Ces trolls qui contrôlent le récit dans les médias et sur internet

Comment dépister les robots, bots, «otaries» qui cherchent à neutraliser les infos dérangeantes

D'après un épisode de Solution's Watch de James Corbett[1]

Soyons honnêtes: les commentaires en bas des vidéos ou des articles sont souvent mauvais. Mais qui peut dire s'ils sont réels? Et quelle est la solution à ces messages désastreux? Ne pas lire les commentaires, bien sûr. Mais ceux qui s'aventurent sur ces champs de bataille publics doivent au moins connaître les différentes tactiques employées par les trolls*, les bots*, les espions et les «otaries» qui cherchent à inhiber leurs pensées et leurs actions.

(Photo mad)

Trafic de robots

Les commentaires peuvent être une source très riche d'information complémentaire, en particulier sur des sujets controversés, et cette section tend à gagner en importance par rapport au contenu principal de la publication. Mais il n'est pas rare d'y trouver une pléthore de propos diffamants – par exemple des expressions antisémites, obscènes ou insultantes. Bien que la plupart des créateurs de contenus aient pris l'habitude de ne pas y attacher trop d'importance, cela peut avoir un sérieux impact sur le partage de la vidéo ou sur le taux d'abonnement à la chaîne.

La première question est de savoir si les commentaires en question proviennent de véritables internautes ou s'ils sont générés par un algorithme. D'après un *article de Tech Radar,*[2] analysant un rapport sur les bots, 47% du trafic web* serait dû – par définition, serait-on tenté de dire – à des robots, un chiffre qui augmente d'environ 5% par an, alors que le pourcentage trafic dû aux humains se réduit chaque année. Et près de 30% de ces «bots» sont malveillants.

Le trafic bot n'est pas négatif en soi, puisqu'il est essentiel pour les assistants numériques, les moteurs de recherche et compagnie, mais il contient malheureusement une multitude de «bots malveillants». Ceux-ci vont par exemple cibler les sites web et les applications mobiles avec des campagnes de «web scraping» (extraction d'information des sites), de «data mining» (exploration de données), mener des attaques directes sur les sites ou des chaînes de diffusion, ou détourner les transactions bancaires.

Certains bots ont des cibles spécifiques et sont dirigés par des agents des services de renseignements désignés pour «lutter contre la désinformation en ligne».

Pour éviter le trafic bot, de nombreux sites utilisent des applications qui obligent les utilisateurs à s'identifier comme «humain», et leur demandent d'exécuter un petit test visuel ou auditif. Mais il est difficile d'appliquer ceci à la section des commentaires ou aux conversations de groupe dans les applications de chat. Une parade des créateurs de contenus qui sont trop souvent attaqués, est de publier leurs contenus sur différentes plateformes, en activant la section des commentaires d'un côté, en la désactivant de l'autre, et en mentionnant partout les liens vers les publications alternatives.

Techniques de trolls

Ce n'est pas un fantasme: l'une des missions des *services de renseignements est de contrôler le récit dans les médias et sur les réseaux sociaux,*[3] puisque le contrôle de l'opinion publique par la fabrique du consentement ou *la censure*[4] sont les éléments clés de toute stratégie politique. La bataille qui a lieu entre le commissaire européen *Thierry Breton* et le patron de *X/Twitter Elon Musk* pour contrôler *les informations sur la guerre entre Israël et Gaza*[5] en est bien la preuve. Tout comme la *censure du candidat aux présidentielles Robert*

Kennedy Jr,[6] le scandale des «fact checkers» payés par *le fonds Marianne*[7] ou le fait que *la Cour Suprême américaine soit amenée à se prononcer sur l'ingérence de la Maison Blanche*[8] dans le contrôle des réseaux sociaux.
Il y a donc des trolls payés par le contribuable en plus des harceleurs 'naturels'. Ces agents sont mandatés pour contrôler le récit, infiltrer les groupes et neutraliser les informations trop dérangeantes. Ils opèrent avec de multiples identités en simultané et sur diverses plateformes, afin de polluer et d'interrompre la conversation ou d'influencer le discours. On trouve une description intéressante de certains de leurs procédés dans un document intitulé *The Gentle Person's Guide to Forum Spies*[9] du site *Cryptome.org* (un site proche de *Wikileaks*) qui se réfère aux méthodes de *Cointelpro.*

Cointelpro est apparemment un programme disruptif des services secrets américains dont l'objectif est la dilution, le détournement ou la prise de contrôle d'un forum ou d'un lieu de discussion sur internet, typiquement une section de commentaires.

