La desinformación rusa en la era de internet

Guillem Colom Piella
Doctor en Seguridad Internacional

Tal y como se expuso meses atrás, la desinformación rusa no es un fenómeno nuevo. Sin embargo, es ahora cuando ha multiplicado su alcance explotando las posibilidades que brinda internet. Ha adaptado sus tácticas e instrumentos al mundo digital, adoptado vectores y lenguajes propios de este dominio, aprovechado las debilidades de las sociedades avanzadas para diluir la línea entre los hechos y la ficción o utilizado la libertad de expresión para introducir contenido extremista.

La desinformación rusa está de moda. Se cita en los debates políticos, se percibe con temor en muchas cancillerías occidentales y Bruselas la considera como un peligro para la estabilidad europea. El *hype* generado por este fenómeno ha motivado que muchos comentaristas la sitúen como uno de los puntales de la doctrina Gerasimov y la guerra híbrida que Moscú está librando contra Occidente a pesar de que estos planteamientos no existen en el pensamiento estratégico ruso. Otros la consideran como algo novedoso por la eficaz explotación de internet, peligroso porque puede estallar cualquier oportunidad –como podría ser la COVID-19 y las campañas de vacunación de muchos países[1]– y alertan de las posibilidades que se abren con el uso de la inteligencia artificial para elaborar deep fakes o chatbots con comportamientos casi-humanos.

Tal y como se expuso meses atrás[2], la desinformación rusa no es un fenómeno nuevo. Sin embargo, es ahora cuando ha multiplicado su alcance explotando las posibilidades que brinda internet. Ha adaptado sus tácticas e instrumentos al mundo digital, adoptado vectores y lenguajes propios de este dominio, aprovechado las debilidades de las sociedades avanzadas para diluir la línea entre los hechos y la ficción o utilizado la libertad de expresión para introducir contenido extremista. Aprovechando un caldo de cultivo propicio, ha sabido explotar la desafección política, el relativismo, las actitudes posmodernas o las contradicciones occidentales, descreditar sus políticas, polarizar a sus poblaciones o manipular sus procesos de toma de decisiones. Y tal y como sucedió durante la Guerra Fría, donde la desinformación mutó en las medidas activas –que combinaban desinformación, propaganda, manipulación y falsificación documental utilizando una amplia gama de medios de propagación– actualmente nos hallamos frente a unas medidas activas digitales que cuentan con un ecosistema propio[3] y que contribuyen a su guerra informativa.

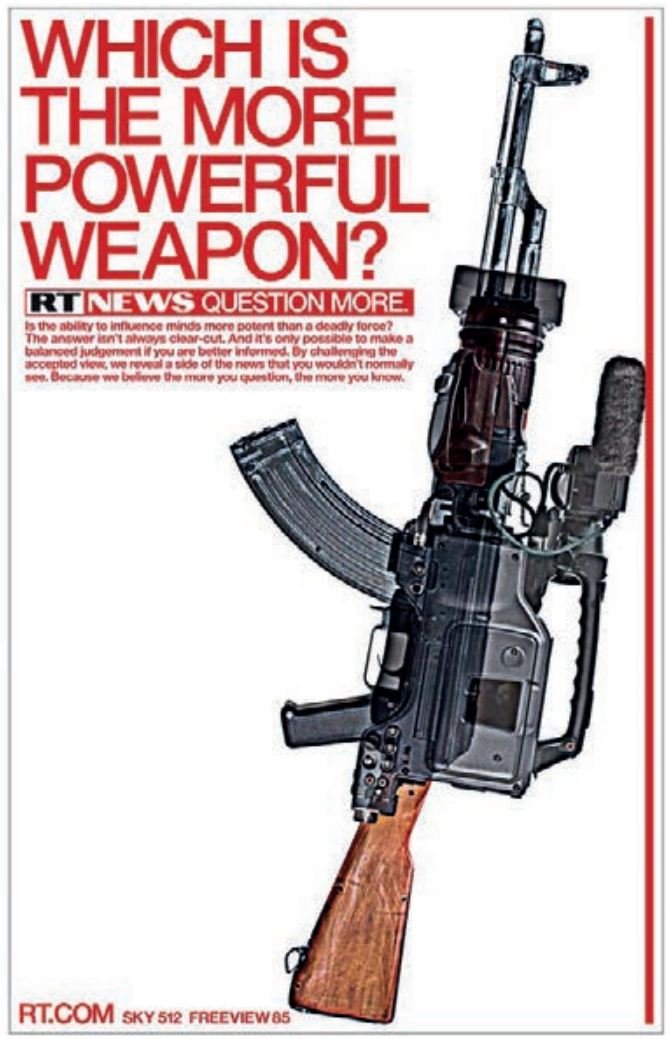
Ejemplo de deepfake. Jim Carrey suplantando a Jack Nicholson en el resplandor

