Computational Propaganda Research Project

OXFORD INTERNET INSTITUTE

UNIVERSITY OF OXFORD

EL ORDEN GLOBAL DE LA DESINFORMACIÓN
INVENTARIO GLOBAL DE LA MANIPULACIÓN ORGANIZADA DE REDES SOCIALES 2019

Samantha Bradshaw. Universidad de Oxford
Philip N. Howard. Universidad de Oxford

RESUMEN EJECUTIVO

La propaganda computacional –uso de algoritmos, automatización y big data para afectar la esfera pública– se está volviendo una parte cada vez más presente en de la vida diaria.

Durante los últimos tres años hemos monitoreado la organización global de la manipulación de las redes sociales por parte de gobiernos y partidos políticos. Nuestro reporte de 2019 analiza las tendencias de la propaganda computacional y las herramientas, capacidades, estrategias y recursos que se van desarrollando.

1. Evidencia de campañas de manipulación de redes sociales organizadas formalmente en 70 países, en comparación a 48 países en 2018 y a 28 países en 2017. En cada país existe al menos un partido político u organismo de gobierno que utiliza las redes sociales para manipular la opinión pública a nivel local (Figura 1).

2. Muchos regímenes autoritarios han cooptado de las redes sociales. En 26 países la propaganda computacional está siendo utilizada como una herramienta de control de la información de tres maneras distintas: para suprimir derechos humanos fundamentales, desacreditar a la oposición política y acallar opiniones discrepantes (Figura 2).

3. Un pequeño grupo de sofisticados actores de estado utiliza la propaganda computacional para operaciones de injerencia extranjera. Facebook y Twitter atribuyeron operaciones de injerencia extranjera a siete países (China, India, Irán, Pakistán, Rusia, Arabia Saudí y Venezuela), que utilizaron estas plataformas para manipular audiencias globales. (Figura 3).

4. China se ha convertido en un actor importante en el orden global de la desinformación. Hasta la protesta de 2019 en Hong Kong, la mayor parte de evidencia de propaganda computacional en China se centraba en plataformas locales como Weibo, WeChat y QQ. Pero el nuevo interés de China en el uso agresivo de Facebook, Twitter y YouTube debe generar preocupación entre las democracias.

5. A pesar de que existen más plataformas de redes sociales que nunca, Facebook continúa siendo la más popular cuando se trata de manipulación de redes sociales. En 56 países encontramos evidencia de campañas organizadas de propaganda computacional en Facebook (Figura 4).

ÍNDICE

ILUSTRACIONES

INTRODUCCIÓN

Alrededor del mundo, actores gubernamentales usan las redes sociales para moldear el consenso, automatizar la represión y debilitar la confianza en el orden liberal del mundo.

Si bien la propaganda siempre ha formado parte del discurso político, el alcance amplio y profundo de estas campañas genera gran preocupación en asuntos de interés público.

Las tropas cibernéticas son definidas como actores de gobierno o de partidos políticos que tienen el objetivo de manipular la opinión pública en línea (Bradshaw y Howard 2017a). Hemos estudiado comparativamente la organización formal de las tropas cibernéticas en todo el mundo y la manera en la que estos actores usan la propaganda computacional para fines políticos. Esto implica crear un inventario de estrategias, herramientas y técnicas de propaganda computacional en desarrollo, incluyendo el uso de "bots políticos" para reforzar discursos de odio u otras formas de contenido manipulado, acopiar información de manera ilegal o de objetivos específicos (micro-targeting), o desplegar un ejército de "troles" para intimidar u hostigar en línea a disidentes políticos o periodistas. También monitoreamos la capacidad y los recursos invertidos en el desarrollo de estas técnicas, con la finalidad de hacernos una idea de las capacidades de las tropas cibernéticas en todo el mundo.

El uso de propaganda computacional para manipular la opinión pública a través de las redes sociales se ha convertido en un fenómeno generalizado, y se extiende mucho más allá de las malas acciones de un puñado de actores deshonestos. En un entorno de la información caracterizado por grandes volúmenes de información y niveles limitados de atención y confianza del usuario, las herramientas y técnicas de propaganda computacional se están convirtiendo en un componente habitual –y probablemente esencial– en las campañas digitales y hasta la diplomacia pública. Además de elaborar un cuadro comparativo a nivel mundial de las actividades de las tropas cibernéticas, también esperamos promover el debate público y académico sobre cómo definimos y entendemos la naturaleza cambiante de la política en línea y cómo estas tecnologías pueden y deben ser usadas para reforzar la democracia y la libertad de expresión de los derechos humanos en línea.

En el informe de este año analizamos las actividades de las tropas cibernéticas en 70 países: Angola, Argentina, Armenia, Australia, Austria, Azerbaiyán, Baréin, Bosnia y Herzegovina, Brasil, Camboya, China, Colombia, Croacia, Cuba, República Checa, Ecuador, Egipto, Eritrea, Etiopía, Georgia, Alemania, Grecia, Honduras, Guatemala, Hungría, India, Indonesia, Irán, Israel, Italia, Kazajstán, Kenia, Kirguistán, Macedonia, Malasia, Malta, México, Moldavia, Myanmar, Holanda, Nigeria, Corea del Norte, Pakistán, Filipinas, Polonia, Qatar, Rusia, Ruanda, Arabia Saudita, Serbia, Sudáfrica, Corea del Sur, España, Sri Lanka, Suecia, Siria, Taiwán, Tayikistán, Tailandia, Túnez, Turquía,

Ucrania, Emiratos Árabes, Reino Unido, Estados Unidos, Uzbekistán, Venezuela, Vietnam y Zimbabue.

Evidencia creciente de propaganda computacional en todo el mundo

Hallamos evidencia de campañas de manipulación de redes sociales organizadas en 70 países, en comparación a 48 países en 2018 y a 28 países en 2017. Entre las razones de este incremento figura el ingreso de nuevos participantes que experimentan con herramientas y técnicas de propaganda computacional durante las elecciones o como una nueva herramienta de control de la información. Sin embargo, los periodistas, académicos y activistas también están mejor equipados con herramientas digitales y vocabulario más preciso para identificar, reportar y descubrir casos de manipulación de redes sociales formalmente organizadas. Durante los últimos tres años hemos logrado perfeccionar nuestro lenguaje y palabras de búsqueda para identificar casos de propaganda computacional, y nos dimos cuenta que muchos países muestran elementos de manipulación de redes sociales formalmente organizados en la última década. Como resultado, señalamos que la propaganda computacional se ha convertido en una práctica generalizada y extendida dentro del ecosistema de la información digital.

Apropiación de las redes sociales por regímenes autoritarios

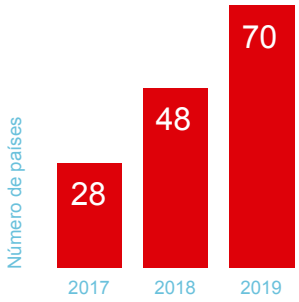
En muchos regímenes autoritarios, la propaganda computacional se ha convertido en una herramienta de control de la información usada estratégicamente en combinación con la vigilancia, censura y amenazas de violencia. Hemos catalogado los tipos de campañas usadas en países autoritarios contra periodistas, disidentes políticos y la sociedad en general, y encontramos tres formas características de uso de la propaganda computacional:

(1) para suprimir derechos humanos fundamentales
(2) para desacreditar a la oposición política
(3) para acallar el disenso político

La apropiación de las tecnologías de las redes sociales ofrece a los regímenes autoritarios una poderosa herramienta para manipular el debate público y difundir propaganda en línea, ejerciendo al mismo tiempo el control, la censura y la restricción del espacio público digital.

