CCN-CERT

BP/13

La Désinformation dans le Cyberespace

RAPPORT DE BONNES PRATIQUES

AOÛT **2021**

centro criptológico nacional

centro criptológico nacional

Édits:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

Date de sortie: Août de 2021

LIMITATION DE LA RESPONSABILITÉ

Ce document est fourni conformément aux termes contenus dans le présent document, rejetant expressément tout type de garantie implicite qui pourrait y être liée. En aucun cas, le Centre National de Cryptologie ne peut être tenu responsable des dommages directs, indirects, fortuits ou extraordinaires dérivés de l'utilisation des informations et des logiciels indiqués, même s'il a été averti d'une telle possibilité.

AVIS JURIDIQUE

La reproduction de tout ou partie de ce document par quelque moyen ou procédé que ce soit, y compris la reprographie et le traitement informatique, ainsi que la diffusion de copies par location ou prêt public, sont strictement interdites sans l'autorisation écrite du Centre national de cryptologie, sous peine des sanctions prévues par la loi.

Index

1. À propos du CCN-CERT

Le CCN-CERT est la capacité de réponse aux incidents de sécurité informatique du Centre national de cryptologie, CCN, rattaché au Centre national de renseignement, CNI. Ce service a été créé en 2006 en tant que **CERT Gouvernemental National espagnol** et ses fonctions sont définies dans la loi 11/2002 réglementant le CNI, le RD 421/2004 réglementant le CCN et dans le RD 3/2010, du 8 janvier, réglementant le schéma national de sécurité (ENS), modifié par le RD 951/2015 du 23 octobre.

Sa mission est donc de contribuer à l'amélioration de la cybersécurité espagnole, en étant le centre national d'alerte et de réponse qui coopère et aide à répondre rapidement et efficacement aux cyberattaques et à faire face activement aux cybermenaces, y compris la coordination au niveau public de l'État des différentes capacités de réponse aux incidents ou des centres opérationnels de cybersécurité existants.

F de la loi 11/2002) et des informations sensibles, défendre le patrimoine technologique de l'Espagne, former du personnel spécialisé, appliquer des politiques et des procédures de sécurité et utiliser et développer les technologies les plus appropriées à cette fin.

Conformément à ce règlement et à la loi 40/2015 sur le régime juridique du secteur public, le CCN-CERT est responsable de la gestion des cyber-incidents affectant tout organisme ou entreprise publique. Dans le cas des opérateurs critiques du secteur public, la gestion des cyber-incidents sera assurée par le CCN-CERT en coordination avec le CNPIC.

CCN-CERT est la capacité de réponse aux incidents de sécurité de l'information du Centre National de Cryptologie, CCN.

2. Introduction

La désinformation, en tant que cyber-attaque, est conçue pour éroder et affaiblir la cohésion interne d'un État.

Chaque jour, l'Espagne subit trois (3) cyberattaques de danger critique ou très élevé contre le secteur public et les entreprises stratégiques[1]. Certaines de ces actions offensives proviennent principalement d'autres États, dont l'objectif est d'affaiblir et de compromettre la capacité économique, technologique et politique de l'Espagne dans un monde de plus en plus complexe, compétitif et globalisé.

Les conséquences de ces attaques peuvent entraîner des millions de dollars de pertes pour les entreprises privées et compromettre pendant quelques minutes, quelques heures ou quelques jours le fonctionnement normal des services publics essentiels pour les citoyens espagnols.

Parfois, les dommages causés par des actions numériques offensives se limitent à des pertes économiques et matérielles qui peuvent être réparées à moyen et long terme. Ces dernières années, les grandes entreprises et les institutions publiques stratégiques ont mis au point des plans et des protocoles qui leur permettent d'éviter, de gérer et de minimiser efficacement les conséquences d'éventuelles attaques contre leurs systèmes et leurs infrastructures; une partie de ces plans est consacrée à la reprise des opérations aussi rapidement et efficacement que possible: c'est ce qu'on appelle la **résilience aux cyberattaques.**

Cependant, on assiste de plus en plus à des attaques utilisant le cyberespace contre les intérêts d'un pays qui ne consistent pas à perturber les systèmes informatiques des entreprises et des institutions, mais qui visent à altérer le fonctionnement de l'un des principaux éléments du développement d'une démocratie libérale et d'un État-nation moderne: **l'opinion publique.**

1. CCN-CERT. Capacité de réponse aux incidents du Centre national de cryptologie (CCN-CERT)

2. Introduction

Des penseurs et philosophes tels que Jürgen Habermas affirment qu'une sphère publique fondée sur la délibération rationnelle est la pierre angulaire d'une démocratie . Ainsi, les conséquences d'une cyber-attaque visant à éroder l'opinion publique d'un État ne peuvent passer inaperçues et, en cas de succès, ses dommages ne se limiteraient pas à des pertes économiques ou matérielles, mais pourraient éroder la nature et la raison d'être d'un système de gouvernement fondé sur la démocratie libérale, en affectant les facteurs qui assurent l'intégrité d'un État-nation.

La communication comme arme de guerre n'est pas nouvelle. Il existe des références à l'utilisation de la guerre communicative dans des contextes de guerre depuis plus de 2.500 ans. Le général chinois Sun Tzu, né en 544 avant Jésus-Christ, a écrit que "l'art de la guerre est la tromperie"[3].

À notre époque, la figure de Joseph Goebbles, ministre de l'Instruction publique et de la Propagande du Troisième Reich entre 1933 et 1945, est étudiée dans les facultés des sciences de l'information du monde entier comme le plus grand représentant de l'utilisation de la propagande comme arme de guerre. Les postulats d'Hitler et de son ministre fixent les lignes directrices de la communication et de la désinformation, avant même le conflit armé: *"il est indispensable de démoraliser la nation ennemie, de la préparer à capituler, de la contraindre moralement à la passivité, avant même qu'une action militaire soit prévue... Nous n'hésiterons pas à fomenter des révolutions sur le sol ennemi"*[4].

Au fil du temps, les techniques de propagande et de désinformation se sont perfectionnées dans tous les domaines et dans tous les pays. Cependant, la révolution technologique qui s'est produite au niveau mondial au cours des dix dernières années a entraîné une augmentation exponentielle de ces actions, tant en termes d'ampleur que de fréquence et d'efficacité. Et elle l'a fait non seulement par le biais des méthodes traditionnelles de désinformation, mais aussi en utilisant des outils de diffusion automatique peu coûteux et dotés d'une traçabilité complexe qui augmente considérablement leur répercussion et leur impact.

Les auteurs de ces attaques sont souvent des gouvernements et des groupes subnationaux qui visent à **éroder et à affaiblir la cohésion interne d'un État ou d'un groupe d'États** considérés comme des adversaires et à redéfinir ainsi leur position géostratégique. En effet, certains pays reconnaissent déjà ouvertement qu'ils mènent et entreprennent systématiquement de telles actions. En ce sens, la Russie est l'un des pays qui a le plus développé le concept de guerre

2. MACNAMARA, Jim. 2016. L'écoute organisationnelle.New York. Peter Lang. P. 10
3. SUN TZU (s. V a. C. /2013). L'art de la guerre. Ed. Medí. S.f
4. RAUSCHINING, H, 1940. Hitler m'a dit. Ed. Atlas. Pag.11

hybride ou, selon les termes de la doctrine militaire russe, de "guerres non déclarées" et de "guerres non linéaires"[5].

Selon le général Valery Gerasimov, chef d'état-major général des forces armées de la Fédération de Russie, un État prospère peut *"en quelques mois, voire quelques jours, se transformer en une zone de conflit armé, subir une intervention étrangère et sombrer dans un tissu de chaos, de catastrophe humanitaire et de guerre civile"*.

Ce général russe, promoteur de la **doctrine** dite **Gerasimov**, qui fonde sa réflexion sur l'étude du printemps arabe, estime que: *"Le rôle des moyens non militaires pour atteindre des objectifs politiques et stratégiques s'est accru et, dans de nombreux cas, ils ont dépassé en efficacité la force des armes. Les méthodes les plus couramment utilisées dans les conflits sont de plus en plus liées à l'utilisation d'informations politiques et économiques, de mesures humanitaires et autres mesures non militaires, appliquées en coordination avec les protestations des citoyens [sic]. Cette action est complétée par des moyens militaires clandestins, y compris l'utilisation d'actions d'information et les actions des forces d'opérations spéciales"*[6].

Il existe au moins six (6) facteurs qui contribuent à l'utilisation de plus en plus récurrente d'actions hostiles basées sur la diffusion de la désinformation:

1

Niveau élevé d'efficacité. La révolution technologique a démocratisé l'accès aux médias et à la technologie de production des messages d'information. Il est désormais relativement bon marché et facile de produire des messages multimédias de haute qualité technique et de les diffuser directement et efficacement auprès des publics jugés les plus aptes à les recevoir.

En l'espace de quelques jours, il est possible de créer des sites web et des plates-formes de communication multimédia ayant le même aspect professionnel que les médias séculaires, ou de manipuler des photographies avec des logiciels d'édition facilement accessibles et utilisables.

De même, avec des ressources limitées, même avec un appareil mobile, il est possible de diffuser massivement des contenus en direct, ou de générer des vidéos avec des images artificiellement retouchées, qui seront ensuite diffusées sur Internet et les réseaux sociaux.

5. Consultar el trabajo "Amenazas Híbridas: new tools for old aspirations". Carlos Galán, PhD. Real Instituto Elcano (2018).
6. COALSON, Robert. «Top Russian General Lays Bare Putin´s Plan for Ukraine» [en ligne], dans le *Huffington Post*. S.f. Disponible sur le web: https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

2 **Difficulté d'établir une attribution directe.** L'une des principales caractéristiques des campagnes de désinformation est de générer la confusion, tant par les messages que par les sources.

Les plateformes numériques et la nature même du web sont propices à l'émergence d'acteurs anonymes qui influencent malicieusement la formation de l'opinion publique. Profils numériques anonymes, programmes permettant d'automatiser la diffusion de messages, logiciels permettant de masquer les adresses IP, technologie permettant de créer de nouveaux médias imitant l'apparence de sociétés de médias établies...

Tout internaute a aujourd'hui à sa portée la technologie permettant de créer des réseaux de communication potentiellement influents qui rendent très complexe la traçabilité de l'information et de sa source d'origine.

Il est donc **laborieux et complexe d'étayer par des preuves une accusation directe**, d'engager des poursuites judiciaires ou de prendre des mesures coercitives à l'encontre d'un pays ou d'un groupe sous-national accusé d'avoir déclenché une guerre de communication.

3 **Régulation complexe.** Contrairement à d'autres actions offensives, comme la guerre ouverte sur un champ de bataille, les actions terroristes ou le piratage numérique, la **désinformation et la manipulation de l'opinion publique ne sont pas faciles à combattre** du point de vue juridique des démocraties libérales.

La liberté d'expression et d'opinion est un principe fondamental dans un État-nation démocratique et il est souvent impossible, pour des raisons de principe démocratique, de limiter ces droits, tant pour les nationaux que pour les étrangers.

Créer un média qui diffuse des informations non vérifiées n'est pas un crime, pas plus que la gestion d'une multitude de comptes anonymes sur les médias sociaux, ou la création de filiales ou de médias associés à des groupes liés à des gouvernements étrangers. Les acteurs étatiques et non étatiques actuellement engagés dans de telles opérations sont conscients des limites et des contradictions posées par les règlements susmentionnés et en tirent parti.

4 **Limite pour établir une relation de cause à effet.** Les méthodologies techniques actuelles permettent de détecter les tentatives de désinformation et de les attribuer, avec plus ou moins de certitude, à des acteurs nationaux ou sous-nationaux spécifiques ayant l'intention de conditionner malicieusement le débat public dans un État.

Cependant, il est encore **très difficile de prouver une relation de cause à effet** entre les tentatives de modification de l'opinion publique et les changements de comportement des citoyens.

5 **Exploiter les vulnérabilités sociales existantes.** Les acteurs chargés de mener des actions de désinformation contre un État ne partent pas de zéro. Tout d'abord, ils détectent les vulnérabilités sociales et politiques réelles et spontanées qui apparaissent dans le débat public d'un État et s'attachent ensuite à **intensifier et à polariser ce débat.**

De cette manière, il est difficile d'accuser ces acteurs de provoquer des crises politiques ou sociales, car leur rôle est en fait de fausser le jeu, en faisant monter ou descendre en intensité des conflits préexistants, ou en introduisant de nouveaux facteurs pour en modifier le cours.

6 **Infiltration de la désinformation illégitime dans les méthodes de communication sociale et politique légitime.** La prolifération des actions de désinformation illégitimes menées par des acteurs désireux d'influencer les publics de citoyens dans les pays fait, en soi, partie de l'utilisation légitime que les acteurs politiques et sociaux font des nouvelles plateformes technologiques de diffusion massive d'informations pour distribuer leurs propres messages et contenus.