Precisamente, el potencial de las nuevas tecnologías para influir sobre las opiniones públicas y desestabilizar gobiernos ha sido un asunto recurrente en la comunidad de inteligencia rusa desde el fin de la Guerra Fría. Estos miedos se fundamentaban en varios supuestos: que la *Glasnost* erosionó el monopolio informativo gubernamental y facilitó la penetración de la propaganda occidental que motivaría la caída de la URSS. Que la libertad informativa entre 1991 y 2000 hizo a la población vulnerable a la manipulación y a las promesas de prosperidad económica. Que internet podía usarse para desestabilizar el país y desmoralizar a la población o que, en Chechenia, un adversario militarmente más débil pero informativamente más efectivo y la presencia de periodistas independientes, podían condicionar el desenlace de una operación militar. Asimismo, muchos pensadores militares añadieron –interpretando los debates estadounidenses sobre la Revolución en los Asuntos Militares– que estas tecnologías permitirían desestabilizar un país en pocos días o derrotar un oponente militarmente más poderoso sin la necesidad de combatir[4].

Estos factores motivaron la elaboración de la primera *Doctrina de Seguridad de la Información* y la ejecución de una amplia batería de medidas encaminadas a blindar el espacio informativo ruso frente a cualquier amenaza interna e injerencia externa[5], sino también el desarrollo de la guerra informativa[6], relevante para la configuración de las «guerras de nueva generación» y uno de los fundamentos de los conflictos futuros.

En cualquier caso, parece que desde hace años –se tiende a situar el ascenso de Putin al poder como punto de inflexión– la desinformación ha ido adaptando progresivamente sus instrumentos (especialmente los medios de comunicación, los agentes de influencia o los colaboradores[7]) para diseminar desinformaciones, falsificaciones, manipulaciones o datos personales obtenidos de forma ilegal para debilitar adversarios políticos en el mundo físico y digital. Además, también está explotando otros vectores y lenguajes característicos del entorno virtual.

En este sentido, aunque los medios de comunicación continúan siendo fundamentales, sus tácticas respecto a las utilizadas durante la Guerra Fría han cambiado y su alcance se ha multiplicado. Por un lado, actualmente Moscú dispone de medios y plataformas multilingües con fuerte



Publicidad del canal de noticias de televisión RT

presencia en línea y segmentadas por audiencias tipo (desde la agencia *TASS* o *Russia Beyond* a los populares *Sputnik* o *RT*). Concebidos como una herramienta de poder blando para promover internacionalmente la imagen de Rusia y erosionar el monopolio informativo occidental, estos pueden difundir propaganda gubernamental y actuar como altavoz de otras actividades en blogs o redes sociales. Sus narrativas muestran distintos niveles de sofisticación y pueden usar una amplia gama de expertos y comentaristas para otorgar credibilidad a la desinformación[8].

También parece emplear medios clandestinos para diseminar propaganda gris o negra. Baratos de crear, mantener o replicar y difíciles de atribuir al Kremlin, normalmente se los vincula con plataformas de periodismo alternativo que difunden bulos, conspiraciones o falsificaciones procedentes de otros blogs y webs[9]. Quizás, también deberían incluirse las plataformas que publican material obtenido por medios ilícitos como *DCleaks* –creada por la inteligencia rusa para apoyar el *hack&leak* del partido demócrata estadounidense– o *Wikileaks*. Aunque no existen vinculaciones concluyentes entre esta última plataforma y el Kremlin, sí diseminó documentación obtenida ilegalmente por el Directorado Central de Inteligencia (GRU) para influir en los comicios presidenciales estadounidenses de 2016[10].