Un número limitado de operaciones de injerencia extranjera por parte de actores

Las operaciones de injerencia extranjera constituyen un ámbito importante de preocupación, pero imputar propaganda computacional a actores de estado extranjeros sigue siendo un problema. Facebook y Twitter –que han empezado a publicar algo de información sobre operaciones de injerencia en sus plataformas– han tomado acciones contra las tropas cibernéticas involucradas en operaciones de injerencia



150%

el aumento de países que utilizan campañas organizadas de manipulación de redes sociales en los últimos dos años.

extranjera en siete países: China, India, Irán, Pakistán, Rusia, Arabia Saudita y Venezuela. Si bien esta medida no refleja el alcance que tienen las operaciones de injerencia extranjera, podemos empezar a elaborar un panorama más preciso de este fenómeno altamente reservado.

China demuestra su fuerza en el campo de la desinformación

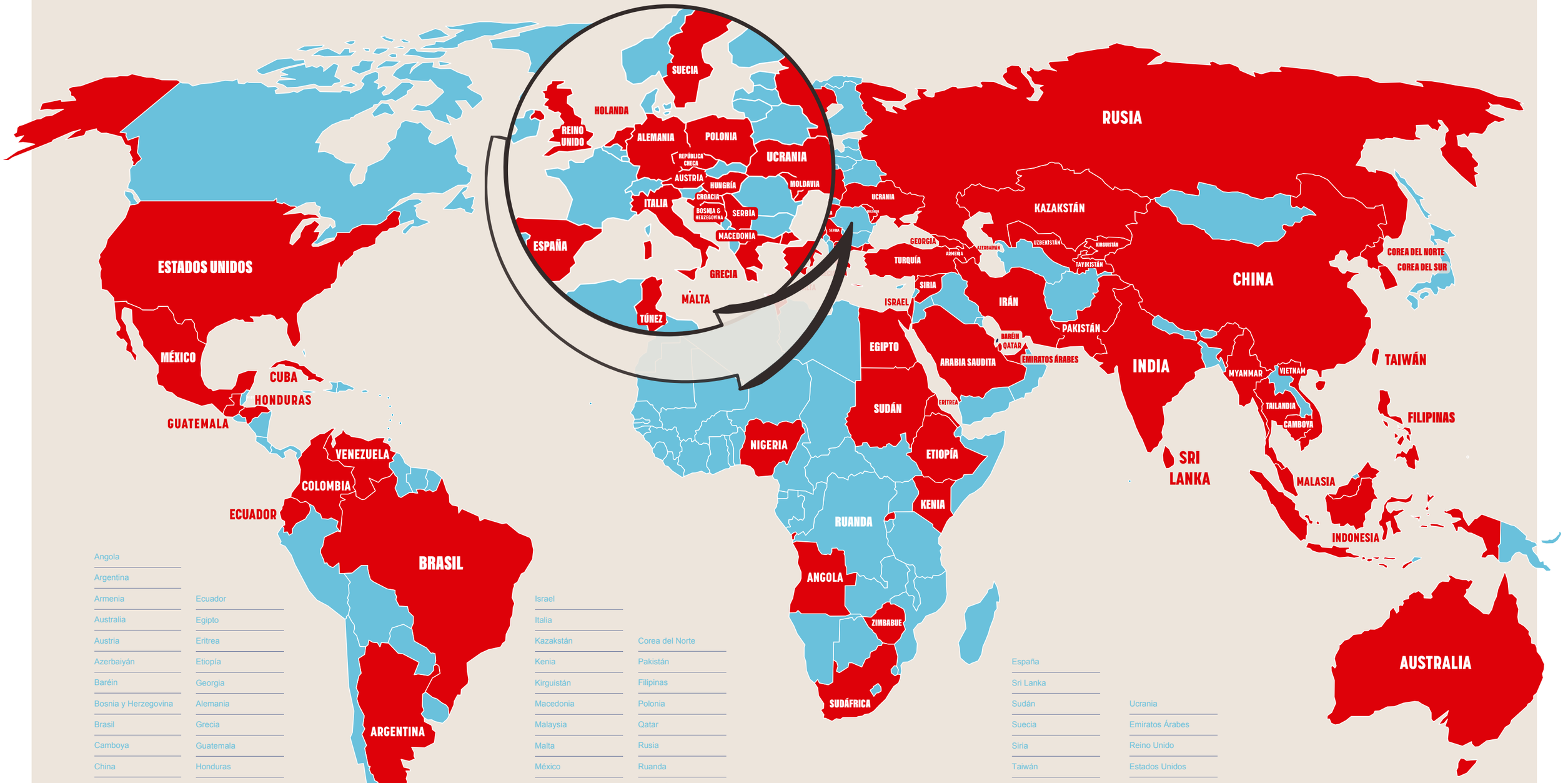
Hasta hace poco, China usaba las redes sociales rara vez para manipular la opinión pública en otros países. La audiencia de propaganda computacional se ha centrado mayormente en plataformas locales como Weibo, WeChat y QQ. Sin embargo, en 2019, el gobierno chino empezó a usar las plataformas de redes sociales para presentar a los defensores de la democracia como radicales violentos carentes de apoyo popular (Lee Myers y Mozur 2019). Más allá de las plataformas destinadas al plano local, la creciente sofisticación y uso de tecnologías de redes sociales globales demuestra cómo China también está volcándose hacia dichas tecnologías como una herramienta de influencia y control geopolítico.

Facebook continúa siendo número uno

A pesar de que existen más plataformas que nunca, Facebook sigue siendo la plataforma dominante en el campo de las actividades de las tropas cibernéticas. Esto podría explicarse, en parte, por el tamaño de su mercado –una de las plataformas de redes sociales más grandes del mundo–, así como por las posibilidades de acción específicas de la plataforma, tales como una comunicación cercana con la familia y amigos, una fuente de noticias políticas e información, o la capacidad para crear grupos y páginas. Desde 2018, hemos encontrado evidencia de una mayor actividad de las tropas cibernéticas en las plataformas que comparten imágenes y videos, tales como Instagram y YouTube. También hemos hallado evidencia de tropas cibernéticas organizando campañas por WhatsApp. Creemos que estas plataformas irán cobrando mayor importancia en los próximos años, a medida que más gente use las tecnologías de redes sociales con fines de comunicación política.

GRÁFICO 1. EL ORDEN GLOBAL DE LA DESINFORMACIÓN

PAÍSES QUE PARTICIPAN EN LA MANIPULACIÓN DE LAS REDES SOCIALES



Angola
Argentina
Armenia
Australia
Austria
Azerbaiyán
Baréin
Bosnia y Herzegovina
Brasil
Camboya
China
Colombia
Croacia
Cuba
República Checa

Ecuador
Egipto
Eritrea
Etiopía
Georgia
Alemania
Grecia
Guatemala
Honduras
Hungría
India
Indonesia
Irán

Israel
Italia
Kazakstán
Kenia
Kirguistán
Macedonia
Malaysia
Malta
México
Moldavia
Myanmar
Holanda
Nigeria

Corea del Norte
Pakistán
Filipinas
Polonia
Qatar
Rusia
Ruanda
Arabia Saudita
Serbia
Sudáfrica
Corea del Sur

España
Sri Lanka
Sudán
Suecia
Siria
Taiwán
Tayikistán
Tailandia
Túnez
Turquía

Ucrania
Emiratos Árabes
Reino Unido
Estados Unidos
Uzbekistán
Venezuela
Vietnam
Zimbabue

GRÁFICO 2. PROPAGANDA COMPUTACIONAL COMO HERRAMIENTA DE CONTROL DE LA INFORMACIÓN

PAÍSES AUTORITARIOS QUE UTILIZAN PROPAGANDA COMPUTACIONAL

GRÁFICO 3. OPERACIONES DE INJERENCIA EXTRANJERA EN REDES SOCIALES

PAÍSES SEÑALADOS POR FACEBOOK Y TWITTER POR PARTICIPAR EN OPERACIONES DE INJERENCIA EXTRANJERA

Fuente: Evaluaciones de los autores en base a la información recopilada. **Nota:** Facebook también ha cerrado cuentas relacionadas con "comportamiento inauténtico coordinado", que no están explícitamente vinculadas con un gobierno o partido político. Estos cierres incluyen cuentas que se originan en: Egipto, Macedonia, Kosovo, Tailandia y Emiratos Árabes. Adicionalmente, algunas actividades de tropas cibernéticas identificadas por Facebook y Twitter se centran en el ámbito local, como es el caso de Bangladesh u Honduras y, por lo tanto, no se incluyen en este gráfico de operaciones extranjeras.