Dans ce scénario de conversations avec des milliers d'acteurs sur les réseaux sociaux et de conversations croisées sur des questions socialement ou politiquement controversées, le défi pour évaluer et réagir de manière appropriée aux campagnes de désinformation, en les annulant ou en les contrecarrant, est de **séparer le "grain de l'ivraie":** discerner quelles opinions et informations diffusées massivement sur les plateformes numériques font partie de la tentative légitime d'influence des acteurs sociaux, économiques ou politiques; et quelles autres utilisent les techniques d'influence et les nouvelles possibilités des réseaux sociaux à des fins d'ingérence malveillante.

Par exemple, le projet *Computational Propaganda* de l'Internet Institute de l'université d'Oxford[7], au Royaume-Uni, étudie "la manière dont les *bots,* les algorithmes et d'autres formes d'automatisation sont utilisés par les acteurs politiques dans les pays du monde entier", en partant du principe que les technologies d'automatisation font déjà partie des conversations politiques dans les démocraties également, et donc que la désinformation à des fins d'ingérence malveillante sera imbriquée dans cette réalité.

7. https://www.oii.ox.ac.uk/research/projects/computational-propaganda/

3.Objectif du guide

Aujourd'hui, le moyen le plus efficace de renforcer la résilience face à la désinformation est de protéger la principale cible des attaques de désinformation: les citoyens. Les habitants d'un État doivent disposer des ressources et développer **les compétences nécessaires pour identifier les produits et les plateformes de communication des outils de désinformation.**

Ces stratégies de désinformation seront couronnées de succès dans la mesure où leurs messages parviennent à être hégémoniques, assumés et partagés par les utilisateurs finaux qui, dans la plupart des cas, ignorent l'origine et la motivation véritables des sources d'information qu'ils consomment et partagent.

L'objectif de ce guide de bonnes pratiques est précisément d'expliquer les principales caractéristiques et la méthodologie des actions de désinformation actuelles, dans le but de fournir aux citoyens et aux utilisateurs finaux des médias numériques les outils qui leur permettent de consommer et de partager l'information de manière critique et d'éviter d'être les complices involontaires d'actions offensives contre les intérêts de l'État.

Il est nécessaire que les habitants d'un État disposent des ressources et développent les compétences nécessaires pour identifier les produits et les plateformes de communication qui sont caractéristiques des outils de désinformation.

4. What is the risk for Spain?

Plus de 20 millions de citoyens espagnols risquent d'être victimes de la désinformation.

Des pays comme l'Espagne ont déjà reconnu officiellement la menace que représente ce nouveau type d'action pour la sécurité. La **stratégie de sécurité nationale**[8], élaborée par le gouvernement espagnol en 2017, inclut explicitement la menace des actions hybrides comme l'un des principaux défis de sécurité auxquels le pays est confronté[9].

La stratégie de sécurité nationale de l'Espagne situe l'origine de ces nouvelles menaces dans un contexte sociopolitique et économique complexe et reconnaît également que ce type de menace peut provenir aussi bien d'"acteurs étatiques" que d'"acteurs non étatiques", et qu'ils combinent l'utilisation de "moyens militaires avec des cyberattaques, des éléments de pression économique ou des campagnes d'influence sur les réseaux sociaux"[10].

L'Espagne compte actuellement 27,6 millions d'internautes, dont 25,5 millions utilisent quotidiennement les réseaux sociaux. Les sources consultées indiquent que 92 % de la population espagnole âgée de 16 à 65 ans s'informe quotidiennement via Internet et que 85 % le font via les réseaux sociaux, selon les données de l'Observatoire national des télécommunications et de la société de l'information (ONTSI) en 2017[11].

8. GOUVERNEMENT D'ESPAGNE. Département de la sécurité intérieure. http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf
9. GOUVERNEMENT D'ESPAGNE. Op. cit., p. 16.
10. GOUVERNEMENT D'ESPAGNE. Op. cit., p. 32
11. OBSERVATOIRE NATIONAL DES TELECOMMUNICATIONS ET DU SI. 2018. Profil sociodémographique des utilisateurs d'Internet. Analyse des données de l'INE 2017. https://www.ontsi.red.es/ontsi/sites/ontsi/files/Perfil%20sociodemogr%C3%A1fico%20de%20los%20internautas%2 02017.pdf

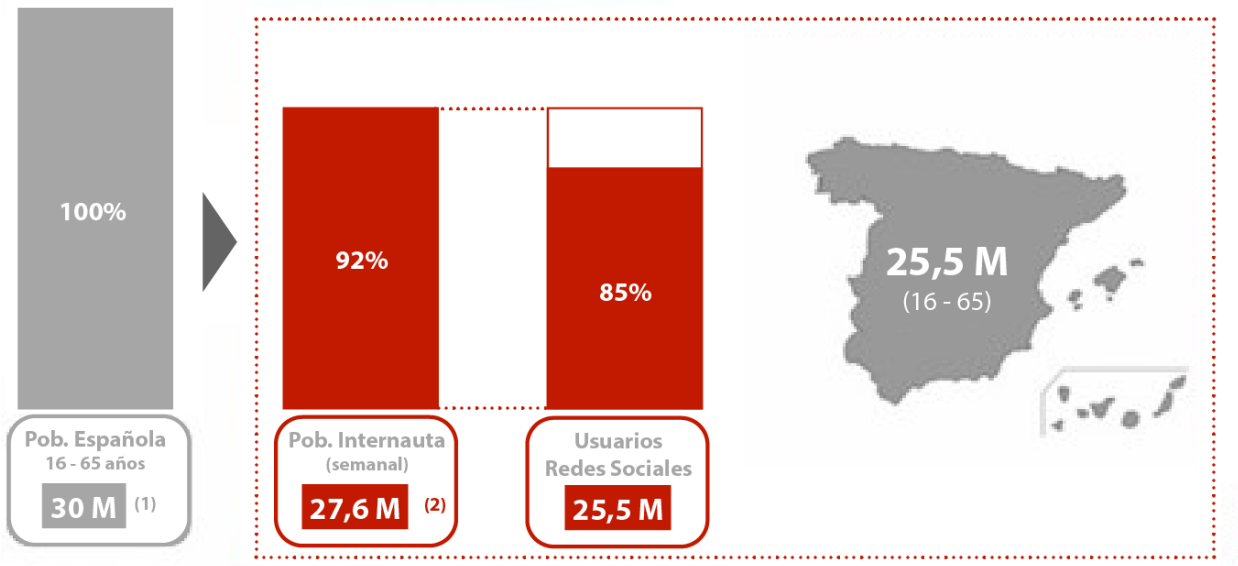


Illustration 1.- Graphique élaboré por l'Association de la publicité, du marketing et de la communication numérique en Espagne (IAB Espagne). Étude annuelle sur les médias sociaux 2018.

Selon les données de l'Asociación para la Investigación de Medios de Comunicación (AIMC), le principal usage que les citoyens espagnols font d'Internet est la lecture des actualités, comme l'ont déclaré 84,6% des personnes interrogées entre octobre et décembre 2017[12].

Ces études sur l'utilisation d'Internet et les habitudes de consommation d'informations numériques suggèrent qu'environ **90% de la population espagnole âgée de 16 à 65 ans pourrait potentiellement être victime d'une attaque de désinformation.** D'autres recherches récentes ont montré que, malgré l'utilisation répandue de l'internet et des réseaux sociaux parmi les citoyens espagnols, il existe encore un pourcentage important d'utilisateurs qui ne savent pas comment fonctionne la distribution des informations sur les plateformes numériques.

12. ASSOCIATION POUR LA RECHERCHE SUR LES MÉDIAS (AIMC). 2018. Surfeurs de la 20e édition sur le net. Enquête AIMC sur les utilisateurs d'Internet. (octobre-décembre 2017). https://www.aimc.es/otros-estudios-trabajos/navegantes-la-red/infografia-resumen-20o-navegantes-la-red/

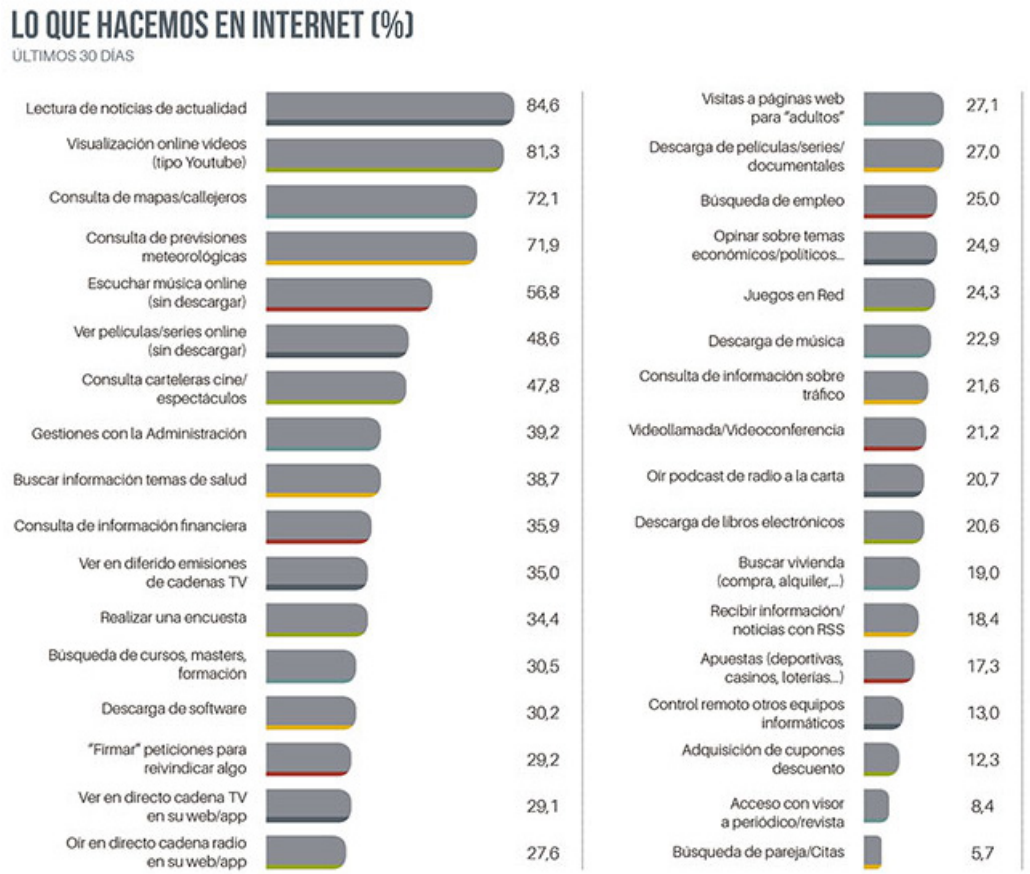


Illustration 2.- Illustration 2.- Graphique réalisé par l'Asociación para la Investigación de Medios de Comunicación (AIMC[13]).

Le "Digital News Report", réalisé en 2018 par l'Université d'Oxford et l'Université de Navarre, reconnaît par exemple qu'à peine trois utilisateurs numériques sur dix en Espagne savent que les nouvelles qu'ils lisent sur le réseau social Facebook dépendent d'un algorithme[14]. **Cette méconnaissance de l'environnement numérique de l'information est une vulnérabilité de l'opinion publique espagnole.**

13. Disponible sur https://www.aimc.es/otros-estudios-trabajos/navegantes-la-red/infografia-resumen-20o-navegantes-la-red/

14. UNIVERSITÉ DE NAVARRA/UNIVERSITÉ D'OXFORD. 2018. Digital News Report.ES 2018. Un public diversifié et préoccupé par la désinformation. Coordonné par Avelino Amoedo, Alfonso Vara-Miguel et Samuel Negredo. Center for Intenet Studies and Digital Life School of Communication et Reuters Institute for the Study of Journalism. https://drive.google.com/file/d/1_MqxpbPvMQM1IpvjsGm4QOKxIMC8IZ_D/view