Por último, como sucedía en el pasado, también pueden valerse de medios afines en todo el espectro ideológico que divulgan las narrativas rusas voluntariamente, o plataformas legítimas que difunden la desinformación involuntariamente. En este último caso, Rusia lo tiene más fácil que en el pasado porque explota la crisis del periodismo tradicional, los nuevos modelos de negocio de los medios o la sobreinformación para insertar su propaganda. La difusión de contenidos sin verificar para mantener el ciclo informativo, visibilizar el medio, maximizar el tráfico u obtener *clickbait* o por estándares éticos laxos e insuficientes medios a disposición de las plataformas actuales permite el empleo de numerosos *proxies* para implantar desinformación y falsificaciones en estos medios neutrales[11].

Los agentes de influencia y los colaboradores típicos de la Guerra Fría también se han adaptado al siglo XXI. Ahora, las personas con proyección pública o autoridad en su disciplina que difunden las

Ad ID	6053177352305
Ad Account ID	119004211765422 Payment sources associated with account:
Ad Text	Today Americans are able to elect a president with godly moral principles. Hillary is a Satan, and her crimes and lies had proved just how evil she is. And even though Donald Trump isn't a saint by any means, he's at least an honest man and he cares deeply for this country. My vote goes for him!
Ad Landing Page	https://www.facebook.com/login/?next=https%3A%2F%2Fl.facebook.com%2Flsr.php%3Fu%3Dhttps%253A%252F%252Fwww.facebook.com%252FArmy-of-Jesus-1195795607160174%252F%26ext%3D1481104016%26hash%3DAcmulRZFkln8arsE_PgiwkOZA8g8cu3a4cDhraLMfh0f7w
Ad Targeting	Location - Living In: United States Interests: Laura Ingraham, God, Ron Paul, Christianity, Bill O'Reilly (political commentator), Rush Limbaugh, Andrew Breitbart, Bible, Conservatism in the United States, Michael Savage, Faith, Mike Huckabee or Jesus Age: 18 - 65+ Placements: News Feed on desktop computers or News Feed on mobile devices
Ad Impressions	71
Ad Clicks	14
Ad Spend	64.00 RUB
Ad Creation Date	10/19/16 08:45:02 AM PDT
Ad Start Date	10/19/16 08:45:01 AM PDT
Ad End Date	10/20/16 08:45:00 AM PDT

Metadatos relacionados con el anuncio pagado en Instagram en los que se observa el target del mismo

narrativas pro-rusas son más y tienen mayor visibilidad[12]. Mientras antiguamente las voces amigas oscilaban entre el comunismo y el internacionalismo, ahora se sitúan en todo el espectro político. Todos ellos pueden colaborar en medios y participar en redes sociales diseminando propaganda revestida de aparente objetividad e interactuando con sus seguidores para modelar el debate e influir en la opinión pública.

También se están utilizando herramientas del mundo virtual para incrementar sus efectos y dificultar la atribución de responsabilidades. En primer lugar, grupos de hackers –como los populares *Fancy Bear* o *Cozy Bear*– relacionados con el Servicio Federal de Seguridad (FSB), el Servicio de Inteligencia Extranjera (SVR) o el GRU se encargan de obtener información sensible[13]. Entre otros objetivos, esta puede utilizarse para extorsionar o difamar a la víctima. Empleada también en el entorno físico[14], esta técnica entraña el acceso y filtración de los datos obtenidos en foros, agregadores de noticias, plataformas específicas o medios de comunicación[15] y su posterior amplificación mediante campañas en redes sociales.

Se están utilizando herramientas del mundo virtual para incrementar sus efectos y dificultar la atribución de responsabilidades (...) entre otros objetivos, estas pueden utilizarse para extorsionar o difamar a la víctima

En segundo lugar, la popular combinación de *trolls* que interactúan con otros usuarios en línea y *bots* automatizados que amplifican el impacto de los primeros. En tres lustros, estos han pasado de ser jóvenes aficionados que actuaban por convicción en el internet de habla rusa intimidando a periodistas, blogueros y comentaristas críticos con Putin, redistribuyendo información oficialista o alterando el posicionamiento web de páginas contrarias al gobierno, a ser un ejército de *trolls* profesional. Asistida por una legión de colaboradores, este ejército global continúa participando en foros, blogs o redes sociales generando discusiones, desviando debates y ridiculizando o acosando a los críticos[16]. Sin embargo, ahora también adopta múltiples perfiles e interactúa con otros internautas para diseminar contenido falso, proveer relatos alternativos, otorgar credibilidad a la desinformación o suprimir las voces que exponen las inconsistencias de las narrativas falsas. Explotando las redes de *bots*, manipulando los rankings de contenido y aprovechándose de la pasividad de las plataformas sociales para eliminar estas cuentas que siguen patrones distinguibles, esta nueva generación de *trolls* ha conseguido amplificar el alcance de la desinformación para alterar la percepción de la realidad, inducir a la polarización social o crear una falsa impresión de consenso en la red.

