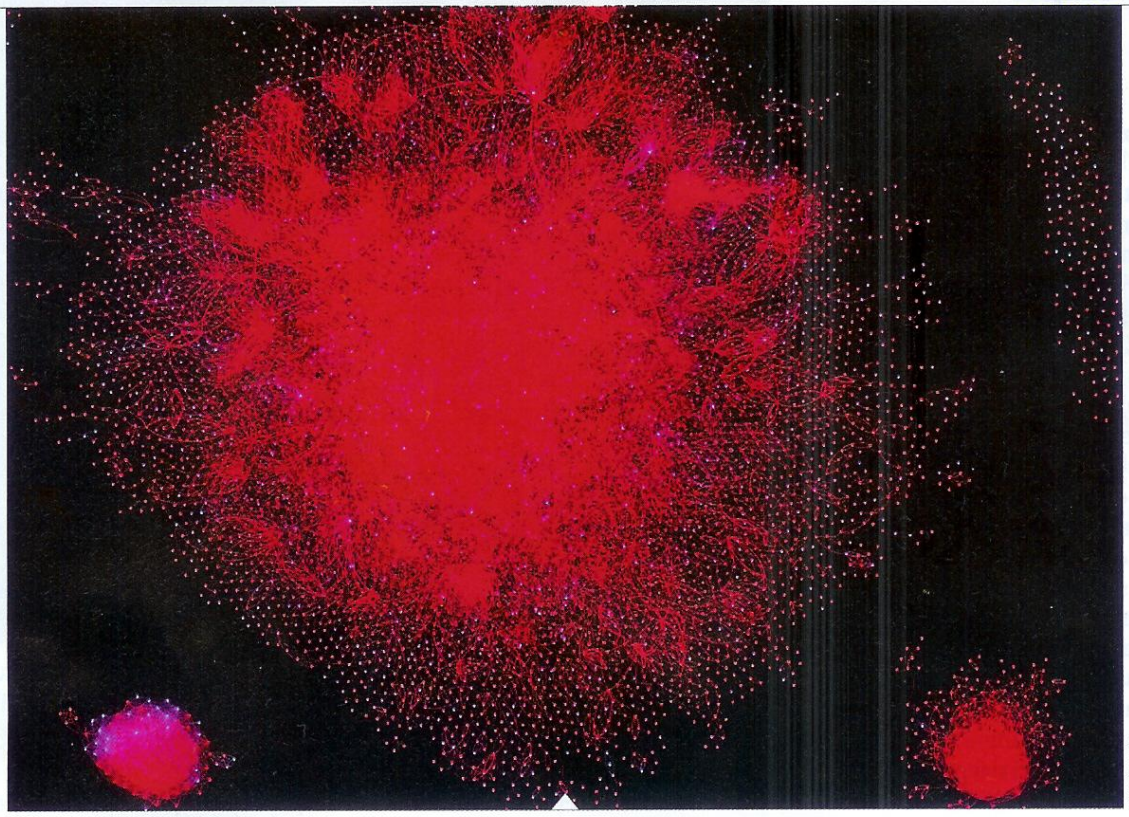


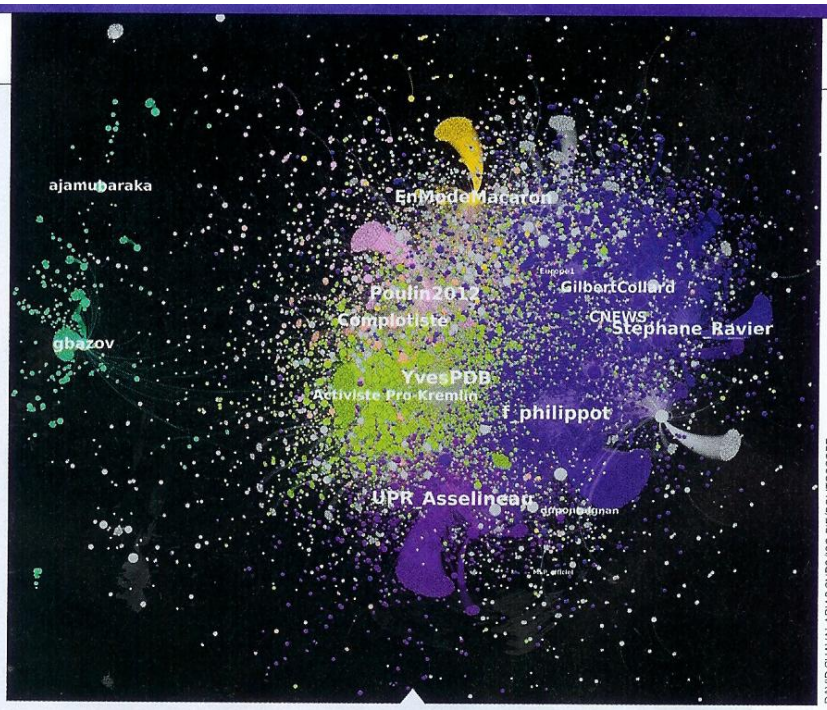
TIM GRAHAM

Selon cette modélisation, l'écrasante majorité des 10 000 comptes Twitter ayant relayé en mars des messages de propagande russe (#StandWithP*tin) après l'invasion de l'Ukraine a été générée par des « bots » (robots, en rouge), plutôt que par des humains (en bleu).