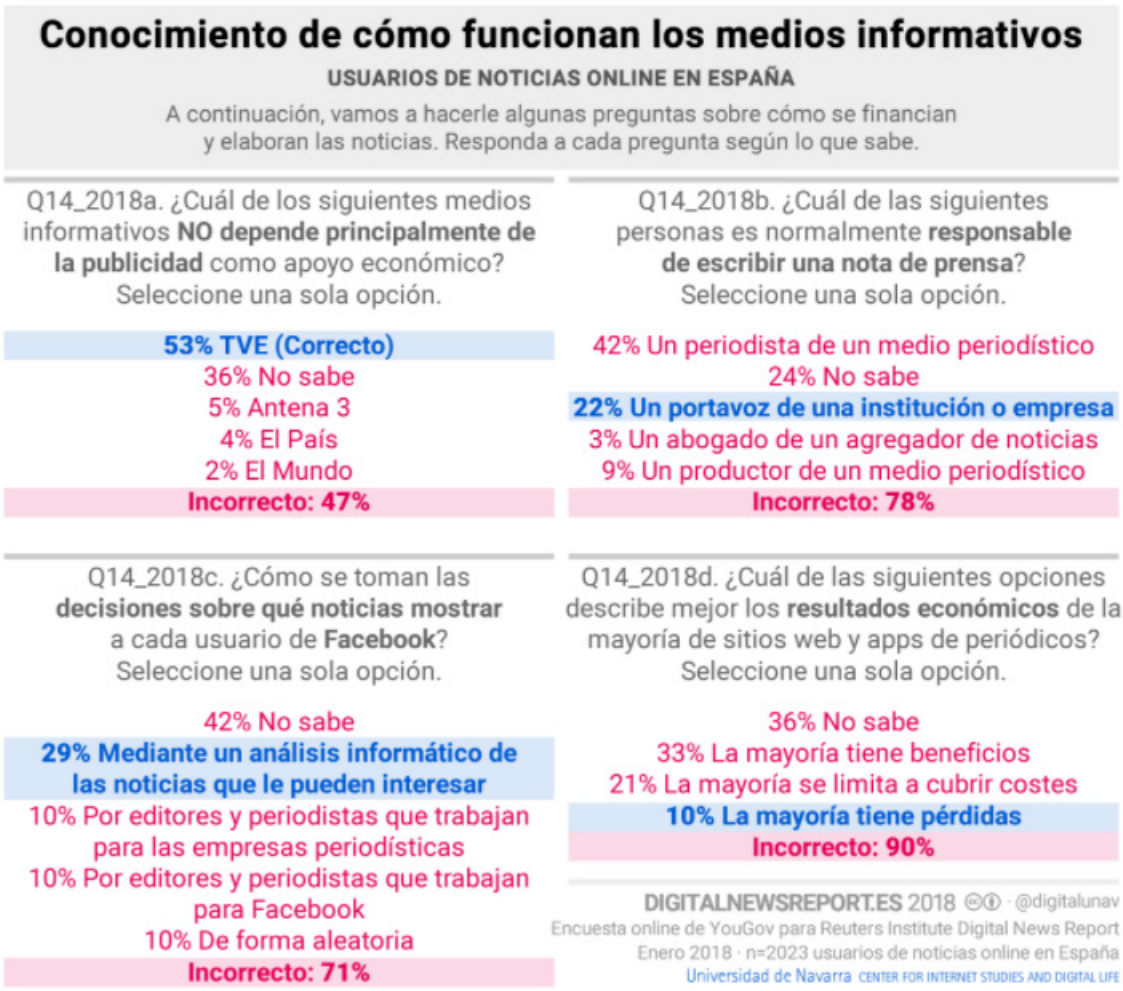


Illustration 3.- Reportage d'actualité numérique. EN 2018. Université de Navarre. Université d'Oxford[15].

15. Disponible sur: https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8IZ_D/view

5. Quelles sont les conséquences d'une attaque de désinformation?

Les conséquences d'une campagne systématique et malveillante de désinformation du public peuvent avoir des conséquences dangereuses pour une démocratie libérale.

L'objectif principal d'une campagne de désinformation est d'introduire dans le processus de formation de l'opinion publique d'un pays des fausses nouvelles, des demi-vérités, des informations hautement subjectives présentées comme factuelles **(confusion délibérée entre opinion et information)** et des informations conçues pour produire un effet émotionnel sur le destinataire, minimisant ainsi la probabilité qu'il les traite en exerçant un jugement critique.

Ces informations sont diffusées à partir de plateformes et de profils qui semblent crédibles, mais qui dissimulent leur véritable origine et rendent leur traçabilité difficile. La diffusion malveillante et systématique d'informations de mauvaise qualité dans le débat public vise à briser la confiance entre les citoyens d'un pays et deux (2) des principaux acteurs chargés de maintenir la cohésion sociale: les institutions et les médias.

L'État-nation moderne est sous-tendu par un **contrat social fondé sur la confiance que les citoyens placent dans son administration et ses institutions.** La rupture de cette relation de confiance peut compromettre la solidité du tissu démocratique d'un État. En ce sens, les conséquences d'une campagne systématique et malveillante de désinformation du public peuvent avoir des conséquences dangereuses pour une démocratie libérale.

5.1 La perte de confiance dans les médias traditionnels

Les citoyens européens, et en particulier les Espagnols, font de moins en moins confiance aux médias, comme en témoigne une enquête menée en 2018 par le baromètre Eldman Trust, qui conclut que seuls 44% des Espagnols[16] maintiennent leur confiance dans les médias.

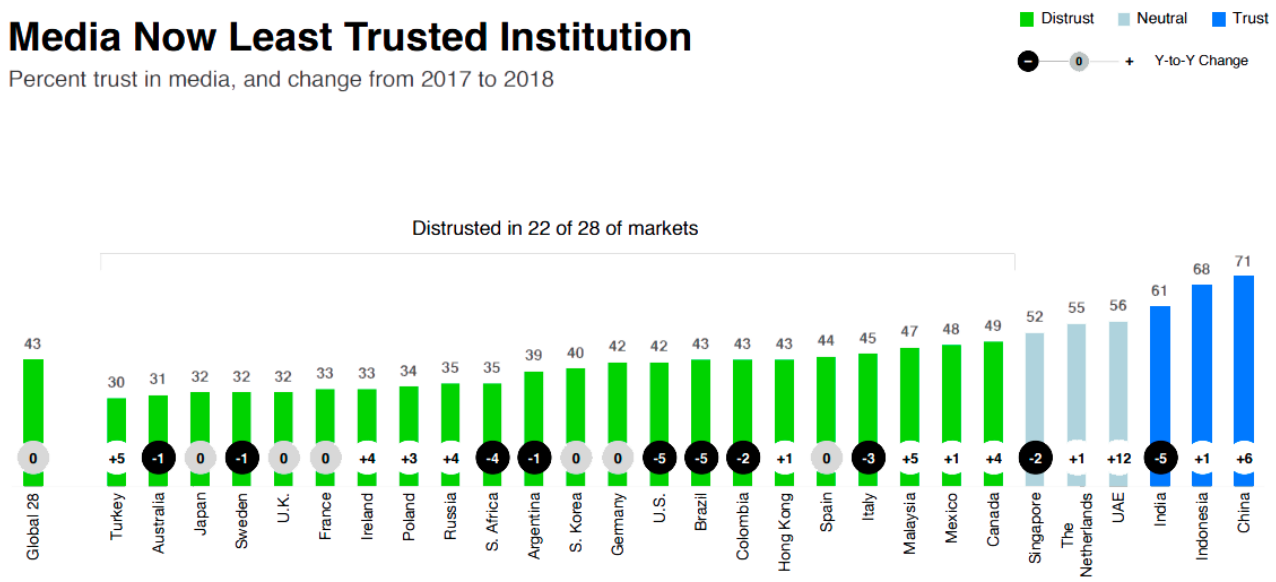


Illustration 4.- Graphique produit par le Baromètre de confiance Edelman[17].

16. EDELMAN. 2018. "2018 Edelman Trust Barometer. Global Report". https://www.edelman.com/sites/g/files/aatuss191/files/201810/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
17. Disponible sur: https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

5.1 La perte de confiance dans les médias traditionnels

Jusqu'à la fin du XXe siècle, les médias traditionnels ont joué le rôle de médiateurs dans le processus de formation de l'opinion publique. Ce sont des agents identifiés et crédibles qui créent et transmettent des messages qui fixent l'agenda et façonnent le débat public et, par conséquent, la cohésion sociale d'un État.

Ce chiffre coïncide avec les données de l'étude conjointe susmentionnée de l'université de Navarre et de l'université d'Oxford, qui indique également que seuls 44% des internautes espagnols font confiance aux informations qu'ils lisent dans les médias[18].

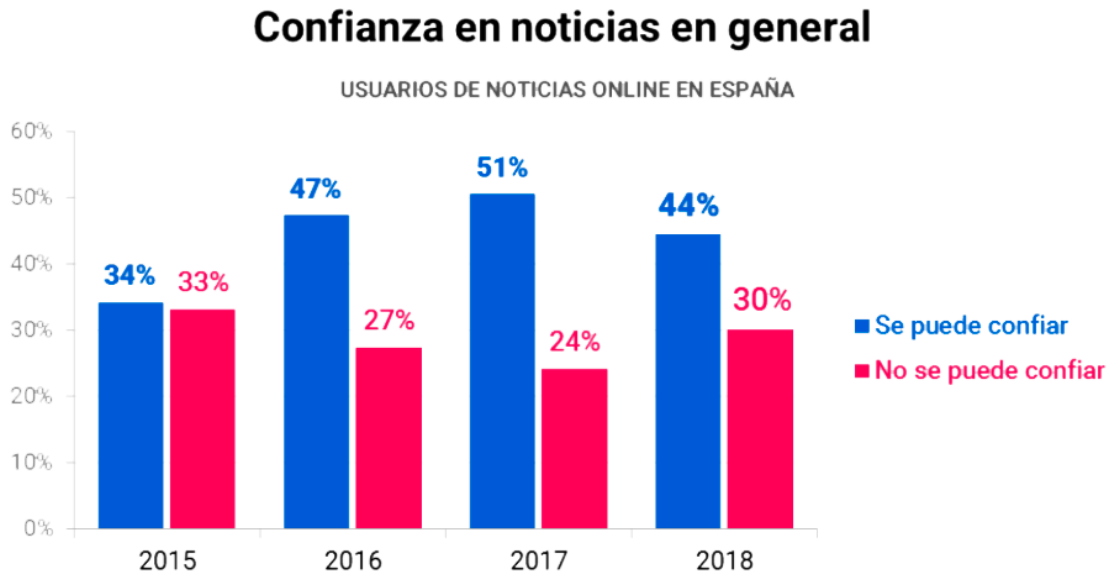


Illustration 5.- Rapport d'actualité numérique.ES 2018. Université de Navarre. Université d'Oxford.[19].

Le déclin de la confiance du public dans les médias peut s'expliquer par des mécanismes historiques de causalité dans lesquels interviennent de nombreux facteurs structurels, liés à l'évolution des sociétés, de la politique, de la technologie, de la génération et de la transmission de l'information, ainsi qu'à la révolution à laquelle est confrontée la pratique journalistique elle-même.

18. UNIVERSITÉ DE NAVARRA/UNIVERSITÉ D'OXFORD. 2018. Digital News Report.ES 2018. Un public diversifié et préoccupé par la désinformation. Coordonné par Avelino Amoedo, Alfonso Vara-Miguel et Samuel Negredo. Center for Intenet Studies and Digital Life School of Communication et Reuters Institute for the Study of Journalism. https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8IZ_D/view
19. Disponible sur: https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8IZ_D/view

5.1 La perte de confiance dans les médias traditionnels

Ce scénario **d'évolution de l'opinion publique vers la crédibilité des médias** est exploité par des stratégies offensives de désinformation pour se multiplier et générer une instabilité de l'opinion publique.

Selon le rapport susmentionné de l'université de Navarre et de l'université d'Oxford, l'Espagne est l'un des pays du monde où les internautes craignent le plus d'être victimes de campagnes de désinformation numérique. Plus précisément, **69% des utilisateurs d'Internet reconnaissent être préoccupés par le fait qu'ils ne savent pas comment faire la différence entre ce qui est vrai et ce qui est faux sur Internet[20].** Le rapport Edelman souligne également que l'Espagne est l'un des pays au monde où le nombre d'internautes préoccupés par les fausses nouvelles en ligne est le plus élevé[21].