GRÁFICO 4. PLATAFORMAS PROMINENTES PARA LA MANIPULACIÓN DE REDES SOCIALES

PLATAFORMAS DE REDES SOCIALES UTILIZADAS PARA ACTIVIDADES DE TROPAS CIBERNÉTICAS

METODOLOGÍA DEL INFORME

La metodología de este informe consta de 4 pasos:

1. Análisis de contenido sistemático de noticias que reportan actividades de tropas cibernéticas

2. Revisión de fuentes secundarias de archivos públicos e informes científicos

3. Elaboración de estudios de caso de país

4. Consultas con expertos

Durante los últimos tres años, nuestra metodología de tres pasos nos permitió acceder a un amplio rango de documentos públicos que contribuían a explicar las campañas organizadas de manipulación a nivel mundial. Es muy posible que existan operaciones de tropas cibernéticas que no han sido documentadas abiertamente, y ya hemos visto que estos casos aumentan con el tiempo. Si bien este informe no pretende brindar un panorama completo de cómo los actores de Estado están operando en este espacio, sí podemos empezar a elaborar un panorama más preciso recomponiendo la información pública. En la página web del informe de 2019 se pueden encontrar los perfiles específicos de país y una lista completa de noticias y fuentes secundarias.

El análisis de contenido es un método de investigación establecido en el campo de los estudios de medios y comunicación (Herring 2009). Ha sido usado para ayudar a entender cómo el Internet y las redes sociales interactúan con la acción política, transformación de regímenes y control digital (Bradshaw y Howard 2018a, 2017b; Edwards, Howard y Joyce 2013; Joyce, Antonio y Howard 2013; Strange et al. 2013). Este análisis de contenido cualitativo fue realizado para conocer mejor a los actores de Estado que usan activamente las redes sociales para manipular la opinión pública, así como su capacidad, estrategias y recursos con los que cuentan. Elaboramos nuestro análisis de contenido en base al informe del año pasado, usando el muestreo intencional para trabajar una hoja de cálculo codificada con variables específicas que aparecen en los artículos noticiosos. Las siguientes palabras clave fueron elegidas y usadas de manera combinada en nuestra investigación: bot, Cambridge Analytica, desinformación, Facebook, cuenta falsa, guerra de la información, Instagram, militar, información falsa, propaganda, operaciones psicológicas, redes sociales, identidad falsa (sock puppet), troles, Twitter, WhatsApp, YouTube.

Existen dos limitaciones importantes para la elaboración de nuestro análisis de contenido cualitativo: el sesgo y lenguaje de las redes. Para mitigar el sesgo, usamos LexisNexis y los tres principales proveedores de motores de búsqueda –Google, Yahoo! y Bing–, que ofrecen hits a diversas fuentes de noticias profesionales, locales y de aficionados. Para asegurarnos de incluir solo fuentes noticiosas de alta calidad en la creación de nuestro conjunto de datos, usamos un puntaje de credibilidad para cada artículo, en base a una escala de tres puntos. Los artículos calificados con uno provenían de medios de prensa importantes y profesionales. Los artículos clasificados con dos provenían de medios más pequeños y locales, así como de comentarios de expertos y blogs profesionales. Los artículos clasificados con tres provenían de “granjas de contenidos”, blogs personales o “partidistas acérrimos”. Estos artículos eran retirados de la muestra.

El lenguaje fue una segunda limitación al momento de realizar nuestro análisis. Para el inventario mundial de este año, pudimos aprovechar noticias y fuentes secundarias escritas en árabe, inglés, francés, alemán, griego, húngaro, italiano, persa, polaco, portugués, ruso y español. También trabajamos con BBC Monitoring , que nos ofreció un portal adicional para recabar y agregar noticias e información de primera calidad relacionadas con las actividades de las tropas cibernéticas, así como servicios de traducción para noticias provenientes de Bosnia, Croacia, Georgia, Kazajistán, Kirguizistán, Malasia, Macedonia del Norte, Taiwán, Tayikistán, Turkmenistán y Uzbekistán. Utilizamos información de noticias escritas solo en inglés en el caso de Armenia, Azerbaiyán, Camboya, China, República Checa, Eritrea, Etiopía, Hungría, Israel, Moldavia, Myanmar, Holanda, Corea del Norte, Pakistán, Filipinas, Serbia, Corea del Sur, Sri Lanka, Tailandia, Turquía y Vietnam.

Después de realizar un análisis de contenido, un equipo de asistentes de investigación terminó la revisión de fuentes secundarias, brindando con ello un perfil detallado de las actividades de las tropas cibernéticas en un contexto específico de país. Estos estudios de caso se basaron en la información recopilada en el análisis de contenido, así como en la revisión de las fuentes secundarias detalladas, mientras que los autores de los estudios de caso buscaron otras fuentes confiables de información de dominio público sobre las actividades de las tropas cibernéticas. Esto implicó buscar informes de gobierno, artículos de grupos de expertos (think tank papers), estudios académicos e investigaciones realizadas por organizaciones de la sociedad civil. Se puede encontrar un archivo completo de las fuentes noticiosas y fuentes secundarias utilizadas en este informe en la base de datos en línea Zotero. Esperamos que esta biblioteca pública sirva para investigaciones futuras.

Después de terminar el análisis de contenido cualitativo y la revisión de fuentes secundarias, los asistentes de investigación sintetizaron los hallazgos en breves estudios de caso de país. Los estudios de caso brindan más información sobre los casos de propaganda computacional que identificamos en el análisis de contenido, así como información detallada sobre el contexto específico de país y el entorno mediático en el que tiene lugar la manipulación de redes sociales. Además del análisis de contenido y la revisión de fuentes secundarias, terminamos los estudios de caso para el 84% de países, los cuales se pueden encontrar en línea como complemento de la información junto con este informe.

Finalmente, el último paso de nuestra metodología de investigación –consultas con expertos–permitió que los estudios de caso fueran revisados por pares, así como recibir feedback sobre la calidad de la cobertura informativa y las fuentes secundarias que encontramos, y discutir sobre los recursos adicionales y referencias en distintos idiomas con hablantes nativos. Se pidió a los expertos revisar los estudios de caso elaborados por los asistentes de investigación, así como (1) la verificación de datos e información para comprobar su exactitud; (2) brindar referencias adicionales al material de dominio público; y (3) ofrecer feedback general sobre la fiabilidad de la información. En los casos de Polonia, Sri Lanka, Taiwán, Túnez y Ucrania, consultamos con especialistas la información recopilada en el análisis de contenido y la revisión de las fuentes.