En último lugar, el referéndum sobre el *brexit* y los comicios presidenciales estadounidenses de 2016 sugieren que la propaganda computacional también participa en la desinformación[17]. Basada en el minado de datos para perfilar el usuario, el uso de algoritmos para seleccionar aquellas narrativas que refuercen sus prejuicios y filtrando la difusión de noticias (texto, videos, imágenes o *memes*), cronología o resultados de búsquedas para manipularlo[18], la militarización del *microtargeting* amplifica el alcance de la propaganda y refuerza el filtro burbuja. Realizada en connivencia con las empresas tecnológicas, que consiguen nuevos usuarios, más reacciones emocionales y mayores interacciones para obtener perfiles más ricos, y aprovechándose de la ingenuidad humana, partícipe involuntaria de su propio perfilado, del refuerzo de sus prejuicios y de la dispersión de desinformación (en redes sociales, servicios de mensajería o en vivo), la propaganda computacional abre las puertas a campañas masivas de ingeniería social. Éstas podrán estar apoyadas por toda la gama de medios sintéticos que, producidos, manipulados o modificados mediante algoritmos de inteligencia artificial, difuminan cada vez más las fronteras entre la realidad y la ficción. En otras palabras, la desinformación está en permanente evolución, explotando las oportunidades que brinda la tecnología y la coyuntura sociopolítica para desinformar, desmoralizar, desestabilizar e influir sobre el adversario.

CONCLUSIONES

Aunque apenas ha cambiado en su concepción por la continuidad que existe en su cultura estratégica, la desinformación rusa ha adaptado sus técnicas al siglo XXI y desarrollado nuevas herramientas para influir en el mundo digital. Ha aprovechado el potencial de las nuevas tecnologías para globalizar la propaganda, asimilado el lenguaje de internet para influir sobre el adversario y explota-

Propaganda rusa en Instagram para las elecciones presidenciales de 2016

do el poder de las redes sociales –en connivencia con las empresas tecnológicas y la colaboración involuntaria de los usuarios– para posibilitar la manipulación masiva. También han aprovechado las debilidades de las sociedades avanzadas –desde la desafección política o la libertad de expresión a las actitudes posmodernas y relativistas de la ciudadanía– para explotar sus clivajes políticos, socioeconómicos, ideológicos o étnicos apelando a las emociones, denigrando los hechos objetivos, reforzando los prejuicios, encumbrando a conspiradores, planteando realidades alternativas y posibilitando la desinformación. Y todo para influir estratégicamente, desestabilizar socialmente o subvertir políticamente al adversario.

La experiencia acumulada en múltiples escenarios –desde la propaganda en su área de influencia directa, la desinformación en apoyo a las operaciones militares en Ucrania o Siria hasta las intromisiones en procesos políticos– revela que Moscú posee un amplio conjunto de vectores físicos y digitales para apoyar sus actividades de influencia. Su ejército de *trolls*, sus grupos de hackers, sus agencias y servicios de noticias, sus medios encubiertos, su desinformación en línea o su propaganda son los que más atención reciben de los analistas. Sin embargo, forman parte de un complejo ecosistema en constante evolución que combina los nuevos vectores con herramientas tradicionales para alcanzar otras capas de la sociedad menos expuestas a internet. Aunque es posible especular sobre el empleo masivo de medios sintéticos, nuevas tácticas de troleo o mejores perfilados, la desinformación del siglo XXI continuará sorprendiendo mediante la explotación de nuestras debilidades, irrumpiendo por donde menos esperamos, utilizando vectores que ignoramos y herramientas que desconocemos. No obstante, conociendo el contexto, historia, objetivos y medios, situándola en su contexto estratégico y recabando el apoyo de unas empresas tecnológicas y unos medios de comunicación que han contribuido al problema y parecen interesados en colaborar en su solución, quizás será más fácil identificar las campañas, prever sus objetivos, limitar su impacto y no caer en la trampa de centrarse en este asunto a costa de dejar descubiertos otros flancos quizás más relevantes.