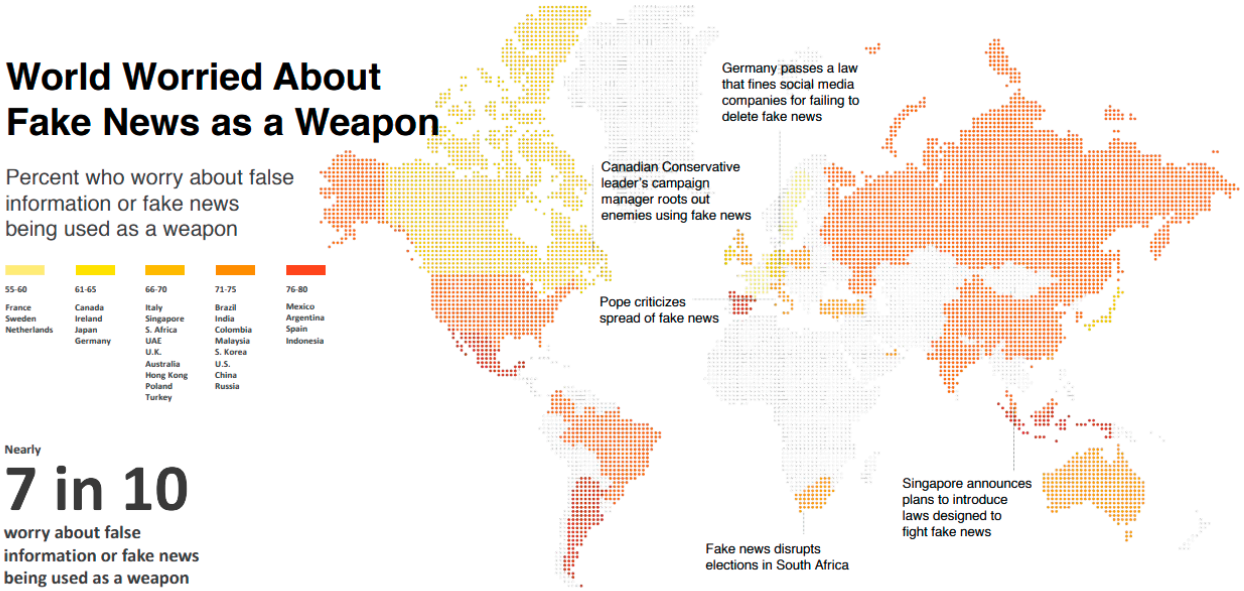


Illustration 6.- Graphique produit par le Baromètre de confiance Edelman [22]

20. Ibid.
21. EDELMAN. 2018. "2018 Edelman Trust Barometer. Global Report". https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
22. Disponible sur: https://www.edelman.com/sites/g/files/aatuss191/files/2018- 10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

5.1 La perte de confiance dans les médias traditionnels

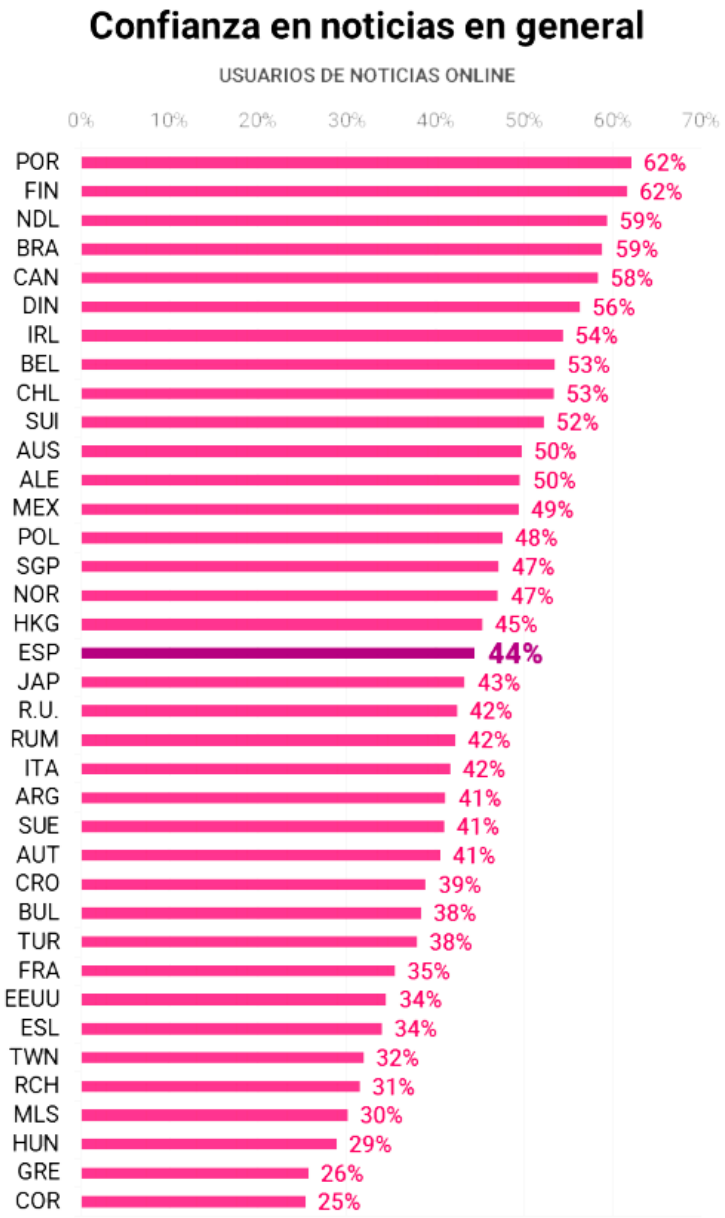


Illustration 7.- Reportage d'actualité numérique. ES2018. Université de Navarre. Université d'Oxford[23].

Enfin, l'Eurobaromètre de l'Union européenne de décembre 2018 a révélé que 83% des citoyens européens considèrent les fake news comme une menace réelle pour la démocratie, tandis que 73% sont préoccupés par les campagnes de désinformation numérique en période préélectorale[24].

23. Disponible sur: https://drive.google.com/file/d/1_MqxpbPvMQM1IpvjsGm4QOKxlMC8IZ_D/view
24. COMMISSION EUROPÉENNE. 2018. Plan d'action contre la désinformation. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=55907

5.2 La perte de confiance dans les institutions publiques

Tout porte à croire que les campagnes de désinformation profitent de la crise sociale de confiance dans les médias pour s'installer et se propager plus facilement. Toutefois, il est encore plus inquiétant de constater que la confiance des citoyens dans les institutions publiques de leur pays atteint également des niveaux historiquement bas.

Dans le cas de l'Espagne, seuls 24% des citoyens font confiance à leurs institutions gouvernementales, selon le rapport Endelman[25]. L'un des principaux objectifs des campagnes de désinformation est précisément de **détecter les points de vulnérabilité du contrat social d'un pays et de les renforcer afin** d'accroître la méfiance entre les citoyens et les institutions publiques.

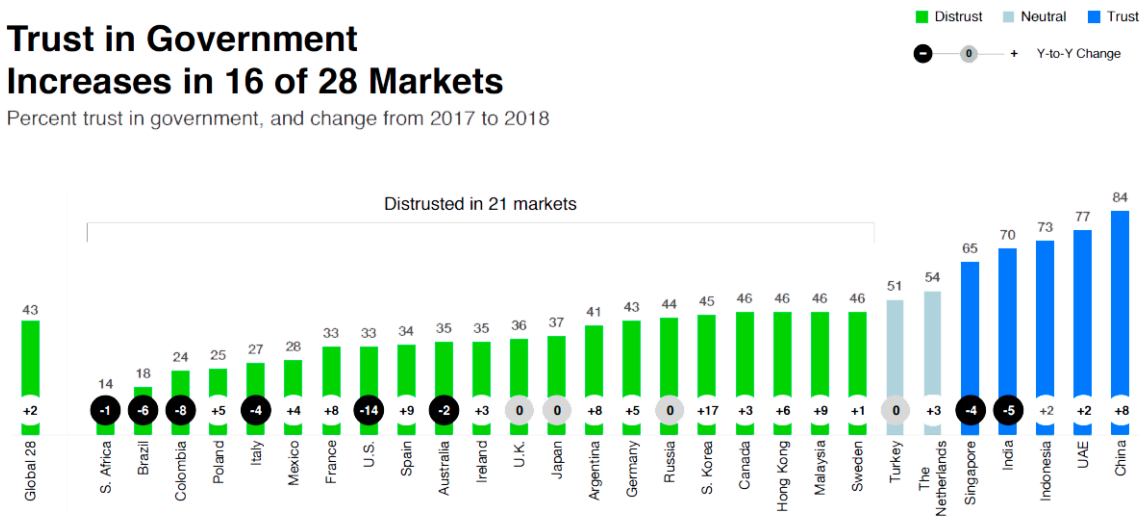


Illustration 8 - Graphique produit par le Baromètre de confiance Edelman [26]

25. EDELMAN. 2018. "2018 Edelman Trust Barometer. Global Report". https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
26. Disponible sur: https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

5.3 La perte de confiance dans la souveraineté du citoyen

En ce qui concerne la crise de confiance dans les médias traditionnels et l'érosion de la confiance dans les institutions publiques démocratiques, certaines stratégies de désinformation peuvent chercher à déstabiliser le fondement même de ces deux phénomènes: **la confiance des démocraties dans le fait que le citoyen le mieux informé sera capable de prendre les meilleures décisions pour leur gouvernance.**

Cette ligne d'action désinformatrice vise à **saper la confiance des citoyens dans l'essence de l'information comme élément de la prise de décision démocratique.** D'une part, si elle parvient à semer et à faire germer le sentiment que les médias traditionnels ne sont pas crédibles et que, d'autre part, seules des informations poubelles ou de mauvaise qualité circulent sur les réseaux sociaux (ce qui est également utilisé par des pays étrangers pour influencer le sens du vote lors d'élections démocratiques), elle tentera d'installer chez les citoyens le sentiment qu'il n'y a aucun moyen d'obtenir des informations de qualité pour établir un jugement de valeur afin de prendre leurs décisions de vote et, par conséquent, leurs décisions de gouvernance.

Lors de l'analyse des campagnes de désinformation, notamment celles attribuées à des pays étrangers ayant des intérêts géo-économiques ou géopolitiques, il est de **bonne pratique d'examiner dans quelle mesure on tente de saper la confiance des citoyens dans les médias** (presse écrite, médias sociaux, plateformes numériques), plutôt que de se demander si l'intention est de polariser la conversation sur des questions sociales ou politiques dans des directions fallacieuses.

Par exemple, si un État aux intentions malveillantes parvient à faire la une des journaux et des analyses académiques dans le monde entier qui lui attribuent la capacité de manipuler les citoyens et d'influencer les processus démocratiques dans une grande partie des scénarios électoraux des pays de n'importe quel continent, l'un des effets générés est que le pouvoir et les capacités d'exercer cette influence sont attribués à cet État malveillant.

Les citoyens peuvent en déduire qu'ils sont moins en mesure de s'informer légitimement pour décider de leur démocratie, étant donné qu'un État étranger manipule les réseaux sociaux dans un scénario où la confiance dans la presse et les institutions a également diminué.

5.3 La perte de confiance dans la souveraineté du citoyen

Ainsi, le défi de **contrer et d'annuler les campagnes de désinformation** est au moins quintuple

1. Détecter et combattre les tentatives d'influence illégitime sur des questions spécifiques de polarisation sociale et politique.
2. Analyser correctement ces tentatives illégitimes pour les distinguer des processus d'influence politique et sociale des acteurs légitimes.
3. Contextualiser correctement les attributions d'intentions et de capacités des acteurs ayant des objectifs de désinformation, afin d'encadrer correctement la petite ou grande dimension de ces acteurs dans la communication de masse et transmédia globale qui a déjà lieu dans tout processus démocratique.
4. Mener des campagnes pour informer les citoyens sur la désinformation, ses intentions et sa portée, ainsi que sur les tentatives de certains acteurs de faire croire au public qu'ils peuvent exercer une "manipulation totale" sur l'opinion publique, alors qu'ils n'ont pas les ressources ou souvent des intentions aussi ambitieuses.
5. Introduire de bonnes pratiques dans l'analyse académique ou médiatique pour, en décrivant les tentatives de campagnes de désinformation sur les médias sociaux, dimensionner correctement la portée que ces campagnes peuvent avoir et comment ces campagnes malveillantes partagent l'espace avec d'autres informations légitimes qui, dans la plupart des cas, sont celles qui atteignent le citoyen en plus grande quantité et qualité.

5.4 Polarisation sociale

La nature même des plateformes d'information numériques, qui utilisent des algorithmes pour sélectionner de manière personnalisée les nouvelles qu'elles considèrent comme étant au goût de l'utilisateur, contribue à la création de conversations numériques hautement polarisées. Les campagnes de désinformation cherchent précisément à accroître cette polarisation.

Tout d'abord, en détectant les conversations numériques les plus controversées ou les plus conflictuelles dans le débat public et, de manière malveillante, en encourageant et en amplifiant ces débats afin d'opposer les citoyens d'un pays sur certaines questions politiques ou sociales.

Une étude du MIT Social Machines Lab sur les conversations numériques (chats) lors de la campagne électorale américaine de 2016 a détecté des taux élevés de polarisation autour de deux communautés politiques: l'une en faveur de Donald Trump et l'autre en faveur d'Hillary Clinton. Le

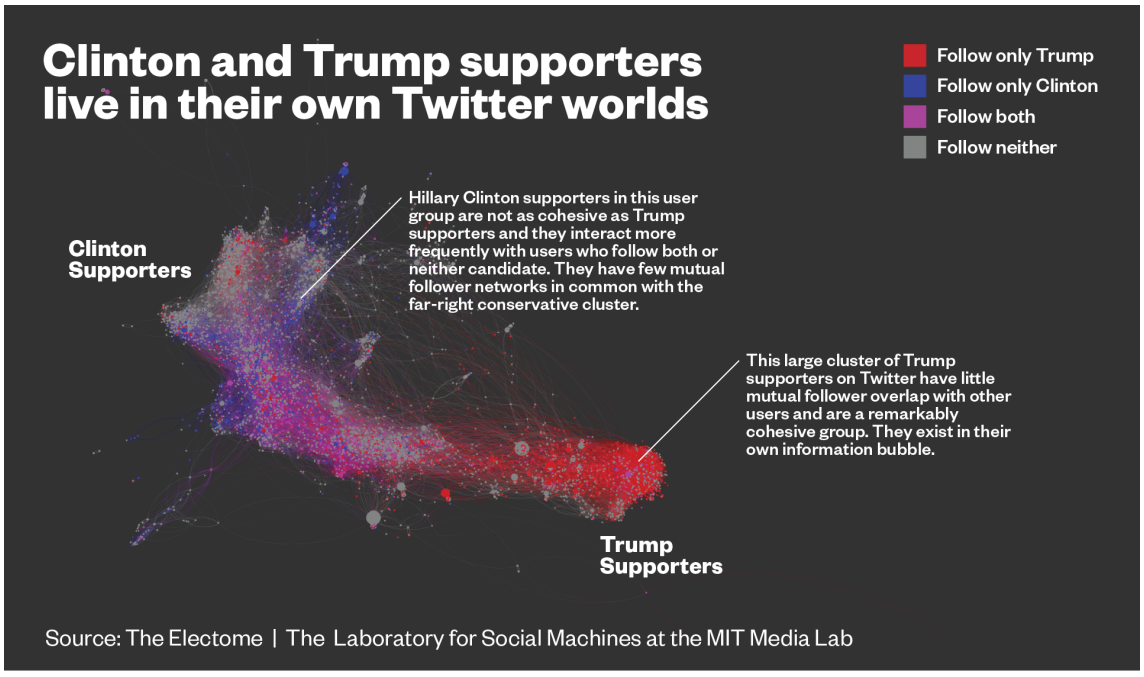


Illustration 9.- Graphique produit par Vice News. 8 décembre 2016 avec des données provenant des Machines sociales du MIT Media Lab[27].