1 https://monitoring.bbc.co.uk/

FORMA DE ORGANIZACIÓN

Las actividades de las tropas cibernéticas tienen muchas formas de organización y diversos actores aprovechan las redes sociales para manipular la opinión pública, establecer agendas políticas y difundir ideas.

Si bien muchos países vienen siendo testigos de un aumento de la propaganda computacional en las redes sociales, atribuir este fenómeno a un actor en particular sigue siendo problemático.

En este informe nos centramos específicamente en las tropas cibernéticas –o en el uso de las redes sociales por parte de los gobierno o de los partidos políticos– para manipular la opinión pública. En 44 países encontramos evidencia de algún organismo de gobierno usando propaganda computacional para este fin. En esta categoría de actores están incluidos los ministerios de comunicaciones o digitales, o campañas dirigidas por los militares. En los países que no son considerados libres, por la organización Freedom House, encontramos evidencia de un ministerio de gobierno o partido en el poder usando propaganda computacional para manipular la opinión a nivel local. En un pequeño número de democracias, encontramos evidencia de iniciativas lideradas por el gobierno o los militares. En el caso del presente informe, incluimos las actividades de Joint Threat Research Intelligence Group (JTRIG) en el Reino Unido, que estructuró grupos en Facebook y creó videos en YouTube conteniendo comunicaciones persuasivas diseñadas para “desacreditar, generar desconfianza, disuadir, frenar, retrasar y perturbar” (Greenwald 2015). También consideramos algunas actividades en los Estados Unidos, tales como el programa de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID por sus siglas en inglés), que creó redes sociales falsas en Cuba (Greenwald 2014). A medida que la propaganda computacional se vuelve una herramienta dominante en el campo de la política, la seguridad nacional y las operaciones de inteligencia, esperamos que estos ejemplos promuevan el debate sobre el uso apropiado, democrático y aceptable de dichas herramientas en manos de los actores de estado.

Además de las iniciativas gubernamentales y militares, también tomamos en cuenta a los partidos políticos. En 45 de los 70 países analizados, hallamos evidencia de partidos políticos o políticos que postulaban a cargos públicos usando herramientas y técnicas de propaganda computacional durante las elecciones. Aquí, consideramos los casos de políticos acumulando seguidores falsos, tales como Mitt Romney en los Estados Unidos (Carroll 2012), Tony Abbott en Australia (Rolfe 2013) o Geert Wilders en Holanda (Blood 2017). También incluimos casos de partidos que usan publicidad para captar votantes con redes manipuladas, como por ejemplo en India (Gleicher 2019), o casos de captaciones ilegales más específicas aún, como el uso de la empresa Cambridge Analytica en el referéndum del Brexit en el Reino Unido por Vote Leave (Cadwalladr 2017). Por último, consideramos otros casos de partidos políticos que difunden o magnifican intencionalmente la desinformación en las redes sociales, como las campañas por WhatsApp en Brasil (Rio 2018), India (Dwoskin y Gowen 2018) y Nigeria (Hitchen et al. 2019).

Una característica importante de la organización de las campañas de manipulación es que las tropas cibernéticas trabajan a menudo junto con la empresa privada, organizaciones de la sociedad civil, subculturas de Internet, grupos de jóvenes, colectivos de hackers, movimientos extremistas, influencers en redes sociales y voluntarios que apoyan su causa en términos ideológicos. La distinción entre estos grupos puede ser a menudo difícil de establecer, sobre todo considerando que las actividades pueden ser sancionadas implícita y explícitamente por el Estado. En este informe, buscamos evidencia de coordinación formal o de actividades que son oficialmente sancionadas por el Estado, más que campañas que podrían ser implícitamente coordinadas debido a factores como ideologías o metas que se comparten. En 25 de los 70 países encontramos evidencia de actores de Estado trabajando con compañías privadas o empresas de comunicación estratégica que ofrecían propaganda computacional como uno de sus servicios. En 30 de los 70 países hallamos evidencia de coordinación formal entre el gobierno y la ciudadanía u organizaciones de la sociedad civil. En algunos casos, como en Azerbaiyán, Israel, Rusia, Tayikistán y Uzbekistán, los organismos de gobierno contratan a grupos de jóvenes para usar propaganda computacional.

TABLA 1. FORMA DE ORGANIZACIÓN Y PREVALENCIA DE LA MANIPULACIÓN DE REDES SOCIALES

País	Organismos de gorbierno	Políticos y Partidos	Contratistas Privados	Organizaciones de la sociedad civil	Ciudadanía e influenciadores
Angola	■	■			
Argentina	■	■	■		
Armenia	■				
Australia		■			
Austria		■	■		
Azerbaiyán	■			■	■
Baréin	■		■		■
Bosnia y Herzegovina	■				
Brasil		■	■		■
Camboya	■	■			■
China	■		■	■	
Colombia		■	■		
Croacia		■			
Cuba	■			■	
República Checa		■			
Ecuador		■			
Egipto	■	■			■
Eritrea	■				
Etiopía	■				
Georgia	■		■	■	
Alemania		■		■	
Grecia		■			
Guatemala	■	■	■		■
Honduras	■				
Hungary	■				
India		■	■	■	■
Indonesia		■	■		
Irán	■				■
Israel	■	■		■	
Italia		■			■
Kazajistán	■	■			
Kenia		■	■		
Kirguistán		■	■		■
Macedonia		■			■
Malasia	■	■	■	■	■

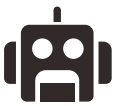
País	Organismos de gorbierno	Políticos y Partidos	Contratistas Privados	Organizaciones de la sociedad civil	Ciudadanía e influenciadores
Malta	■	■	■		
México		■	■	■	
Moldavia	■	■			
Myanmar	■				
Holanda		■			
Nigeria	■	■	■		
Corea del Norte	■				
Pakistán	■	■			
Filipinas	■	■	■	■	■
Polonia		■	■		
Qatar	■				
Rusia	■		■	■	
Ruanda	■	■			
Arabia Saudita	■		■	■	■
Serbia	■	■		■	
Sudáfrica		■	■		
Corea del Sur		■			
España		■		■	
Sri Lanka	■	■			
Sudan	■			■	
Suecia		■			
Siria	■		■	■	
Taiwán		■	■		
Tayikistán	■				■
Tailandia	■				■
Túnez		■			
Turquía	■	■			■
Ucrania	■			■	
Emiratos Árabes	■		■	■	■
Reino Unido	■	■	■		
Estados Unidos	■	■	■		
Uzbekistán	■			■	■
Venezuela	■	■	■	■	
Vietnam	■				■
Zimbabue		■			

Fuente: Evaluaciones de los autores en base a la información recopilada. **Nota:** Esta tabla indica los tipos de actores políticos que recurren a operaciones de influencia a través de las redes sociales y el número de ejemplos de las organizaciones encontradas. En el caso de organismos de gobierno, partidos políticos, agrupaciones de la sociedad civil y contratistas privados, ■= una organización encontrada; ■= dos organizaciones encontradas; ■= tres o más organizaciones encontradas. Dado que es difícil calcular el número de ciudadanos individuales usando estas herramientas, la evidencia de uso de esta categoría se indica con ■.

ESTRATEGIAS, HERRAMIENTAS Y TÉCNICAS

Si bien no hay nada necesariamente nuevo sobre la propaganda, los ofrecimientos de las tecnologías de las redes sociales –algoritmos, automatización y *big data*– cambian la dimensión, alcance y precisión de cómo se transmite la información en la era digital.