Les réseaux sociaux au cœur de la manipulation

Facebook et Twitter sont devenus des outils de choix pour influencer l'opinion et semer le doute. Des chercheurs ont développé des algorithmes qui mettent en lumière l'ampleur de cette désinformation.

La manœuvre a lieu sur le réseau social Twitter. Son objectif : contrer les informations dénonçant l'invasion russe en Ukraine. Des messages nient ainsi le bombardement par les Russes de la maternité de Marioupol ; affirment que des images de victimes civiles ukrainiennes sont des mises en scène ; dénoncent la russophobie de l'Occident... Les auteurs ? Une myriade de comptes officiels relevant du ministère des Affaires étrangères russe : missions russes à Genève (Suisse), Vienne (Autriche) et aux Nations unies, ambassades de Russie au Canada ou au Royaume-Uni... Tous se retweetent les uns les autres, donnant une large visibilité aux messages. C'est le chercheur australien Timothy Graham, de l'université de technologie du Queensland, qui a repéré le phénomène, recensant pas moins de 75 comptes officiels se donnant pour but d'occuper le terrain numérique.



Cette cartographie du Politoscope représente les comptes Twitter politiques français mobilisant une terminologie typique de la propagande du Kremlin, entre le 23 février et le 10 avril 2022.

Ce n'est pas tout. Grâce à des outils informatiques capables de détecter des actions coordonnées, Timothy Graham et son équipe montrent que ces comptes retweetent les mêmes choses de manière simultanée (dans les 60 secondes). « *J'ai entrepris de prolonger l'analyse vers des comptes automatisés ou semi-automatisés diffusant la désinformation pro-russe* », ajoute le chercheur à *Sciences et Avenir*. Bilan ? Il a découvert au moins 870 « bots », c'est-à-dire des comptes programmés pour « aimer » automatiquement les tweets du gouvernement russe. Son équipe s'est servie pour cela d'un outil d'apprentissage automatique appelé Botometer (développé à l'université de l'Indiana, aux États-Unis). En analysant les caractéristiques de profils Twitter donnés, cet algorithme calcule la probabilité que ceux-ci soient authentiques ou faux. Là encore, le rôle des « bots » est de gonfler artificiellement la diffusion de la propagande du Kremlin.

À la fois gratuits et offrant une audience potentiellement massive sans passer par les médias traditionnels, les réseaux sociaux, Facebook et Twitter en tête, sont devenus des outils de choix pour influencer l'opinion et semer le doute. Sur Twitter, par exemple, plus des contenus sont retweetés et suscitent d'interactions, plus ils apparaissent dans la rubrique « Tendances » du réseau social. En organisant une campagne de retweets, on peut ainsi créer des « Tendances ». La pratique, connue sous le nom d'*astroturfing*, sert à faire croire qu'un débat, une polémique sont nés spontanément et mobilisent plus qu'ils ne le font en réalité. Les proches du candidat d'extrême droite à l'élection présidentielle Éric Zemmour en ont beaucoup usé pour imposer leurs thèmes (immigration, islamisme) ou exagérer l'engouement pour le candidat (« Femmes avec Zemmour », « Zemmoureuses »). En l'occurrence, l'équipe s'est particulièrement bien approprié le numérique, comme l'ont constaté les mathématiciens du projet Linkage grâce à des technologies d'apprentissage automatique appliquées aux interactions et aux contenus des réseaux sociaux : « *Il existe un premier petit cercle d'internautes, les lieutenants d'Éric Zemmour, qui émettent les messages, sont très connectés entre eux et se retweetent mutuellement,* détaille Pierre Latouche, professeur à l'université Paris-Cité. *Un deuxième cercle retweete massivement ce qui est posté par le premier, puis un troisième, plus lâche, forme une nébuleuse. Cette distinction est si nette qu'elle a sans doute été pensée ainsi.* »

La mécanique du ciblage publicitaire

Autre pratique en vogue, le *hashtag hacking* permet de forcer l'exposition de communautés d'internautes à un message. L'astuce ? Marquer une publication avec un ou des mots clefs (hashtag) correspondant à telle ou telle communauté. Par exemple, entre les deux tours de l'élection présidentielle française de 2017, des hashtags anti-Emmanuel Macron étaient associés à des hashtags comme #Fillon, #Melenchon ou #laforcedupeuple, pour s'adresser aux sympathisants de candidats éliminés au premier tour.