27. Diposnible sur: https://news.vice.com/en_us/article/d3xamx/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows

débat entre ces deux communautés dans l'environnement numérique était pratiquement inexistant et la conversation n'a fait que contribuer à radicaliser les positions des membres de chacune de ces communautés. Actuellement, les autorités judiciaires et le Congrès américain lui-même analysent si des pays étrangers ont utilisé cette polarisation pour accroître la tension sociale et éroder malicieusement la cohésion interne du pays.

De même, une étude menée par la société espagnole Alto Analytics a montré que le débat numérique sur l'immigration lors de la campagne pré-électorale italienne de 2017 a également montré que la société italienne était fortement polarisée autour de deux communautés qui interagissaient à peine entre elles.

La même étude a fourni des indications selon lesquelles les médias étrangers et d'autres acteurs non identifiés pourraient avoir contribué à accroître cette division dans la société italienne par le biais de campagnes de désinformation systématiques[28].

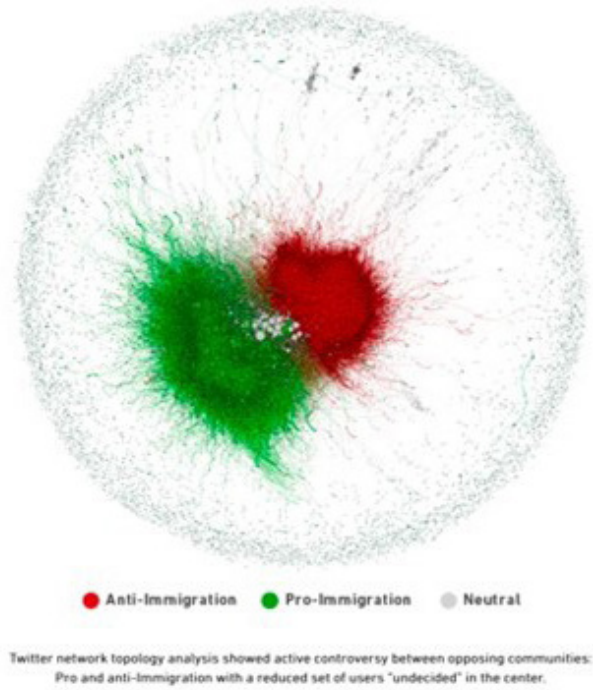


Illustration 10.- Graphique élaboré par Alto Analytics[30].

28. VICE NEWS. 2016. Parallel narratives. ClilInton and Trump supporters really don´t listen to each other on Twitter. Alex Thompson. 8 diciembre 2016. https://news.vice.com/en_us/article/d3xamx/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows
29. ALTO ANALYTICS. 2017. The Construction of Anti-immigration electoral messages in Italy. The role of foreign media in the anti-immigration debate one year before the 2018 election. https://www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/
30. Disponible en: https://www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/

6. La méthodologie des campagnes de désinformation

This methodology is based on a combination of different disciplines, such as sociology, politics, literature, journalism and technology.

Les actions de piratage, de manipulation ou de perturbation de l'opinion publique par des actions de désinformation suivent un schéma constant, tant dans les actions offensives des États-nations que dans celles des groupes subnationaux. Cette méthodologie est basée sur une combinaison de différentes disciplines, telles que la sociologie, la politique, la littérature, le journalisme et la technologie.

Les quatre (4) étapes nécessaires à la mise en œuvre d'une campagne de perturbation numérique et de communication réussie pour déstabiliser l'opinion publique d'un État sont les suivantes:

6. La méthodologie des campagnes de désinformation

1 **Analyse et détection des vulnérabilités sociales et politiques d'un pays.**

Les actions de désinformation reposent sur l'exploitation du terreau de questions qui, dans la dynamique interne d'un pays, génèrent déjà des confrontations dans l'opinion publique.

L'altération de l'opinion publique ne consiste pas à créer de nouvelles confrontations dans la politique intérieure du pays considéré comme un adversaire. Au contraire, cette stratégie vise à alimenter les débats et les confrontations politiques qui existent déjà et qui polarisent une société.

Dans le cas des États-Unis, la perturbation communicationnelle générée, prétendument par la Russie, a alimenté les débats politiques et sociaux existants. Pour sa part, DAESH a mené une analyse sociale et politique approfondie des communautés sunnites en Irak et en Syrie dans le but de détecter et d'exploiter les principales vulnérabilités de ces États et de proposer un récit visant à générer un nouveau contrat social avec les citoyens sunnites de ces pays.

2 **Création de récits transmédias.**

Une fois que les espaces d'un pays où se produisent des scénarios de confrontation sociale ou politique ont été détectés, les responsables d'une action perturbatrice de désinformation créent des scripts et des récits transmédias efficaces, capables de générer une résonance culturelle et une mobilisation parmi leurs publics potentiels.

Ces récits sont conçus pour être distribués à travers différents caractères, formats et plateformes de communication, en s'adaptant aux particularités culturelles et esthétiques des groupes cibles.

3 **Création d'un réseau de ressources propres.**

Depuis la première décennie du XXIe siècle, la distribution de contenu de marketing numérique repose sur une stratégie à trois volets appelée "owned media, paid media et earned media". Il existe un consensus général dans le secteur de la communication selon lequel la combinaison de ces trois (3) éléments constitue la base d'une diffusion efficace du contenu d'une campagne de marketing.

Les médias propriétaires désignent les plateformes et les canaux de communication qu'une marque ou un produit crée pour communiquer directement avec ses publics; les médias payés désignent les publicités et les espaces que la marque insère dans d'autres canaux

de communication en échange d'une compensation financière; et les médias gagnés désignent les informations, commentaires ou communications non rémunérés que les utilisateurs et les influenceurs font sur la marque.

Les récits construits pour canaliser et alimenter les conflits socio-économiques et politiques d'un État sont introduits dans le débat numérique par le biais d'un réseau de médias propres contrôlés hiérarchiquement par les responsables d'un mécanisme de perturbation à des fins de désinformation.

4 **Création de canaux de distribution automatisés.**

La dernière étape de la disruption est la distribution directe, automatisée et segmentée de récits, destinés à des publics potentiels dans des environnements numériques.

Pour cela, les responsables de l'action communicative ont des stratégies dans les réseaux sociaux de comptes automatisés (bots) qui diffusent des messages avec une grande ampleur et segmentation, sans attendre que l'utilisateur atteigne volontairement la plateforme où le contenu est publié.

L'existence de ces outils de distribution automatisés a été démontrée dans des cas d'ingérence d'acteurs étatiques[30], ainsi que les acteurs non étatiques[31].

31. Javier. "Pourquoi les médias sociaux russes ont-ils envahi la conversation numérique sur l'indépendance de la Catalogne?" [en ligne], dans Washington Post. 22 noviembre 2017. Disponible sur web: https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/?noredirect=on&utm_term=.126764742aa3.
32. BERGER, J.M.; MORGAN, Jonathon. «The ISIS Twitter Census. The Brookings Project on U.S. Relations with the Islamic World» [en línea], en Brookings, Analysis Paper. N.º 20. Marzo 2015. Disponible en web: https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

7. Les 10 éléments clés d'une campagne de désinformation

La Commission européenne identifie le phénomène de la désinformation aux fake news. Selon cette institution, "*la désinformation ou les fake news consistent en des informations manifestement fausses ou incorrectes qui sont préparées, présentées et diffusées à des fins de gain financier, pour tromper malicieusement le public ou pour causer un préjudice*".

Cette définition rend très clairement compte de la nature des actions de communication offensive. Cependant, il est également évident que les fake news ne sont qu'un outil de plus dans le mécanisme complexe d'une campagne de désinformation.

Les actions de communication offensive sont des phénomènes complexes qui utilisent différents outils et procédures (pas seulement les fake news) pour atteindre les citoyens avec des messages qui provoquent le chaos et la confusion dans l'opinion publique d'un pays considéré comme un adversaire.

Dans ce qui suit, nous allons identifier certains des outils les plus couramment utilisés dans les campagnes de désinformation. Les deux (2) premières techniques sont liées à la création de contenu ou de récits et les huit (8) suivantes sont liées au processus de distribution du contenu (par les médias, les réseaux sociaux ou les algorithmes).

Les actions de communication offensive sont des phénomènes complexes qui utilisent différents outils et procédures pour atteindre les citoyens avec des messages qui provoquent le chaos et la confusion.

33. COMISIÓN EUROPEA. 2018. "Fake News and Online Disinformation". https://ec.europa.eu/digital-single-market/en/fake-news-disinformation

7.1 Fake news

Les fausses nouvelles peuvent être acceptées comme crédibles ou crédibles par un grand nombre de citoyens et peuvent provoquer de graves crises politiques et de sécurité dans un État.

Les fake news sont des messages informatifs diffusés au public qui ne correspondent à aucun fait vrai ou scientifiquement ou historiquement démontrable. Malgré leur absence de rapport avec la vérité, les fake news peuvent être acceptées comme crédibles ou plausibles par un grand nombre de citoyens et peuvent provoquer de graves crises politiques et sécuritaires dans un État.

L'acceptation de ce type de nouvelles comme vérité est due aux caractéristiques suivantes:

- **Ils sont basés sur des éléments réels.** Ces nouvelles sont basées sur un personnage, un lieu ou un phénomène réel.
- **Ils sont surprenants.** Ces nouvelles sont présentées au lecteur de manière très attrayante et sensationnaliste, généralement avec des titres provocateurs ou surprenants, qui invitent le lecteur à les lire.
- **Ils proviennent de supports récemment créés ou de supports dont la traçabilité est faible.** Les fake news sont à l'origine diffusées par des médias inconnus, soit parce qu'ils sont nouvellement créés (créés ad-hoc pour initier des actions de ce type), soit parce qu'ils proviennent de pays étrangers où il est difficile d'enquêter sur l'origine et la traçabilité des médias.
- **Manque de sources.** Les fausses nouvelles sont rapportées dans des textes où aucune source fiable ou reconnue n'est identifiée ou mentionnée. Si une source est présentée, c'est uniquement pour donner la parole à ceux qui réaffirment la théorie de l'information et aucune possibilité d'expression n'est donnée aux voix ou aux pensées qui remettent en question la thèse maintenue dans l'information.

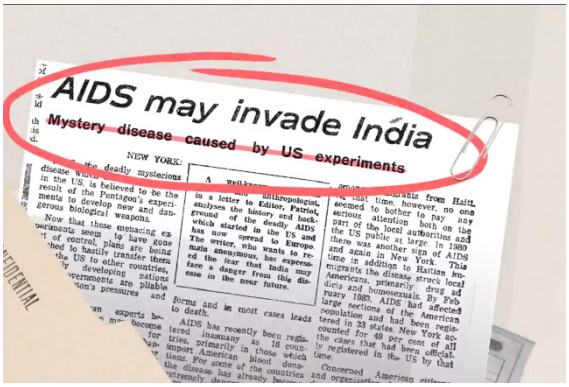
7.1 Fake news

Ils misent sur le long terme. Les fausses nouvelles peuvent avoir un impact à court terme, mais elles peuvent aussi développer leur capacité offensive à long terme. Parfois, les fausses nouvelles sont publiées dans un média inconnu dans un pays étranger, dans l'espoir qu'au fil du temps, elles entrent dans la chaîne de distribution des médias plus fiables et acquièrent un semblant de crédibilité.

De même, ces informations publiées dans des médias inconnus peuvent finir par être citées dans des recherches universitaires ou sur des sites web de référence largement utilisés (tels que Wikipedia) et ainsi, après des mois ou des années, acquérir une apparence de crédibilité et contaminer le processus de formation de l'opinion publique.