87%
de los países usaron cuentas humanas



80%
de los países usaron cuentas bot

11%
de los países usaron cuentas cyborg

7%
de los países usaron cuentas pirateadas o robadas

Tipos de cuentas

Las cuentas falsas son usadas por las tropas cibernéticas para difundir propaganda computacional. En los últimos tres años hemos rastreado el predominio de tres tipos de cuentas falsas: bot, humanas y cyborg. Las bots son cuentas altamente automatizadas, diseñadas para imitar el comportamiento humano en línea. A menudo son usadas para reforzar discursos o para acallar el disenso político. Encontramos evidencia de cuentas bot en 50 de los 70 países analizados. Sin embargo, incluso más comunes que este tipo de cuentas son aquellas administradas por personas, que no hacen uso de la automatización. En vez de eso, se involucran en conversaciones posteando comentarios o tweets, o enviando mensajes privados a personas a través de las plataformas de redes sociales. En el informe de este año se encontraron cuentas operadas por personas en 60 de los 70 países. Las cuentas cyborg, que combinan la automatización con la operación humana, son otro tipo de cuentas que pudimos identificar.

Este año hemos añadido a nuestra tipología de cuentas falsas, las cuentas pirateadas o robadas. Si bien estas cuentas no son "falsas" per se, las cuentas de perfil alto son usadas estratégicamente por las tropas cibernéticas para difundir propaganda en favor del gobierno o para censurar la libertad de expresión al revocar el acceso a la cuenta por parte de su propietario legítimo. Un pequeño número de actores de Estado ha empezado a usar cuentas pirateadas o robadas en sus campañas, evidenciando la interconectividad de la propaganda computacional con formas más tradicionales de ataques cibernéticos.

Por último, es importante observar que no todas las cuentas usadas en las actividades de las tropas cibernéticas son falsas. En algunos países como Vietnam o Tayikistán, los actores de Estado animan a las tropas cibernéticas a usar sus cuentas verdaderas para difundir propaganda en favor del gobierno, trolear a disidentes políticos o hacer denuncias masivas de contenidos. A medida que las compañías de redes sociales se vuelven más agresivas para cerrar las cuentas asociadas con actividades de tropas cibernéticas, la integración de cuentas verdaderas podría convertirse en una estrategia más prominente.

TABLA 2. TIPOS DE CUENTAS FALSAS

País	Bots	Humana	Cyborg	Pirateada o robada
Angola	●			
Argentina	●	●		
Armenia	●	●		
Australia	●	●		
Austria	●	●		
Azerbaiyán	●	●		
Baréin	●	●		
Bosnia y Herzegovina		●		
Brasil	●	●	●	
Camboya	●			
China	●	●		
Colombia	●	●		
Croacia		●		
Cuba	●			
República Checa		●		
Ecuador		●		
Egipto	●	●		
Eritrea		●		
Etiopía		●		
Georgia	●	●		
Alemania	●	●	●	
Grecia	●	●		
Guatemala	●	●		●
Honduras		●		
Hungría	●	●		
India	●	●		
Indonesia	●	●		
Irán	●	●		●
Israel	●	●		
Italia	●			
Kazajistán	●	●		
Kenia	●	●		
Kirguistán		●		
Macedonia	●	●		
Malasia	●			

País	Bots	Humana	Cyborg	Pirateada o robada
Malta	●	●		
México	●	●	●	
Moldavia	●	●		
Myanmar	●	●		
Holanda	●			
Nigeria	●	●		
Corea del Norte		●		●
Pakistán	●	●		
Filipinas	●	●		
Polonia	●			
Qatar	●			
Rusia	●	●	●	●
Ruanda		●		
Arabia Saudita	●	●	●	
Serbia	●	●		
Sudáfrica	●	●		
Corea del Sur	●	●		
España	●	●		
Sri Lanka	●	●	●	
Sudan		●		
Suecia	●	●		
Siria	●	●		
Taiwán	●			
Tayikistán		●		
Tailandia	●	●		
Túnez	●	●		
Turquía	●	●		
Ucrania	●	●		
Emiratos Árabes	●	●		
Reino Unido	●	●	●	
Estados Unidos	●	●	●	
Uzbekistán		●		●
Venezuela	●	●		
Vietnam		●		
Zimbabue	●	●		

Fuente: Evaluaciones de los autores en base a la información recopilada. **Nota:** Esta tabla muestra los tipos de cuentas falsas identificadas entre 2010-2019. Para tipos de cuentas de redes sociales falsas: ● =cuentas automatizadas, ● =cuentas humanas, ● =cuentas cyborg, ● =cuentas pirateadas o robadas, ● ● ● ● =no se encontró evidencia.

71%
difundió propaganda en favor del gobierno o del partido

89%
usó propaganda para atacar a la oposición política

34%
difundió mensajes polarizadores diseñados para generar divisiones en la sociedad

Mensajería y valencia

Las tropas cibernéticas usan diversas estrategias de mensajería y valencia al momento de comunicarse con los usuarios en línea. La valencia describe cuán atractivo o poco atractivo resulta un mensaje o una cosa. En el caso del informe de 2019, hemos ampliado nuestra tipología de estrategias de mensajería y valencia usadas por las tropas cibernéticas al momento de trabar conversación con los usuarios en línea:

1. difundir propaganda en favor del gobierno o del partido.
2. atacar a la oposición o montar campañas de desprestigio.
3. conversaciones distractoras o críticas para alejar los temas importantes.
4. generar división y polarización.
5. reprimir la participación a través de ataques personales o acoso.

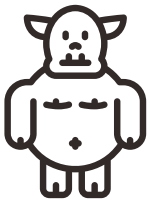
TABLA 3. MENSAJERÍA Y VALENCIA

País	Apoyo	Ataques a la Oposición	Recursos Distractores	Generando División	Reprimiendo
Angola		●			●
Argentina	●	●		●	●
Armenia		●	●	●	●
Australia	●	●			
Austria		●			●
Azerbaiyán	●	●			●
Baréin	●	●		●	●
Bosnia y Herzegovina	●	●	●	●	●
Brasil	●	●	●	●	●
Camboya	●	●			
China	●	●			●
Colombia	●	●		●	
Croacia				●	
Cuba	●	●			●
República Checa		●			
Ecuador		●	●		●
Egipto	●	●			●
Eritrea		●			●
Etiopía	●	●			
Georgia	●	●			●
Alemania	●	●		●	
Grecia		●			●
Guatemala	●	●			●
Honduras	●				
Hungría	●	●	●	●	●
India	●	●		●	
Indonesia	●	●		●	
Irán	●	●			●
Israel	●				
Italia			●	●	
Kazajistán	●	●	●		
Kenia	●	●			
Kirguistán	●	●			●
Macedonia		●		●	●
Malasia	●	●			●

País	Apoyo	Ataques a la Oposición	Recursos Distractores	Generando División	Reprimiendo
Malta		●			●
México	●	●			●
Moldavia	●	●		●	
Myanmar	●	●		●	●
Holanda				●	
Nigeria		●			●
Corea del Norte	●	●			
Pakistán	●	●			●
Filipinas	●	●		●	●
Polonia		●			
Qatar	●				
Rusia	●	●	●	●	●
Ruanda		●			●
Arabia Saudita	●	●		●	●
Serbia	●	●			●
Sudáfrica	●	●			●
Corea del Sur	●	●			
España		●		●	
Sri Lanka	●	●		●	●
Sudan		●			●
Suecia				●	
Siria	●	●	●		●
Taiwán	●	●	●		
Tayikistán	●	●			●
Tailandia	●	●			●
Túnez	●	●			
Turquía	●	●			●
Ucrania	●	●			●
Emiratos Árabes	●	●			●
Reino Unido	●	●	●	●	
Estados Unidos	●	●	●	●	●
Uzbekistán		●			●
Venezuela	●	●	●		●
Vietnam	●	●			●
Zimbabue	●	●			●

Fuente: Evaluaciones de los autores en base a la información recopilada. **Nota:** Esta tabla muestra los tipos de estrategias de mensajería y valencia de las actividades de las tropas cibernéticas entre 2010-2019. Para comentarios en redes sociales: =apoyo, =ataques a la oposición, =recursos distractores, =generando división, =reprimiendo, =no se encontró evidencia.