Parmi les techniques utilisées, l'on note en premier lieu le fait de bombarder une info importante par une succession rapide d'autres messages, afin de la faire «descendre» dans la liste des messages et de la rendre moins visible.

Il y a ensuite la «fragilisation du consensus». Il s'agit de poster une opinion contraire, en démarrant avec une suggestion plutôt faible, sans beaucoup d'arguments, mais que l'on viendra progressivement renforcer sous d'autres noms d'utilisateurs, afin que le lecteur ait vraiment l'impression qu'une contre-argumentation s'élabore progressivement pour renverser le consensus qui régnait auparavant.

La «dilution» de la thématique est une autre technique, qui consiste à constamment emmener les lecteurs sur des sujets secondaires, des voies de garage, pour leur faire perdre du temps et les maintenir dans l'inaction. A la longue, ceci poussera les utilisateurs productifs à déserter le forum, tandis que les autres passeront de l'analyse des faits pertinents au mode du «bavardage».

L'agent en profitera pour collecter des informations dans le groupe en commençant par parler de ses propres intérêts. Par exemple en posant une question telle que: quel système utilisez-vous pour protéger votre vie privée? Ou bien, où trouvez-vous vos ressources? Voire même des questions concernant la vie personnelle des internautes.

Une autre tactique récurrente est la discussion violente entre deux identités contrôlées par l'agent «troll». Lorsque les autres prendront part à la discussion enflammée, ils diront probablement des choses qui dépassent leur pensée, mais que l'on pourra ensuite retenir contre eux, par exemple des insultes, ou des incitations à la haine et à la violence.

Démolir l'argumentation

Les techniques les plus utilisées pour démolir une argumentation solide sont les suivantes: dévier l'attention de la thématique vers ceux qui sont impliqués ou qui l'exposent: lynchage, moquerie, insultes ou indignation, il y a généralement tout un registre émotionnel qui est déployé pour détourner l'attention du véritable argument.

Une autre méthode pour interrompre le discours, que l'on détecte moins facilement, est la «technique de l'otarie». Elle consiste en un harcèlement poli et «ingénu» à force de demandes répétées. Il s'agira par exemple de contester chaque affirmation en demandant de 'fournir des preuves' que l'on invalidera ensuite à l'infini. Cela peut aussi être des questions secondaires auxquelles il faut toujours répondre, ou une demande constante d'entamer un débat inutile. L'objectif est de faire perdre patience à l'internaute et aux lecteurs, en poussant à l'énervement ou à l'abandon de la conversation. Comme toujours avec les trolls, la meilleure attitude est de dénoncer leur action avant de cesser de répondre.

Pour neutraliser ce travail de sape, il faut avant tout prendre conscience de l'existence de ces techniques. Le mieux est alors de les dénoncer sur le lieu de discussion. Il n'est pas nécessaire de savoir s'il s'agit d'une véritable infiltration ou si l'on est en présence de saboteurs spontanés. L'important est surtout de montrer que ces interactions sont contre-productives, et qu'il ne faut pas tomber dans ce piège.

En somme, rester attentif à la manière dont les conversations se déroulent permet déjà de recentrer sur le fondement de sa propre opinion. Dans quelle mesure et par quel biais notre attention a-t-elle finalement été déviée vers des sujets secondaires ou des conclusions erronées? Et quel impact cela peut-il avoir sur nos actions? Car il faut se rappeler que ces techniques sont avant tout utilisées pour désarmer les arguments et les personnes qui pourraient provoquer un changement concret dans l'organisation so-

ciale, en prenant par exemple une action politique ou en recourant aux tribunaux.

Et finalement, avant même de soupçonner les participants à la conversation d'être d'infâmes agents à la solde des pouvoirs en place, il faut aussi se demander dans quelle mesure l'on est soi-même susceptible d'utiliser inconsciemment ces techniques peu louables. Après tout n'est-ce pas là l'attitude du véritable gentleman?