Toutes ces manœuvres peuvent être orchestrées depuis l'étranger. Deux jours avant le second tour de la présidentielle française de 2017, des activistes américains d'extrême droite relayaient ainsi vers l'Internet français les « Macron-Leaks », un dossier de 15 gigaoctets de courriels piratés du parti d'Emmanuel Macron, posté sur le forum 4chan et

DÉTECTION

Viginum, une agence contre la désinformation

Un décret français du 13 juillet 2021 a créé un « service de vigilance et de protection contre les ingérences numériques étrangères ». Surnommé Viginum, il est rattaché au secrétaire général de la Défense et de la Sécurité nationale. Son rôle ? Détecter et analyser les campagnes de désinformation, en identifier l'origine, repérer des bots, alerter les autorités. Mais Viginum n'a pas de rôle d'intervention ni de sanction.

MODÈLE ÉCONOMIQUE

Capter l'attention de l'internaute

L'économiste américain Michael Goldhaber propose en 1997 l'expression « économie de l'attention » pour définir un fonctionnement vertueux promis par Internet, où l'internaute détiendrait le pouvoir grâce à sa faculté d'accorder ou non son attention. Le concept peut être valable à l'époque des forums, des sites collaboratifs et des blogs où prime le partage de connaissances et où Google naît à peine. Mais avec les réseaux sociaux, tout bascule. « *Capter l'attention de l'internaute est devenu une discipline à part entière. Le modèle économique, la technique, le design sont développés à cette fin* », explique Anne Alombert, coauteure d'un rapport sur le sujet en janvier pour le Conseil national du numérique (Cnnum). Avec des services devenus omniprésents, les contenus peuvent passer de l'un à l'autre (Facebook, Twitter, Instagram, WhatsApp, Instagram, YouTube…) en un clic, consultables en un flux ininterrompu, constamment mis à jour. C'est cet environnement qui porte en germe une « économie de la manipulation », estime le rapport du Cnnum. La différence ? « *L'attention est une ressource destinée à être revendue ; la manipulation sous-entend le rôle d'un acteur précis derrière certaines manœuvres ayant un objectif* », souligne Anne Alombert.

POUR EN SAVOIR PLUS

- « Le micro-ciblage publicitaire, comment biaiser une élection » : **sciav.fr/904ciblage**
- Interview de David Chavalarias : **sciav.fr/904chavalarias**
- Dossier du Cnnum sur l'économie de l'attention : **sciav.fr/904cnnum**

supposément compromettants. Or, non seulement il n'y avait aucune révélation, mais certains fichiers avaient été trafiqués, des indices laissant penser que les manœuvres provenaient de la Russie.
L'arme de choix de cet arsenal numérique reste la mécanique sur laquelle est fondé le modèle économique des réseaux sociaux : le ciblage et la personnalisation des contenus publicitaires grâce à l'analyse des données des utilisateurs. « *Les contenus que l'on nous montre ne sont sélectionnés qu'en fonction de critères économiques servant les intérêts de ces plateformes* », explique David Chavalarias, directeur de recherche au CNRS et auteur du livre *Toxic Data* détaillant ces pratiques. Selon cette logique, chaque internaute ne voit que ce que les algorithmes jugent pertinent de lui montrer, le confortant dans ses goûts, croyances et opinions, et évitant de l'exposer à la contradiction.
Il est possible d'envoyer un contenu en définissant la cible selon quantité de critères : langue, genre, opinions, valeurs, origines, profession, tranche d'âge, localisation, voire état émotionnel ou système d'exploitation mobile. « *Les réseaux sociaux accumulent tellement de données sur leurs usagers, atteignent une telle finesse de profilage qu'il est devenu possible pour eux d'anticiper leurs centres d'intérêt voire leurs votes* », estime Olga Kokshagina, coauteure d'un dossier consacré à l'économie de l'attention au Conseil national du numérique *(lire l'encadré ci-dessus)*. Ces pratiques ont été massivement employées aux États-Unis en 2016 contre Hillary Clinton. Par la désormais célèbre société britannique Cambridge Analytica, mais aussi par une entreprise russe financée par le Kremlin, Internet Research Agency. Celle-ci a notamment créé une page Facebook de soi-disant Texans sécessionnistes. En la suivant, des dizaines de milliers d'internautes américains permettaient, sans le savoir, aux administrateurs de les cibler avec des publications partisanes (appels à manifester, théories du complot, renvois vers des sites Web ou d'autres pages de réseaux sociaux contrôlés aussi par l'agence, etc.). Le but étant d'accentuer clivages et divisions aux États-Unis. « *Quand on dit qu'il faut interdire la publicité politique sur les réseaux sociaux, cela n'a pas beaucoup de sens,* estime David Chavalarias. *Il n'existe pas de frontière nette entre une publicité politique et un contenu qui ne le serait pas.* » Triste ironie que des services faits pour « *rapprocher les gens* », selon les mots du fondateur de Facebook Mark Zuckerberg, soient devenus les meilleurs instruments de l'agitation et du conflit. ■

Arnaud Devillard @A_Devila


D.CHAVALARIAS

« Les contenus que l'on nous montre ne sont sélectionnés qu'en fonction de critères servant les intérêts des plateformes »
David Chavalarias, mathématicien, directeur de recherche au CNRS