Y es que, mientras los focos se centran en la desinformación rusa o china, otros actores están utilizando tácticas, técnicas y procedimientos similares para alcanzar los mismos fines. Otros están explotando esta atención para influir sobre las sociedades objetivo con estos y otros medios. La desinformación explota y amplifica los problemas inherentes de las sociedades avanzadas hasta convertirse en una amenaza para la estabilidad social y política de los sistemas democráticos, pero no es la única. No cometamos el error de centrar todos los esfuerzos en este fenómeno y dejemos otros flancos al descubierto. ■

NOTAS

[1]Gordon, M.; Volz, D. (2021, 7 de marzo): «Russian Disinformation Campaign Aims to Undermine Confidence in Pfizer, Other Covid-19 Vaccines», Wall Street Journal [en línea] https://www.wsj.com/articles/russian-disinformation-campaign-aims-to-undermine-confidence-in-pfizer-other-covid-19-vaccines-u-s-officials-say-11615129200 Sin embargo, muchos actores se han intentado aprovechar de esta situación.

[2]Colom, G. (2021): «La desinformación rusa en su contexto histórico», Revista de Aeronáutica y Astronáutica, n.º 900, pp. 176-181.

[3]Global Engagement Centre (2020): Pillars of Russia's Disinformation and Propaganda Ecosystem. Washington DC: Department of State.

[4]Gareev, M. (1998): If War Comes Tomorrow? The Contours of Future Armed Conflict. Londres: Frank Cass. En

la década de 1990, mientras EEUU debatía sobre el potencial revolucionario de las plataformas furtivas, los sensores avanzados y las armas inteligentes en los conflictos futuros, los tratadistas rusos teorizaban sobre los efectos disruptivos de la informatización sobre las fuerzas armadas. Una década después, mientras Washington aprovechaba su supremacía tecnológica para desarrollar cibercapacidades, Moscú ya había madurado la guerra informativa y la había probado en Estonia y Georgia, extrayendo lecciones e identificando vectores que aplicaría en Crimea, Ucrania o Siria.

[5]Tarín, A. et al. (eds.) (2018): Sistema mediático y propaganda en la Rusia de Putin. Salamanca: Comunicación Social. Ello se plasmaría en el control de las licencias de radiotelevisión y los servicios de telefonía e internet, la vigilancia de la actividad de asociaciones y organizaciones extranjeras en territorio ruso, la promoción del desarrollo de hardware y software nacional o la creación de una muralla digital aparentemente inexpugnable para proteger la moral, cultura y estabilidad social rusa frente a cualquier amenaza interna o externa.

[6]Colom, G. (2019). «¿Por qué hablamos de desinformación cuando es guerra informativa?», Revista de Aeronáutica y Astronáutica, n.º 888, pp. 850-855.

[7]Los proxies y organizaciones pantalla también se han adaptado con la financiación de partidos políticos populistas, fundaciones, proyectos culturales, ONGs o think tanks (Polyakova, A; Boyer, S. (2018): The future of political warfare: Russia, the West, and the coming age of global digital competition. Washington DC: Brookings). También podría argumentarse algo similar de proyectos procedentes de occidente. En cualquier caso, no puede concluirse que todas las iniciativas sean vectores de medidas activas.

[8]Abrams, S. (2016). «Beyond propaganda: Soviet active measures in Putin's Russia». Connections, vol. 15 n.º 1, pp. 5-31.

[9]Jeangène, J. et al. (2018): Information Manipulation: A Challenge for Our Democracies. París: CAPS-IRSEM.

