliste ».* Même si la normalisation progressive des relations sino-américaines ne s'explique pas seulement par le traité signé en 2015, ce dernier a fait des émules. Le Royaume-Uni et la Chine sont parvenus à un accord similaire. L'Allemagne s'est, en juin, à son tour entendue avec le plus grand partenaire commercial asiatique de l'Europe.

Depuis plusieurs années, les efforts des Russes pour faire adopter un accord sur la cybersécurité aux Nations unies n'ont pas été couronnés de succès. Les discussions engagées entre Moscou et Washington ont été interrompues par les crises en Ukraine et en Syrie. Une poignée de hauts fonctionnaires se sont malgré tout réunis à Genève au printemps pour reprendre langue. L'accusation portée aujourd'hui par l'administration Obama pourrait bien repousser sine die ces tentatives d'apaisement.

Martin Untersinger

Labels, moteur de recherche… les nouveaux dispositifs de Facebook sur la publicité politique

Critiqué durant la campagne présidentielle états-unienne de 2016 pour avoir laissé des annonceurs étrangers tenter d'influencer le cours de l'élection, Facebook a mis en place des mesures.

Par Perrine Signoret Publié le 25 mai 2018 à 14h53 - Mis à jour le 25 mai 2018 à 14h53

Environ 3 000 annonces publiées sur Facebook pendant la campagne électorale états-unienne de 2016 provenaient de Russie. QUENTIN HUGON / « LE MONDE »

Malgré une semaine bien chargée, partagée entre son audition devant le Parlement européen et sa venue au Salon VivaTech à Paris, Mark Zuckerberg a annoncé l'implémentation de nouvelles mesures concernant les publicités politiques sur Facebook. Dans un post publié jeudi 24 mai, il a expliqué vouloir rendre ces dernières plus *« transparentes »* aux yeux des utilisateurs.

Un moteur de recherche pour retrouver des publicités

Désormais, les publicités politiques affichées sur Facebook et Instagram (qui appartient au premier) seront, aux Etats-Unis uniquement (le dispositif seraétendu dans les prochains mois à d'autres pays), *« clairement labellisées »* : l'identité de l'annonceur apparaîtra. En cliquant dessus, les utilisateurs pourront accéder aux archives de l'activité de l'annonceur – combien il a dépensé pour telle ou telle campagne de publicité, combien de personnes l'ont vue, quel est leur âge, leur localisation et leur genre.

Autre nouveauté : un moteur de recherche permet désormais d'effectuer une recherche de publicités politiques par annonceur ou par mot-clé, que la campagne soit en cours ou terminée. Cela concerne aussi bien les contenus mentionnant des candidats à des élections que ceux évoquant des*« problématiques qui divisent »*, explique Facebook. Il est accessible en France, mais n'est supposé concerner que les contenus qui ciblaient un public américain.

Le moteur de recherche lancé par Facebook permet par exemple de voir les annonces sponsorisées qui concernent Donald Trump.

Ces données sont conservées et répertoriées, précise Mark Zuckerberg, pour une durée de sept ans.

« L'une des plus grandes priorités pour 2018 »

Enfin, chaque annonceur politique devra justifier de son identité et de sa localisation, ce qu'avait déjà expliqué Facebook. En février, l'entreprise avait annoncé qu'elle allait envoyer des courriers postaux pour vérifier ces informations.

Une manière, pour le réseau social, d'éviter que des entités étrangères ne s'impliquent dans des élections américaines. Durant la campagne présidentielle américaine de 2016, lui comme Twitter avaient fait l'objet de critiques, pour avoir laissé des publicités politiques venues de l'étranger envahir leurs plates-formes.

Environ 3 000 publicités diffusées sur Facebook et Instagram avaient ainsi été achetées en Russie. En mai, les démocrates de la commission du renseignement de la Chambre des représentants ont publié ces contenus, dont

l'objectif semblait être d'attiser les dissensions de la société américaine, et de favoriser Donald Trump face à son adversaire, Hillary Clinton.

« L'une de mes plus grandes priorités pour 2018 est de m'assurer que nous empêcherons les interférences et la désinformation pendant les élections, a expliqué Mark Zuckerberg. *Ces changements ne résoudront pas tout, mais ils rendront* [la tâche] *plus difficile. »*

Perrine Signoret