L'une des opérations de désinformation les plus réussies utilisant des fake news est l'opération "Infektion"[34]. Cette campagne a été lancée par le gouvernement russe au début des années 1980 dans le but de faire passer le message que le virus du sida avait été créé par le gouvernement américain pour éliminer sa population afro-américaine et homosexuelle. L'histoire a été publiée pour la première fois en juillet 1983 dans un journal local inconnu en Inde et est passée presque inaperçue.

Au fil du temps, cependant, l'histoire a été citée et mentionnée par des médias d'autres pays, jusqu'à ce que, le 30 mars 1987, la chaîne américaine CBS reprenne l'histoire dans une émission en prime-time et transforme une fausse nouvelle, créée quatre ans plus tôt par les services de renseignement soviétiques en Inde, en un sujet de débat public et politique aux États-Unis.


AIDS may invade India

Mystery disease caused by US experiments

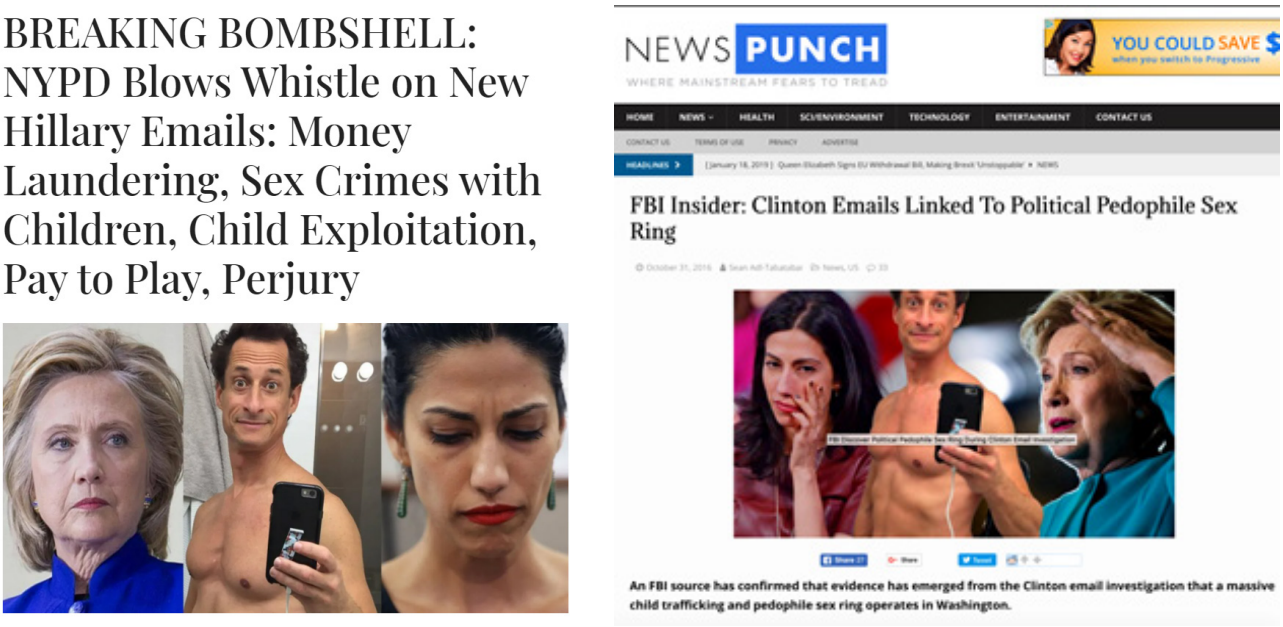
NEW YORK:

Illustration 11.- Article original publié en Inde en juillet 1983 rapportant que le SIDA a été créé par le gouvernement américain.

34. NEW YORK TIMES. 2018. "Operation Infektion. Russian Disinformation: from Cold War to Kanye", by Adam B. Ellick and Adam Westbrook. https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html

Une réussite plus récente, fin octobre 2016, où des comptes Facebook anonymes et des médias peu crédibles ont commencé à diffuser la nouvelle selon laquelle la candidate démocrate à la présidentielle américaine Hillary Clinton faisait partie d'un réseau sexuel d'enfants basé dans une pizzeria bien connue de Washington.

Cette information s'est rapidement répandue et des milliers de citoyens y ont prêté foi. En fait, à peine un mois après la publication de cette histoire, un citoyen américain est entré dans le restaurant avec une arme et a commencé à tirer pour tenter de libérer les enfants prétendument exploités sexuellement[32].



Captures d'écran de certains des médias qui ont diffusé les fausses nouvelles fin octobre 2016 sur les relations d'Hillary Clinton avec un réseau présumé de pédophilie[36].

Un autre exemple de fake news, portant dans ce cas sur l'actualité espagnole, s'est produit le 28 octobre 2017, lorsque le média RT News, basé en Russie, a publié un titre annonçant la présence de chars dans les rues de Barcelone (l'histoire a été partagée sur Facebook par 11 800 utilisateurs).

35. ROLLING STONE. 2017. "Anatomy of a Fake News Scandal", by Amanda Robb. https://www.rollingstone.com/politics/politics-news/anatomy-of-a-fake-news-scandal-125877/
36. La nouvelle est toujours disponible sur internet aux liens: https://newspunch.com/fbi-clinton-email-pedophile-ring/ https://truepundit.com/breaking-bombshell-nypd-blows-whistle-on-new-hillary-emails-money-laundering-sex-crimes-with-children-child-exploitation-pay-to-play-perjury/

"Tanques en las calles de Barcelona": España y Cataluña al borde de un desenlace violento

Publicado: 28 oct 2017 02:56 GMT

El analista político John Wight considera que el movimiento separatista está siguiendo un camino peligroso, en medio de la determinación de Madrid de "desatar la violencia".

Capture d'écran de l'information publiée par RT News suggérant la présence de chars dans les rues de Barcelone en octobre 2017[37].

Illustration 14.- Capture d'écran de deux profils numériques désinformateurs sur Twitter affirmant que des miliciens étrangers "assassinent des innocents" dans les rues de France pendant la crise des Gilets jaunes.

37. Disponible sur: https://actualidad.rt.com/actualidad/253812-espana-cataluna-violencia-conflicto

7.1.1 Fake news profondes

Dans le cadre du phénomène des fake news, il est important de souligner l'évolution et la popularisation de ce que l'on appelle les deep fake news. Il s'agit d'une technologie qui peut ajouter encore plus de complexité et de capacité offensive à cette technique. Elle consiste à utiliser un logiciel pour créer de véritables images vidéo d'autorités et d'hommes politiques, mais avec des sons et des mouvements de bouche modifiés.

De cette manière, il est possible de diffuser des discours ou des déclarations d'autorités publiques qui semblent réels, mais dont le message est totalement ou partiellement falsifié.

7.2 L'approche

Les inclinaisons manipulent les perceptions qui peuvent être générées par les titres et les photographies de l'information.

Les campagnes de désinformation ne reposent pas uniquement sur des contenus erronés. À d'autres moments, les informations diffusées de manière malveillante sont basées sur un fait réel, mais sont présentées au public avec une approche élaborée et construite de telle sorte que l'utilisateur final interprète ce fait d'une manière qui ne coïncide pas avec la réalité.

Les inclinaisons manipulent les perceptions qui peuvent être générées par les titres et les photographies de l'information, ce que l'on appelle le "premier niveau de lecture" d'un reportage. Ce premier niveau de lecture attire non seulement la première attention de l'utilisateur, mais, avec les habitudes actuelles de consommation de l'information sur les appareils mobiles, c'est souvent la seule information reçue d'une actualité.

Un exemple de ce type de désinformation est la nouvelle publiée le 1er octobre 2017 sur la chaîne d'information russe RT News dans sa version espagnole. La dépêche portant le titre suivant: "Vidéos fortes : répression policière brutale contre les électeurs du référendum catalan" est un exemple de ce type de désinformation.

FUERTES VIDEOS: La brutal represión de la Policía contra los votantes del referéndum catalán

Publicado: 1 oct 2017 12:18 GMT

Los oficiales han irrumpido en numerosos centros de votación y han disparado balas de goma y utilizado otros medios violentos contra las multitudes de votantes.

Illustration 15.- Information publiée par RT News le 1er octobre 2017[38].

Le titre est accompagné de la photo d'une personne allongée sur le sol, les yeux fermés, avec une plaie sanguinolente pixellisée sur le front. A aucun moment le texte ne ment explicitement avec l'information, il ne peut donc pas être présenté comme un cas de fake news. La photo est réelle et montre une personne blessée lors d'une confrontation avec la police pendant la célébration du référendum illégal sur l'indépendance en Catalogne.

Cependant, le premier niveau de lecture, composé du titre ("vidéos fortes, répression brutale") et de la photographie (une personne allongée les yeux fermés et avec une plaie saignante sur le front) peut amener le lecteur à la conclusion qu'il y a eu des personnes tuées durant le 1er octobre 2017 en Catalogne (la nouvelle a été partagée par 22.800 personnes sur Facebook en janvier 2018).

38. Disponible sur: https://actualidad.rt.com/actualidad/251682-represion-brutal-policia-espa%C3%B1ola-referendum-catalan

7.3 Nouveaux médias

Les nouveaux médias servent de plateformes pour la publication initiale d'informations malveillantes.

Le phénomène des fausses nouvelles a connu une popularité exponentielle au début du 21e siècle en raison de la facilité et de l'efficacité avec lesquelles des acteurs intéressés, des acteurs politiques clandestins ou des pays étrangers peuvent créer des médias et des plateformes de communication d'apparence professionnelle et crédible dans une variété de langues.

Ces nouveaux médias servent de plateformes pour la publication initiale d'informations malveillantes et peuvent, en quelques jours ou mois, rivaliser en influence avec des médias établis depuis des décennies dans l'opinion publique d'une société.

Ils partagent souvent certaines des caractéristiques suivantes:

- Création récente et absence de trajectoire professionnelle reconnue.
- Absence de signature sur les nouvelles.
- Manque d'informations sur les responsables du contenu éditorial et sur les gestionnaires financiers ou les actionnaires.
- Manque d'informations sur le siège physique de l'entreprise.
- Liés à des gouvernements étrangers, qui cachent leur relation gouvernementale et tentent même d'imiter les médias locaux ou nationaux afin de créer la confusion.

Les médias de qualité mettent en œuvre des mesures pour se différencier des nouvelles plateformes numériques visant à diffuser des campagnes de désinformation. L'un de ces projets est le *"Trust Projet"*, auquel plusieurs médias du monde entier, ainsi que des institutions universitaires, ont adhéré.

7.3 Nouveaux médias

Ce projet établit huit (8) indicateurs de confiance qui garantissent que le processus de production et de diffusion de leurs informations est régi par des critères de qualité et de confiance[39].

- **Meilleures pratiques:** Quels sont les principes du média, qui le finance, quelle est sa mission? Il s'agit également d'inclure le code d'éthique, l'engagement en faveur de la diversité, la rigueur, les corrections et d'autres normes.
- **Expertise journalistique:** Qui a écrit cet article? Informations sur l'auteur, notamment son parcours et ses articles publiés.
- **Type de travail:** A quel genre de journalisme appartient l'article? Tags qui distinguent l'opinion, l'analyse ou la publicité des nouvelles.
- **Citations et références:** Quelle est la source? Pour les articles d'investigation ou de fond, l'accès aux sources qui se cachent derrière les faits et les affirmations.
- **Méthodes de travail:** Comment a-t-il été construit? De même, pour les histoires approfondies, des informations sur les raisons pour lesquelles les journalistes ont décidé de poursuivre une histoire et comment ils ont abordé le processus.
- **Source locale:** Identifiée lorsque l'histoire est née dans un endroit où le média a une connaissance approfondie du contexte local ou de la communauté qu'il cible.
- **Diversité:** Quel est l'engagement de la salle de presse à fournir des perspectives diverses?
- **Commentaires des lecteurs:** aménagez des espaces pour encourager la participation et les commentaires des lecteurs.

39. https://elpais.com/estaticos/que-es-the-trust-project/

7.4 Forums sociaux

Les auteurs des campagnes de désinformation diffusent les messages malveillants dans l'espoir que d'autres utilisateurs donneront de la crédibilité à l'information et diffuseront le contenu.

Les forums de discussion en ligne (qu'ils soient ouverts, sur des plateformes publiques, ou fermés, sur des sites Internet profonds) sont également utilisés de manière récurrente pour la diffusion de messages de campagne de désinformation.

Le succès de ces forums réside précisément dans le fait que les utilisateurs peuvent commenter n'importe quel sujet d'actualité de manière totalement anonyme et qu'il n'y a aucun contrôle ou censure sur la véracité des messages partagés.

Les auteurs des campagnes de désinformation diffusent les messages malveillants dans l'espoir que d'autres utilisateurs donneront de la crédibilité à l'information et diffuseront le contenu sur d'autres plateformes numériques ouvertes, ainsi que sur des réseaux sociaux personnels.