Source: Information de CovidHub, https://www.covidhub.ch/guide-gentleman-trolls/, 23 octobre 2023

[1] *https://www.bitchute.com/video/8dyhRfC5lAWx/*

[2] *https://www.techradar.com/news/bots-now-make-up-nearly-half-of-all-internet-traffic-and-thats-very-bad-news-for-our-security*

[3] *https://sentadepuydt.substack.com/p/la-cia-et-le-fbi-a-la-tete-de-la*

[4] *https://www.covidhub.ch/incontournables-3-censure/*

[5] *https://www.covidhub.ch/guerre-gaza-europe-controle-info/*

[6] *https://www.covidhub.ch/la-censure-des-geants-dinternet/*

[7] *https://www.francesoir.fr/recherche?search_api_fulltext=fonds%20marianne&page=0*

[8] *https://childrenshealthdefense.org/defender/texas-law-social-media-censorship-supreme-court/*

[9] *https://cryptome.org/2012/07/gent-forum-spies.htm*

*** Glossaire**

Troll

Dans le jargon informatique, le terme «troll» désigne une «personne» qui cherche délibérément à déclencher une dispute verbale sur Internet par des commentaires «incendiaires» ou à énerver délibérément les internautes. Cela se fait généralement en «postant» des messages et des contributions inflammatoires et digressifs, non pertinents ou sans rapport avec le sujet dans une communauté en ligne. Leur communication dans ces communautés se limite à des messages visant à provoquer émotionnellement ou à déstabiliser les autres participants à la conversation.

Bot

Le terme «bot» est dérivé du mot «robot». Comme les robots mécaniques, les bots informatiques sont programmés pour exécuter des tâches spécifiques et répétitives. Pour ce faire, ils exécutent des ordres clairement définis sous forme d'algorithmes et de scripts, qu'ils mettent en œuvre plus rapidement que n'importe quel être humain ne pourrait le faire. Les bots sont donc des programmes informatiques qui agissent de manière autonome et automatisée et qui ne dépendent pas, dans leur fonctionnement, de la participation ou de la surveillance d'un être humain.

Les «bots malveillants servent différents objectifs illégaux. En font partie:

- Le vol de données et d'identité par le biais du scraping, du phishing et du keylogging d'informations sensibles telles que les mots de passe, les données bancaires et les données d'adresse.
- Attaques par déni de service distribué (DDoS), dont le trafic massif de données peut paralyser des serveurs.
- Utilisation de portes dérobées dans le système de sécurité d'un PC pour infecter le système.
- Retransmission avec du spam pour détourner des paquets de données.

Les bots ou logiciels malveillants comprennent les types suivants:

- Bots de propagande ou de manipulation: bots sociaux qui simulent des profils d'utilisateurs, qui forment des opinions numériques et diffusent des déclarations politiques, des fausses nouvelles et des théories du complot ou qui réagissent aux commentaires et aux posts à l'aide de mots-clés.
- Bots d'escroquerie/d'hameçonnage: ces bots pratiquent le vol de données par le biais de pseudo-liens, de faux courriels et de faux sites web.
- Enregistreurs de frappe: bots qui enregistrent le trafic des messages ou qui notent, enregistrent et transmettent toute activité sur un PC.
- Bots de partage de fichiers: ils réagissent à des demandes de recherche ciblées et proposent aux utilisateurs un lien vers le terme de recherche souhaité. En cliquant sur ce lien, le bot peut infecter le PC utilisé par l'homme.
- Spambot: ils envoient de grandes quantités de spams et collectent des adresses électroniques sur les pages web et les contacts d'utilisateurs innocents pour élargir leur rayon de spam.
- Bots zombies: ce sont des ordinateurs infectés par des logiciels malveillants ou qui font partie d'un réseau de bots et fournissent la puissance de calcul nécessaire à des attaques de botnet de grande envergure. Souvent, les ordinateurs compromis ne sont pas facilement reconnaissables comme faisant partie d'un réseau de zombies.
- Botnet: Désigne l'ensemble des PC infectés qui sont réunis en un réseau et utilisés par les utilisateurs de logiciels malveillants pour des attaques DDoS.

Les cinq attaques de bots les plus fréquentes sont les suivantes:

- Attaques DDoS: surcharge de serveurs provoquée de manière ciblée.
- Spamming et surveillance du trafic: surcharge des serveurs de messagerie ou vol de données à grande échelle.
- Attaques par déni de service distribué (DDoS): Attaques contre des boutiques en ligne afin de répertorier des produits comme «non disponibles».
- Attaques par grattage de compte: Vol de données et vente de données.
- Attaques par bourrage d'identifiants: accéder de manière frauduleuse à un compte utilisateur d'une application Web à la suite de tentatives de connexion automatisées à partir d'une liste de données d'accès, généralement volée auprès d'une autre application Web.