75%
de los países usó desinformación y manipulación de las redes para confundir a los usuarios.



68%
de los países usó el troleo patrocinado por el estado en contra de disidentes políticos, la oposición o periodistas

73%
reforzó los mensajes y el contenido con seguimiento de *hashtags*

Estrategias de comunicacións

Las tropas cibernéticas usan diversas estrategias de comunicación. Hemos dividido estas actividades en cinco categorías:

1. Generación de desinformación o manipulación de redes.
2. Denuncias masivas de contenidos o cuentas.
3. Estrategias orientadas a la información.
4. Troles, recopilación de la mayor cantidad de información de una persona (doxing) o acoso.
5. Refuerzo de contenidos y redes en línea.

La generación de desinformación o redes manipuladas es la estrategia de comunicación más común. En 52 de los 70 países analizados, las tropas cibernéticas generaron contenidos en forma de memes, videos, sitios web con noticias falsas o redes manipuladas para confundir a los usuarios. A veces, el contenido generado por las tropas cibernéticas está destinado a comunidades o segmentos específicos de usuarios. Al usar fuentes de datos en línea y fuera de línea sobre los usuarios y al pagar por publicidad en las plataformas populares de las redes sociales, algunas tropas cibernéticas atacan a comunidades específicas con desinformación o redes manipuladas.

El uso de troles, el doxing o el acoso es un problema creciente y resulta una amenaza para los derechos humanos fundamentales. En 2018, identificamos a 27 países usando troles patrocinados por el Estado para atacar a opositores políticos o activistas a través de las redes sociales. Este año, 47 países usaron troles como parte de su arsenal cibernético. Las tropas cibernéticas también censuraron el discurso y la libertad de expresión a través de las denuncias masivas de contenidos o cuentas. Las publicaciones en línea por parte de activistas, disidentes políticos o periodistas a menudo son reportadas por una red de cuentas coordinadas de tropas cibernéticas, que engañan a los sistemas automatizados que las empresas de redes sociales utilizan para retirar contenidos inapropiados. El troleo y cierre de cuentas o posts puede ocurrir junto con la violencia del mundo real, lo que puede generar efectos profundos y paralizadores en materia de expresión de los derechos humanos fundamentales.

TABLA 4. ESTRATEGIAS DE COMUNICACIÓN

País	Desinformación	Denuncias Masivas	Estratégias basadas en datos	Troles	Refuerzo de contenidos
Angola	✓				✓
Argentina	✓		✓	✓	✓
Armenia	✓	✓			✓
Australia					✓
Austria	✓		✓	✓	✓
Azerbaiyán	✓	✓		✓	✓
Baréin				✓	✓
Bosnia y Herzegovina	✓			✓	✓
Brasil	✓		✓	✓	✓
Camboya	✓				✓
China	✓	✓		✓	✓
Colombia	✓			✓	
Croacia	✓				✓
Cuba	✓			✓	✓
República Checa					
Ecuador	✓	✓		✓	
Egipto	✓			✓	✓
Eritrea				✓	
Etiopía	✓			✓	
Georgia	✓			✓	✓
Alemania	✓			✓	✓
Grecia	✓			✓	✓
Guatemala	✓	✓		✓	✓
Honduras	✓		✓		✓
Hungría	✓			✓	✓
India	✓		✓	✓	✓
Indonesia	✓				✓
Irán	✓	✓	✓	✓	✓
Israel	✓		✓		
Italia	✓				✓
Kazajistán	✓				✓
Kenia	✓		✓		✓
Kirguistán				✓	
Macedonia	✓				✓
Malasia	✓		✓		✓
Malta	✓			✓	
México	✓	✓	✓	✓	✓
Moldavia	✓		✓	✓	✓
Myanmar	✓			✓	✓
Holanda	✓				✓
Nigeria	✓		✓	✓	
Corea del Norte	✓				
Pakistán	✓		✓		✓
Filipinas	✓			✓	✓
Polonia				✓	
Qatar					✓
Rusia	✓	✓	✓	✓	✓
Ruanda				✓	
Arabia Saudita	✓			✓	✓
Serbia	✓			✓	✓
Sudáfrica	✓		✓	✓	✓
Corea del Sur					✓
España	✓				
Sri Lanka	✓			✓	✓
Sudan		✓		✓	
Suecia	✓			✓	✓
Siria	✓			✓	✓
Taiwán			✓	✓	
Tayikistán				✓	✓
Tailandia				✓	
Túnez	✓				✓
Turquía		✓		✓	✓
Ucrania	✓			✓	✓
Emiratos Árabes	✓		✓	✓	✓
Reino Unido	✓		✓		✓
Estados Unidos	✓		✓		✓
Uzbekistán				✓	
Venezuela	✓			✓	✓
Vietnam	✓	✓		✓	✓
Zimbabue	✓			✓	

Fuente: Evaluaciones de los autores en base a la información recopilada. **Nota:** Esta tabla muestra las estrategias de comunicación usadas por las tropas cibernéticas. Para estrategias de comunicación: =desinformación y manipulación de redes, =denuncias masivas de contenidos/cuentas, =estrategias basadas en datos, =troles, =refuerzo de contenido, =no se encontró evidencias.

CAPACIDAD, PRESUPUESTO Y COMPORTAMIENTO ORGANIZACIONAL

Si bien existe poca información pública sobre el tamaño y operaciones de los equipos de tropas cibernéticas, podemos empezar a elaborar un panorama de cuánto presupuesto gastan, cómo cooperan y los tipos de comportamientos y capacidad de organización que tienen.

Tamaño del equipo y permanencia

El tamaño y la permanencia de los equipos varían de un país a otro. En algunos países, los equipos aparecen temporalmente durante las elecciones o para influir en la opinión pública en torno a otros temas políticos importantes. En otros, las tropas cibernéticas están integradas en la escena de las redes sociales y las comunicaciones, con un equipo a tiempo completo que trabaja para controlar, censurar y manipular conversaciones e información en línea. Algunos equipos están compuestos por un grupo de personas que manejan centenares de cuentas falsas.

En otros países –como China, Vietnam o Venezuela– el Estado contrata equipos más grandes para manipular activamente la opinión pública y el discurso político a través de canales en línea.

Presupuesto y gastos

La propaganda computacional sigue siendo un gran negocio. Encontramos ingentes cantidades de dinero gastado en empresas de relaciones públicas o de comunicación estratégica para trabajar en campañas en países como Filipinas (Mahtani y Cabato 2019), Guatemala (Currier y Mackey 2018) y Siria (York 2011). Estos contratos varían de tamaño, y van desde pequeños montos pactados con empresas especializadas locales o regionales, hasta contratos millonarios con compañías globales como Cambridge Analytica (ver, por ejemplo, Kazeem 2018).

El aumento de la industria de los troles es un área de creciente interés público y académico, que hay que observar para estudios futuros e investigaciones periodísticas.