7.5 Profils numériques malveillants

La diffusion de nouvelles fausses ou malveillantes ne se fait pas uniquement par le biais de nouveaux médias peu crédibles.

La diffusion de nouvelles fausses ou malveillantes ne se fait pas uniquement par le biais de nouveaux médias peu crédibles. Ils le font également par la **manipulation ou la falsification des profils numériques sur les réseaux sociaux** de personnes ou d'institutions réelles dans le but de faire croire au public qu'elles ont fait des déclarations qu'elles n'ont en réalité jamais faites.

La manipulation de ces profils numériques peut prendre différents aspects ou modalités:

7.5 Profils numériques malveillants

Simulation malveillante de comptes et de profils réels. La méthode la plus efficace pour usurper le profil numérique d'une personne ou d'une institution consiste à utiliser des logiciels ou des sites web qui permettent de recréer l'apparence d'un véritable compte de réseau social, mais en y ajoutant du contenu inventé.

Une fois la récréation effectuée, une photographie ou une capture d'écran de la publication est prise et partagée sur les réseaux sociaux tels que WhatsApp parmi les contacts proches, jusqu'à ce que le faux message devienne viral.

Création de faux profils numériques ou de parodies. Un autre moyen de diffuser des informations malveillantes via les réseaux sociaux consiste à créer le profil numérique d'une personne ou d'une institution sans son consentement et à usurper son identité.

Pour éviter ce type de situation, certaines plateformes numériques offrent la possibilité de vérifier et d'authentifier que le profil numérique d'un individu correspond à sa véritable identité.

Piratage de profils numériques. Une forme plus sophistiquée consiste à pirater ou à voler les mots de passe de l'utilisateur d'un profil numérique pour le contrôler de manière malveillante pendant un certain temps. Certaines de ces actions ont même causé des pertes et des dommages non seulement à la réputation des entreprises, mais aussi à l'économie mondiale.

L'une des actions les plus dommageables menées à l'aide de cette méthodologie s'est produite le 23 avril 2013, lorsque le groupe se faisant appeler "Armée électronique syrienne" a pris le contrôle du compte Twitter de l'agence de presse Associated Press (AP) et a signalé une fusillade à la Maison Blanche. En quelques minutes, ce message a fait chuter la bourse américaine de plus de 150 points pendant cinq minutes[40].

A tweet from the Associated Press was false, and the AP said it had been hacked.
SCREENSHOT

Ilustration 16.- Compte Twitter d'Associated Press.

40. USA TODAY. 2013. "AP Twitter feed hacked; no attack at White House". https://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/

7.6 Comptes automatisés de comportements non-humains

La création de comptes anonymes, gérés de manière automatisée sur les réseaux sociaux, est un autre mécanisme utilisé pour diffuser massivement des messages dans le cadre d'une campagne de désinformation.

La création de comptes anonymes, gérés de manière automatisée sur les réseaux sociaux, est un autre mécanisme utilisé pour **diffuser massivement des messages dans le cadre d'une campagne de désinformation.**

La plupart des plateformes numériques de médias sociaux permettent la création de comptes anonymes et l'utilisation de logiciels qui automatisent la gestion de ces profils. Cela permet aux groupes clandestins de lancer des campagnes de désinformation qui atteignent un grand volume et une diffusion sur les réseaux sociaux.

La détection de profils numériques automatisés dans une campagne de désinformation dépend du niveau de sophistication utilisé dans la création de ces profils. Dans tous les cas, il est possible de définir certaines caractéristiques pour déterminer s'il y a une personne réelle derrière un compte numérique ou s'il s'agit d'un outil automatisé pour diffuser massivement un certain message.

- **Non-correspondance avec une personne réelle vérifiable.** La première caractéristique d'un profil numérique automatisé est que ni le nom, ni la photographie, ni les informations du compte ne correspondent à une personne réelle identifiable dans d'autres sources.

  De même, aucun détail ou commentaire relatif à la vie personnelle d'une personne ou d'une institution réelle n'est visible dans l'historique du contenu du profil.

- **Activité quotidienne élevée ou inhabituelle.** Les comptes automatisés se distinguent par leur comportement temporel inhabituel. Des centaines de messages sur le même sujet au cours d'une même journée ; un nombre anormalement élevé de messages (plus de cinquante par jour) ; des messages publiés 24 heures sur 24, sept jours sur sept, ...

- **Absence de followers ou de followers suspectés d'être des comptes automatisés.** Les profils numériques utilisés dans les campagnes de

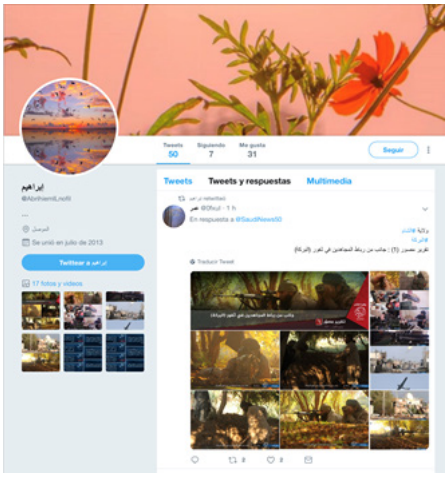
7.6 Comptes automatisés de comportements non-humains

désinformation se distinguent par le faible nombre de suiveurs qu'ils ont sur leur profil ou, au contraire, par le nombre élevé de suiveurs qui pourraient également être des comptes robots automatisés.

- **L'unilatéralité.** Les profils numériques automatisés n'engagent généralement pas de dialogue sur les réseaux sociaux, ils se limitent à diffuser des messages dans les conversations où se trouvent leurs publics potentiels.
- **Absence de contenu original.** L'une des principales caractéristiques des comptes numériques au comportement non humain est l'absence de contenu original. La majorité de ces profils redirigent ou interagissent avec le contenu créé par d'autres profils.
- **Peu de variété thématique.** Les profils numériques automatisés se concentrent sur la publication et la diffusion la plus large possible des messages politiques ou sociaux pour lesquels ils ont été créés.
- **Peu de variété de sources.** De même, ces comptes de campagne de désinformation utilisent exclusivement les sources qui font partie de la même stratégie et créent et diffusent des messages similaires avec les mêmes approches.

De même, **l'utilisation automatisée des réseaux sociaux** est, par exemple, la technique couramment utilisée par le groupe terroriste DAESH pour diffuser ses campagnes sur les réseaux sociaux. Les terroristes génèrent en moyenne une centaine de nouveaux profils numériques, avec quasiment aucun follower, pour diffuser chacune de leurs campagnes de communication, et gèrent ces comptes à l'aide de bots qui automatisent la diffusion des messages.

Ils *viralisent* leurs contenus en parasitant les hashtags les plus populaires dans les conversations de leurs publics potentiels.



Ilustration 17.- Exemple d'un bot utilisé par le groupe terroriste DAESH pour diffuser sa propagande sur les réseaux sociaux.

7.7 Comptes de couverture numérique ou comptes hybrides

Les campagnes de désinformation utilisent des stratégies de plus en plus complexes pour rendre difficile la détection des comptes automatisés responsables de la diffusion de leurs messages.

Les campagnes de désinformation utilisent des stratégies de plus en plus complexes pour rendre difficile la détection des comptes automatisés responsables de la diffusion de leurs messages. Les responsables des stratégies de désinformation offensive savent que les comptes automatisés présentant les caractéristiques décrites ci-dessus sont facilement détectables et n'ont pas la crédibilité nécessaire pour rendre un message viral de manière efficace.

C'est pourquoi **les campagnes de désinformation ont de plus en plus recours à des profils numériques qui ressemblent à un comportement humain,** mais qui font en fait partie d'une armée de fausses identités créées et contrôlées par un groupe organisé travaillant en secret.

Ces profils numériques tentent de dissimuler les caractéristiques des comptes automatisés; ils semblent être associés à des personnes réelles avec un prénom, un nom, une photographie, des hobbies, une date de naissance; ils ont un nombre considérable de followers; ils ont une trajectoire temporelle considérable et interagissent parfois avec d'autres utilisateurs. Cependant, tout cela fait partie d'une couverture soigneusement élaborée pour gagner la confiance

des autres utilisateurs et diffuser efficacement des messages désinformateurs.

Un exemple d'un tel compte est le profil à partir duquel a été diffusée la fausse nouvelle liant Hillary Clinton à un réseau d'exploitation d'enfants dans une pizzeria. Les informations qui ont émergé de forums numériques anonymes ont gagné en crédibilité dès lors qu'elles ont été diffusées par un compte de réseau social qui semblait représenter une personne réelle: David Goldberg (@davidgoldbergNY), un avocat de New York, qui s'est même présenté avec une photographie.

Cependant, aucune personne réelle ne se cachait derrière le compte, qui était utilisé uniquement pour diffuser de fausses informations sur le candidat à la présidence américaine. Le profil a été supprimé par le réseau social Twitter lorsqu'il s'est avéré qu'il était faux.

Ilustration 18.- Message posté depuis le compte @davidgoldbergNY.

7.7 Comptes de couverture numérique ou comptes hybrides

Un autre exemple de faux comptes de médias sociaux prétendant représenter des personnes réelles s'est produit lors de la diffusion d'informations liées à la tenue du référendum d'indépendance illégal en Catalogne en octobre 2017.

Parmi les profils numériques les plus actifs diffusant des informations critiquant l'attitude du gouvernement espagnol figurait le profil d'Ivan (@ivan226622), un ressortissant asiatique (avec de vraies photos) qui se disait passionné par la technologie, les affaires et l'actualité. Il avait 1 287 followers et avait posté 580.000 messages depuis novembre 2012.

Cependant, Ivan ne correspondait à aucune personne réelle, mais faisait partie d'un réseau de faux profils numériques qui, de manière coordonnée, ont diffusé des informations négatives sur l'Espagne au cours des premières semaines d'octobre 2017. En fait, on a pu voir comment @ivan226622 a publié les mêmes nouvelles négatives sur l'Espagne en même temps que d'autres comptes tels que @rick888 ou @bobbit2266, ce qui suggère que tous ces comptes étaient gérés par la même personne ou organisation. Quelques semaines après avoir été détectés, le réseau social Twitter a supprimé ces comptes car ils se sont avérés faux.

Ilustration 19.- Messages Twitter avec la publication d'une même nouvelle à partir de comptes différents.

7.7 Comptes de couverture numérique ou comptes hybrides

Les couvertures numériques ou les comptes hybrides sont également associés à un "faux comportement coordonné"[41], un terme utilisé par Facebook pour désigner les pages et les profils qui collaborent pour tromper les utilisateurs sur leur identité ou leurs activités. un terme utilisé par Facebook pour désigner les pages et les profils qui travaillent ensemble pour tromper les utilisateurs sur leur identité ou leurs activités. Pour des raisons idéologiques ou financières, ces comptes font croire aux gens qu'ils sont employés dans une partie du monde différente de leur origine réelle.

À cet égard, le réseau social Facebook a également détecté la création de faux profils sur sa plateforme, comptes qu'il a procédé à la suppression une fois leur origine identifiée. Le 31 janvier 2019[42], sur sa page officielle, le réseau social a annoncé la fermeture de 207 pages Facebook, 800 profils et 456 groupes, "liés au syndicat en ligne Saracen Group en Indonésie". Selon le site web de Facebook, ces comptes ont été supprimés en raison de leur comportement trompeur et non du contenu qu'ils ont publié.

7.8 Guest stars

La collaboration de personnalités influentes, qui jouissent d'une certaine crédibilité auprès des publics potentiels.

Un autre élément utilisé pour diffuser les messages d'une campagne de désinformation est **la collaboration de personnalités influentes, qui jouissent d'une certaine crédibilité auprès des publics potentiels** et qui, surtout, ne semblent pas avoir de lien ou d'intérêt direct avec les questions politiques ou sociales débattues.

Cette distance apparente confère aux messages délivrés par ces personnalités influentes une plus grande crédibilité et objectivité. Toutefois, il est possible que ces personnes aient des liens politiques ou économiques avec des agents secrets et que leurs messages fassent partie d'une stratégie de désinformation dont les destinataires finaux ne sont pas conscients.

41. GELICHER, Natahniel, 'Coordinated Inauthentic Behaviour´, Facebook, https://newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/
42. GELICHER, Nathaniel, `Taking down coordinated inauthentic behavior in Indonesia', Facebook, https://newsroom.fb.com/news/2019/01/taking-down-coordinated-inauthentic-behavior-in-indonesia/

7.9 Algorithmes, chambres d'écho et réseaux de confiance

Le débat disparaît et où les communautés numériques en conflit ne font que radicaliser et réaffirmer leurs positions au lieu de s'engager dans un débat raisonné.

Les algorithmes utilisés par les nouvelles plateformes de communication numérique, comme les réseaux sociaux, sont devenus des alliés involontaires des campagnes de désinformation. Ces technologies ne privilégient pas la réception par l'utilisateur final d'informations variées et pluralistes sur l'actualité politique, sociale ou économique. Au contraire, les algorithmes utilisés par ces entreprises technologiques sont conçus pour que l'utilisateur ne reçoive et n'interagisse qu'avec des messages qui peuvent potentiellement lui plaire et réaffirmer ses idées.