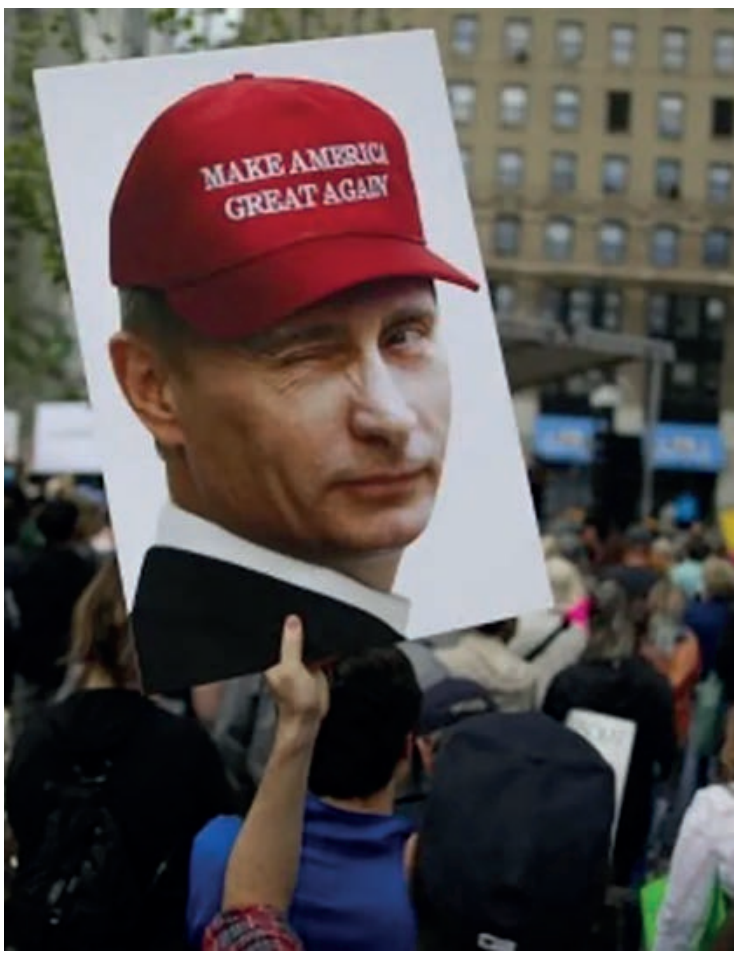
[10]Department of Justice (2019): Report on the Investigation into Russian Interference in the 2016 Presidential Election. 28 C.F.R. § 600.8(c), pp. 44-49.

[11]Helmus, T. et al. (2018). Russian social media influence. Understanding Russian propaganda in Eastern Europe. Santa Monica: RAND Corporation

[12]Ello no significa que cualquier actor que explique, relativice o contextualice las actividades rusas pueda desacreditarse acusándole de colaborador. Algo similar podría decirse de los actores que diseminan voluntaria o involuntariamente narrativa antirusa. Al final, en muchos casos, se trata de actividades para influir en la opinión pública.

[13]Villalón, A. (2016). «La Comunidad de Ciberinteligencia rusa», Security Art Work [en línea] https://www.securityartwork.es/2016/11/28/la-cci-rusa-i-introduccion-vienen-los-rusos/

[14]Un hack&leak físico podría ser el intento de infiltración de la KGB en el partido republicano para obtener información que pudiera comprometer a Ronald Reagan e influir en los comicios presidenciales de 1984. Esta operación se habría realizado junto con la popularización del eslogan «Reagan means war», la difusión de bulos sobre sus supuestas actividades ilícitas y simpatías con macartismo o la crítica a su política exterior, responsabilizándole de la carrera de armamentos y las tensiones con los aliados o su apoyo a regímenes autoritarios.



[15]Por ejemplo, mediante guccifer 2.0, responsable del #DCleaks o el grupo hacktivista cyberberkut, activo en el conflicto ucraniano, en ambos casos se trata de operativos vinculados con el GRU.

[16]Operativo desde 2013, la Internet Research Agency (IRA) emplea un millar de trabajadores que participan en medios, blogs, foros o redes sociales. Apoyados por redes de bots para amplificar el mensaje, estos pueden emplearse tanto para fines comerciales como para difundir desinformación en múltiples contextos. La fiscalía estadounidense los calificó como una organización implicada en operaciones para interferir en procesos políticos por sus posibles relaciones con la inteligencia rusa y su intromisión en los comicios estadounidenses. Sin embargo, también puede apoyar la desinformación y la maskirovka a nivel militar (DiResta, R. et al. (2018). The tactics & tropes of the Internet Research Agency. Austin: New Knowledge).

[17]Select Committee on Intelligence (2018): Report on Russian active measures, Washington DC: House of Representatives.

[18]Kreps, Sarah (2020): The role of technology in online misinformation. Washington DC: Brookings [en línea] https://www.brookings.edu/wp-content/uploads/2020/06/The-role-of-technology-in-online-misinformation.pdf