Habilidades y difusión de conocimiento

Existe también evidencia sobre la difusión de conocimientos formales e informales que traspasan las fronteras geográficas. Por ejemplo, durante las investigaciones sobre las actividades de las tropas cibernéticas en Myanmar, surgió evidencia que mostraba que oficiales militares estaban siendo capacitados por personal ruso, que les enseñaban cómo usar las redes sociales (Mozur 2018). De igual modo, las tropas cibernéticas en Sri Lanka recibieron capacitación formal en India (consulta con expertos 2019). La filtración de correos electrónicos también ha mostrado evidencia de que la Information Network Agency en Etiopía enviaba a funcionarios para recibir capacitación formal en China (Nunu 2018). Si bien existen todavía muchos vacíos sobre cómo se difunden el conocimiento y las capacidades en materia de propaganda computacional a nivel global, ésta también es un área importante para estudios futuros e investigación periodística.

Capacidad de las tropas cibernéticas

Al comparar los comportamientos, gastos, herramientas y recursos que emplean las tropas cibernéticas, podemos empezar a elaborar un panorama comparativo más completo de la organización global de la manipulación de redes sociales. Siempre es importante considerar el contexto local. Sin embargo, consideramos que también es importante generalizar sobre la experiencia de campañas organizadas de desinformación en todos los tipos de regímenes, con la finalidad de comprender mejor este fenómeno. Hemos empezado a desarrollar una medición simplista para evaluar comparativamente la capacidad de los equipos de las tropas cibernéticas en una relación recíproca, tomando en cuenta el número de actores de gobierno involucrados, la sofisticación de las herramientas, el número de campañas, el tamaño y permanencia de los equipos y los presupuestos y gastos ejecutados. Describimos la capacidad de las tropas cibernéticas en una escala del uno al cuatro:

(1) Las **tropas cibernéticas de capacidad mínima** son equipos recientemente creados o que estuvieron activos anteriormente, pero cuyas actividades actuales son inciertas. Los equipos recientemente creados tienen recursos mínimos y solo aplican unas cuantas herramientas de propaganda computacional en un número pequeño de plataformas. La capacidad de actividad mínima de las tropas cibernéticas también incluye a estados donde hemos encontrado que solo uno o dos políticos experimentan con herramientas de propaganda computacional. Estos equipos operan a nivel local, sin operaciones fuera del país. Entre los equipos de capacidad mínima figuran Angola, Argentina, Armenia, Australia, Croacia, Ecuador, Grecia, Holanda, Corea del Sur, Suecia, Taiwán y Túnez.

(2) Entre las **tropas cibernéticas de capacidad baja** se encuentran equipos pequeños que pueden estar activos durante las elecciones o un referéndum, pero que suspenden sus actividades hasta el siguiente ciclo electoral. Los equipos de capacidad baja tienden a experimentar solo con algunas estrategias, tales como el uso de bots para reforzar la desinformación. Estos equipos operan a nivel local, sin operaciones fuera del país. Entre estos figuran Austria, Colombia, República Checa, Eritrea, Alemania, Honduras, Hungría, Indonesia, Italia, Kenia, Macedonia, Moldavia, Nigeria, Corea del Norte, Polonia, Ruanda, Serbia, Sudáfrica, España, Zimbabue.

(3) Entre las **tropas cibernéticas de capacidad media** se encuentran los equipos que tienen formas y estrategias mucho más consistentes, incluyendo personal a tiempo completo empleado todo el año para controlar el espacio de la información. Estos equipos coordinan a menudo con diversos tipos de actores y experimentan con un amplio rango de herramientas y estrategias para la manipulación de redes sociales. Algunos equipos de capacidad media realizan operaciones de injerencia en el extranjero. Entre estos equipos figuran Azerbaiyán, Baréin, Bosnia y Herzegovina, Brasil, Camboya, Cuba, Etiopía, Georgia, Guatemala, India, Kazajistán, Kirguistán, Malasia, Malta, México, Pakistán, Filipinas, Qatar, Sri Lanka, Sudán, Tayikistán, Tailandia, Turquía, Ucrania, Reino Unido y Uzbekistán.

(4) Las **tropas cibernéticas de gran capacidad** son aquellas que involucran un gran número de personal, una importante asignación de recursos en operaciones psicológicas o guerra de la información. También es posible que existan fondos significativos destinados al campo de la investigación y el desarrollo, así como evidencia de uso de una multitud de técnicas. Estos equipos no solo operan durante las elecciones, sino que emplean personal a tiempo completo dedicado a manipular el espacio de la información. Los equipos de tropas cibernéticas de gran capacidad se centran en operaciones locales e internacionales. Entre estos equipo figuran China, Egipto, Irán, Israel, Myanmar, Rusia, Arabia Saudí, Siria, Emiratos Árabes, Venezuela, Vietnam y Estados Unidos.

TABLA 5. CAPACIDAD DE LAS TROPAS CIBERNÉTICAS

GRAN CAPACIDAD

País	Estado	Información sobre el tamaño del equipo, capacitación y gasto
China	Permanente	Equipo estimado entre 300,000 y 2'000,000 de personas trabajando en oficinas locales y regionales
Egipto	Permanente	–
Irán	Permanente	US$ 6,000 de gastos en publicidad en FB
Israel	Permanente	Equipo estimado en 400 personas. Evidencia de capacitación formal. Contratos múltiples valorizados en US$ 778K y 100M
Myanmar	Permanente	Evidencia de capacitación formal en Rusia
Rusia	Permanente	–
Arabia Saudí	Permanente	Costos estimados en 150 libras para tendencias de hashtags en Twitter
Siria	Permanente	Contratos múltiples valorizados en US$ 4,000
Emiratos Árabes	Permanente	Gastos múltiples valorizados en más de US$ 10M
EstadosUnidos	Permanente y temporal	–
Venezuela	Permanente	Equipo estimado en múltiples brigadas de 500 personas. Evidencia de capacitación formal
Vietnam	Permanente y temporal	Equipo estimado en 10,000 personas

TABLA 5. CAPACIDAD DE LAS TROPAS CIBERNÉTICAS

CAPACIDAD MEDIA

País	Estado	Información sobre el tamaño del equipo, capacitación y gasto
Azerbaiyán	Permanente	–
Baréin	Permanente	Contratos múltiples con un estimado valorizado en US$ 32M
Bosnia y Herzegovina	Temporal	–
Brasil	Temporal	Contratos múltiples valorizados en 10M reales, 130K reales, 24K reales, 12M reales
Camboya	Permanente y Temporal	–
Cuba	Permanente	–
Etiopía	Permanente	Evidencia de capacitación en China. Salarios estimados en US$300/mes
Georgia	Temporal	–
Guatemala	Permanente	Contratos múltiples valorados en US$ 100,000
India	Temporal	Equipos múltiples entre 50 y 300 personas. Múltiples contratos y gastos en publicidad valorados por encima de US$ 1.4M
Kazajistán	Temporal	–
Kirguistán	Permanente y Temporal	Equipo estimado en 50 personas. Múltiples contratos valorados en US$ 2,000. Salarios estimados entre US$3-4 al día
Malasia	Permanente	Equipo estimado entre 50-2000 personas. Evidencia de entrenamiento formal encontrado
Malta	Permanente	–
México	Temporal	–
Pakistán	Permanente	–
Filipinas	Permanente	300-500
Qatar	Temporal	–
Sri Lanka	Permanente y Temporal	Evidencia de capacitación formal en India
Sudán	Permanente	–
Tayikistán	Permanente	Equipo estimado en 400 personas
Tailandia	Permanente	Evidencia de capacitación formal
Turquía	Permanente	Equipo estimado en 500 personas
Ucrania	Permanente	Equipo estimado en 20,000 personas
Reino Unido	Temporal	Gasto de 3.5M libras en *Cambridge Analytica* por parte de *Leave Campaigns*
Uzbekistán	Permanente	–