De cette manière, les plateformes de communication offrent des informations à leurs utilisateurs en fonction de leurs préférences politiques, et non de la qualité, de la pluralité ou de la véracité du contenu.

Cette circonstance favorise la création de chambres d'écho dans la conversation numérique, où **le débat disparaît et où les communautés numériques en conflit ne font que radicaliser et réaffirmer leurs positions au lieu de s'engager dans un débat raisonné.**

7.10 Publicités payantes

Les responsables de campagnes de désinformation ont trouvé efficace de créer du contenu sur les questions les plus controversées dans le débat numérique d'un pays et de le promouvoir par des campagnes payantes.

La création de ces chambres de résonance par des algorithmes a favorisé la diffusion massive d'actions de désinformation par des agents infiltrés. Les responsables des campagnes de désinformation ont trouvé efficace de créer du contenu sur les questions les plus controversées dans le débat numérique d'un pays et **de les promouvoir par des campagnes payantes entre chacune des chambres d'écho créées dans ces débats.** De cette façon, chacune des communautés opposées se sent identifiée à ce contenu, interagit avec lui et encourage la polarisation sociale et la confrontation de l'opinion publique.

C'est la stratégie que, selon un rapport de la commission du renseignement de la Chambre des représentants américaine, la Russie a utilisée pour interférer dans l'élection présidentielle de 2016. Selon l'enquête, l'Internet Research Agency (IRA), basée en Russie, a payé Facebook pour promouvoir plus de 3 000 messages auprès du public[37] (non signées et non identifiées) visant à polariser les citoyens américains autour des débats les plus controversés du pays.

De cette façon, l'IRA a pu financer secrètement des campagnes en faveur de l'intégration de la communauté musulmane et, en même temps, des campagnes de promotion de l'islamophobie, comme le montrent les images suivantes, incluses dans le rapport de la Chambre des représentants des États-Unis.

43. THE WALL STREET JOURNAL. 2018. Release of Thousands of Russia-Linked Facebook Ads Shows How Propaganda Sharpened, by Deepa Seetharaman, Georgia Wells and Byron Tau. https://www.wsj.com/articles/full-stock-of-russia-linked-facebook-ads-shows-how-propaganda-sharpened-1525960804

7.10 Publicités payantes

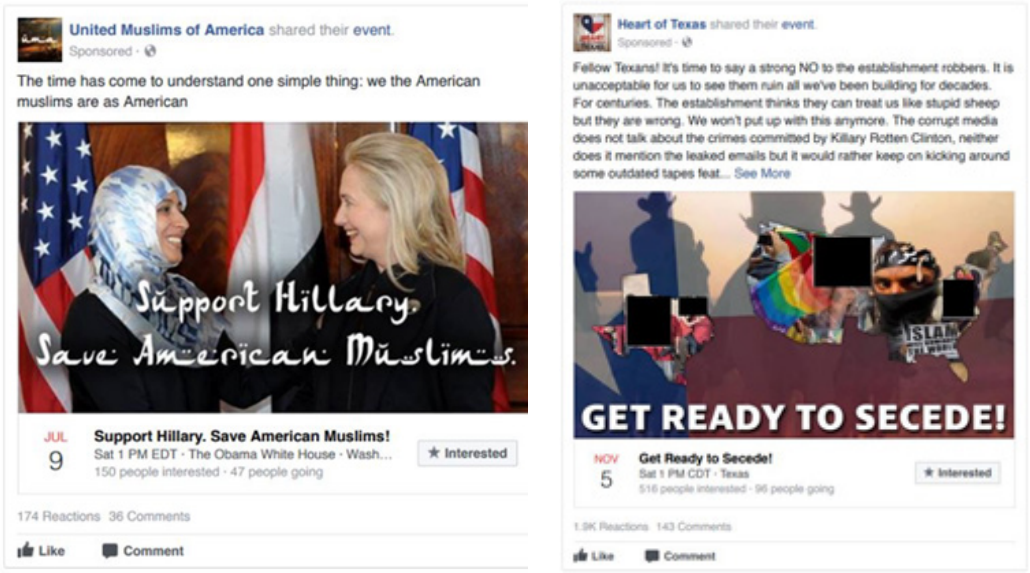


Illustration 20.- Images incluses dans le rapport de la Chambre des représentants des États-Unis.

8. Décalogue de recommandations

Éviter d'être victime d'une campagne de désinformation n'est pas la responsabilité d'un seul acteur. **Les institutions publiques ont l'obligation de développer les capacités nécessaires pour prévenir, détecter et neutraliser les offensives de désinformation** contre un État.

De même, **les entreprises privées ont l'obligation d'empêcher que leurs plateformes numériques ne deviennent des outils utilisés dans des campagnes malveillantes** contre les citoyens et les systèmes gouvernementaux légitimes.

D'autre part, **le monde universitaire doit poursuivre ses recherches sur ce nouveau phénomène et produire des preuves scientifiques sur les méthodologies et les conséquences** que les campagnes de désinformation ont sur l'opinion publique et la gouvernance.

Cependant, les premières et dernières victimes des guerres de communication sont les citoyens. C'est pourquoi il est nécessaire que **les utilisateurs des médias numériques soient prévenus pour détecter une campagne de désinformation et disposent des compétences nécessaires pour éviter d'être manipulés.**

Les institutions publiques ont l'obligation de développer les capacités nécessaires pour prévenir, détecter et neutraliser les offensives de désinformation.

Décalogue de sécurité contre les campagnes de désinformation

1. **Analysez la source des nouvelles que vous recevez et consommez:** chaque jour, nos appareils mobiles reçoivent des dizaines d'impacts communicationnels avec des nouvelles qui nous surprennent, nous indignent ou nous excitent. Parfois, ces nouvelles proviennent de plateformes numériques "non traditionnelles" et peu transparentes. Il est important de savoir quel média publie une nouvelle, quelle est sa trajectoire et quels journalistes, entreprises ou pays sont à l'origine de cette publication[44]. En ce sens, il est conseillé de disposer de liens qui redirigent l'information vers ses sources originales ou vers d'autres textes qui valident les données.

2. **Doutez des captures d'écran que vous recevez sur les réseaux sociaux:** lorsque vous recevez des informations sous forme d'images, il est toujours conseillé de faire preuve d'une dose de prudence et de scepticisme. Il existe une multitude de logiciels et de programmes informatiques faciles à utiliser qui vous permettent de retoucher ou de modifier des images avec de faux titres provenant des médias traditionnels ou des comptes et profils de médias sociaux de personnes réelles. De même, il est très courant de sortir des images de leur contexte, en dissociant la prise de vue réelle du titre, et en donnant de la vraisemblance à une fausse histoire. Si vous doutez de la réalité de certains de ces messages, il est conseillé de toujours aller à la source originale avec ses liens sur Internet ou de faire ce qu'on appelle une "recherche inversée" pour savoir si une photo a déjà été publiée sur Internet. Il est également possible de vérifier si une image est originale ou a été copiée grâce aux informations EXIF[45].

3. **Qui a partagé la nouvelle et dans quel contexte:** n'accordez pas de crédibilité à tous les messages que vous lisez sur les médias sociaux, en particulier aux messages ou commentaires publiés par des comptes et profils anonymes. Demandez-vous, même si elle vous a été envoyée par un ami, quelle est la date de l'information, qui en est la source et quels autres médias l'ont diffusée. Il est même conseillé de rechercher le titre dans un moteur de recherche, car s'il est vrai, d'autres médias l'auront repris. N'accordez de la crédibilité qu'aux informations partagées par des sources réelles[46].

4. **Méfiez-vous des faux comptes "humains":** de plus en plus souvent, on voit apparaître sur les réseaux sociaux des comptes à l'apparence humaine, mais qui sont en fait gérés par des robots ou des tiers chargés de contrôler différents profils. Avant de suivre ou de faire confiance au contenu publié par un profil numérique, analysez combien de personnes il suit, combien de personnes le suivent, s'il génère son propre contenu, s'il fait un usage excessif du réseau social... Autant d'indicateurs pour détecter les faux profils numériques sur les réseaux sociaux[47].

5. **Ne faites pas partie de l'algorithme:** les plateformes numériques que nous utilisons tous les jours pour communiquer et nous informer sont basées sur un algorithme complexe qui nous propose des informations personnalisées en fonction de nos supposés goûts, hobbies ou opinions. Ainsi, les plateformes numériques elles-mêmes nous offrent les informations que le logiciel pense que nous allons aimer. Si nous voulons développer une opinion bien formée, critique et contrastée, il est conseillé d'obtenir des sources d'information alternatives à celles qui, par défaut, nous sont montrées par les algorithmes des plateformes de communication.

6. **Lisez les petits caractères:** les actions de désinformation les plus réussies sont celles qui reposent sur des demi-vérités. Les fausses nouvelles sont relativement faciles à détecter et à démanteler. Cependant, dans de nombreux cas, les promoteurs de la désinformation utilisent des photos et des faits réels qui, lorsqu'ils sont présentés de manière suggestive dans un titre et accompagnés d'une photographie, peuvent être mal interprétés. Lors d'un reportage en format numérique, ne vous contentez pas de la sensation que peuvent générer un titre et une photo. Lisez l'article dans son intégralité et analysez si les données sont vérifiées et si les citations et les opinions reflètent une pluralité d'opinions.

7. **Méfiez-vous des contenus sponsorisés d'origine inconnue:** les plateformes numériques gagnent de l'argent en échange du parrainage de certains contenus par les utilisateurs afin qu'ils apparaissent en bonne place dans le profil d'un public spécifique. Méfiez-vous des contenus politiques ou controversés sponsorisés par des profils anonymes ou non identifiés à de véritables associations, partis politiques ou institutions.

8. **Méfiez-vous des guest stars:** il arrive souvent que des acteurs politiques, sociaux ou culturels importants s'impliquent activement dans des discussions politiques ou sociales dans des pays étrangers. La liberté d'expression et d'opinion est l'un des atouts les plus respectables d'une démocratie libérale. Cependant, il faut également tenir compte du fait que certains de ces acteurs influents participent à certaines discussions en fonction d'agendas politiques et économiques très spécifiques qui ne sont pas connus du public final.

9. **Esprit critique et sang-froid:** certains acteurs politiques, nationaux et infranationaux, utilisent la communication numérique pour affronter l'opinion publique d'un pays étranger et mobiliser le mécontentement légitime d'une partie de ses citoyens autour de questions politiques, sociales ou économiques litigieuses et discutables. Participer aux débats politiques enrichit la démocratie et la pluralité politique. Il convient toutefois de le faire avec rationalité, respect et esprit critique, en évitant de générer des spirales de haine et de disqualification, qui peuvent parfois être encouragées par des agents ou des groupes clandestins.

10. **Vous pouvez arrêter un conflit:** les actions de désinformation contemporaines reposent sur la vitesse et la viralité avec lesquelles les nouvelles, les rumeurs et les commentaires se propagent. Nous faisons tous partie des campagnes de désinformation et nous en sommes les maillons. Il est important d'être conscient que nous pouvons être utilisés comme des pions dans des stratégies sponsorisées et gérées par des acteurs inconnus aux intérêts politiques non déclarés. Il est donc important de toujours être attentif au contenu des informations que nous recevons quotidiennement sur nos ordinateurs ou appareils mobiles et de ne pas contribuer à la diffusion d'informations non vérifiées ou dont la traçabilité et l'origine sont douteuses.

CCN centro criptológico nacional

CCN CERT centro criptológico nacional

44. Il existe diverses organisations, médias et portails web visant à confirmer ou infirmer les données. C'est le cas du site espagnol Maldito bulo, membre du groupe d'experts de haut niveau de la Commission européenne, de BSDetector, Snopes et FactCheck.
45. Il existe plusieurs outils qui le permettent, comme RevEye, qui fonctionne comme une extension pour les navigateurs Chrome et Firefox et recherche plusieurs banques d'images sur le web. Google Images a également une fonction similaire, tout comme TinEye. Il est également possible de disposer d'outils de vérification des vidéos tels que Google Earth (pour comparer la géographie ou les lieux d'intérêt où elle a été enregistrée) ou YouTube Data Wiewer pour connaître l'heure à laquelle la vidéo a été téléchargée et qui extrait des captures d'écran pour savoir s'il existe d'autres versions de la vidéo disponibles sur Internet, et si elles ont été publiées avant ou après.
46. La plupart des réseaux sociaux disposent eux-mêmes d'informations et de bonnes pratiques pour éviter les fake news et les chaînes de diffusion. C'est le cas de Facebook, Google ou Twitter.
47. *Crowdtangle* est un outil que Facebook a acquis en 2016 et qui surveille la façon dont le contenu "bouge" sur les réseaux sociaux, ou encore **Foller.me**, qui détermine si un profil est trompeur ou non. Les indications sont les suivantes : le profil "converse" avec peu de comptes, il a des pics d'activité très élevés ou sa date de création.

centro criptológico nacional

centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es