TABLA 5. CAPACIDAD DE LAS TROPAS CIBERNÉTICAS

CAPACIDAD BAJA

País	Estado	Información sobre el tamaño del equipo, capacitación y gasto
Austria	Temporal	–
Colombia	Temporal	–
República Checa	Temporal	–
Eritrea	Permanente	–
Alemania	Temporal	–
Honduras	Temporal	–
Hungría	Temporal	–
Indonesia	Temporal	Múltiples contratos valorizados entre 1M-5M rupias
Italia	Temporal	–
Kenia	Temporal	Un contrato con Cambridge Analytica valorizado en US$6M
Macedonia	Temporal	–
Moldavia	Temporal	US$20,000 gastados en publicidad en FB e Instragram
Nigeria	Temporal	Un contrato con Cambridge Analytica valorizado en US$2.8M
Corea del Norte	Permanente	Equipo estimado en 200 personas
Polonia	Temporal	–
Ruanda	Temporal	–
Serbia	Permanente	Salario estimado en 370 euros/mes
Sudáfrica	Temporal	Múltiples contratos valorizados en US$ 2M
España	Temporal	–
Zimbabue	Temporal	–

CAPACIDAD MÍNIMA

País	Estado	Información sobre el tamaño del equipo, capacitación y gasto
Angola	Temporal	–
Argentina	Temporal	Equipo estimado entre 30-40 personas. Múltiples contratos valorizados en 14M de pesos, 11M de pesos en 2015, 200M de pesos en 2017
Armenia	Temporal	–
Australia	Temporal	–
Croacia	Temporal	–
Ecuador	Ya no está activo	Múltiples contratos valorizados en US$200,000
Grecia	Temporal	–
Holanda	Temporal	–
Corea del Sur	Ya no está activo	Cuando el equipo estaba activo eran menos de 20 personas
Suecia	Temporal	–
Taiwán	Ya no está activo	–
Túnez	Temporal	–

Fuente: Evaluaciones de los autores en base a la información recopilada. **Nota:** Esta tabla muestra la capacidad de los actores de las tropas cibernéticas.

CONCLUSIÓN

Las redes sociales, que alguna vez fueron reconocidas como una fuerza en favor de la libertad y la democracia, son objeto de un creciente escrutinio por su papel en el refuerzo de la desinformación, incitación a la violencia y disminución de los niveles de confianza en las redes e instituciones democráticas.

Este informe destaca las formas en las que los órganos de gobierno y partidos políticos utilizan las redes sociales para difundir propaganda política, contaminar el ecosistema de la información digital y reprimir la libertad de expresión y libertad de prensa. Mientras que las capacidades de acción de las redes sociales pueden servir para aumentar los alcances y precisión de la desinformación (Bradshaw y Howard 2018b), es importante reconocer que muchos de los temas centrales de la propaganda computacional –polarización, desconfianza o deterioro de la democracia– han existido mucho antes de la aparición de las redes sociales e incluso de Internet. La apropiación de las tecnologías de las redes sociales debe generar preocupación entre las democracias de todo el mundo, pero igual preocupación deberían causar muchos de los retos de larga data que afrontan los países democráticos.

La propaganda computacional ha pasado a formar parte de la esfera pública digital. Estas técnicas también seguirán evolucionando a medida que nuevas tecnologías –incluyendo la inteligencia artificial, la realidad virtual o el Internet de las cosas– aparezcan para remodelar profundamente la sociedad y la política. Pero dado que la propaganda computacional es un síntoma de los retos de larga data que afronta la democracia, es importante que las soluciones tomen en consideración estos retos sistémicos.

Sin embargo, también es necesario tener en cuenta el rol social que han jugado las plataformas de redes sociales en dar forma al ámbito actual de la información. Una democracia fuerte requiere acceso a información de calidad y la capacidad de la ciudadanía para entablar debates, discusiones, deliberaciones, tener empatía hacia el otro y hacer concesiones. ¿Las plataformas de las redes sociales están realmente creando espacios para la deliberación pública y la democracia? O, por el contrario, ¿están reforzando contenidos que mantienen a los ciudadanos adictos, desinformados y enojados?

REFERENCIAS

Blood, David. 2017. Is Social Media Empowering Dutch Populism? The Financial Times. https://www.ft.com/content/b1830ac2-07f4-11e7-97d1-5e720a26771b.

Bradshaw, Samantha y Philip N. Howard. 2017a. The Global Organization of Social Media Disinformation Campaigns. Journal of International Affairs 71(1.5).

Bradshaw, Samantha y Philip N. Howard. 2017b. Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation. Oxford: Oxford Internet Institute. Documento de trabajo.

2018a. Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. COMRPOP Serie de documentos de trabajo 2018(1): 26.

Bradshaw, Samantha y Philip N. Howard. 2018b. Why Does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life. Knight Foundation Working Paper. https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf.

Cadwalladr, Carole. 2017. The Great British Brexit Robbery: How Our Democracy Was Hijacked. The Guardian. http://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijackeddemocracy.

Carroll, Rory. 2012. Fake Twitter Accounts May Be Driving up Mitt Romney's Follower Number. The Guardian. https://www.theguardian.com/world/2012/aug/09/fake-twitter-accounts-mitt-romney.

Currier, Cora y Danielle Mackey. 2018. The Rise of the Net Center: How an Army of Trolls Protects Guatemala's Corrupt Elite. The Intercept. https://theintercept.com/2018/04/07/guatemala-anticorruption-trolls-smear-campaign/ (Agosto 5, 2019).

Dwoskin, Elizabeth y Annie Gowen. 2018. On WhatsApp, Fake News Is Fast — and Can Be Fatal. Washington Post. https://www.washingtonpost.com/business/economy/on-whatsapp-fake-newsis-fast--and-can-be-fatal/2018/07/23/a2dd7112-8ebf-11e8-bcd5 9d911c784c38_story.html (Setiembre 3, 2019).

Edwards, Frank, Philip N. Howard, and Mary Joyce. 2013. Digital Activism & Non-Violent Conflict. http://digital-activism.org/2013/11/report-on-digital-activism-and-non-violent-conflict/ (Mayo 17, 2017).

Gleicher, Nathaniel. 2019. Removing Coordinated Inauthentic Behavior and Spam From India and Pakistan. https://newsroom.fb.com/news/2019/04/cib-and-spam-from-india-pakistan/.

Greenwald, Glenn. 2014. The 'Cuban Twitter' Scam Is a Drop in the Internet Propaganda Bucket. The Intercept. https://theintercept.com/2014/04/04/cuban-twitter-scam-social-media-tool-disseminatinggovernment-propaganda/ (April 10, 2017).

2015. Controversial GCHQ Unit Engaged in Domestic Law Enforcement, Online Propaganda, Psychology Research. The Intercept. https://theintercept.com/2015/06/22/controversial-gchq-unit-domesticlaw-enforcement-propaganda/ (Abril 10, 2017).

Herring, Susan C. 2009. Web Content Analysis: Expanding the Paradigm. In International Handbook of Internet Research, eds. Jeremy Hunsinger, Lisbeth Klastrup y Matthew Allen. Springer Netherlands, 233–49. http://link.springer.com/chapter/10.1007/978-1-4020-9789-8_14 (Mayo 17, 2017).

Hitchen, Jamie, Jonathan Fisher, Nic Cheeseman e Idayat Hassan. 2019. How WhatsApp Influenced Nigeria's Recent Election — and What It Taught Us about 'Fake News. Washington Post. https://www.washingtonpost.com/news/monkey-cage/wp/2019/02/15/its-nigeriasfirst-whatsapp-election-heres-what-were-learning-about-how-fake-newsspreads/ (Setiembre 3, 2019).

Joyce, Mary, Rosas Antonio, and Philip N. Howard. 2013. Global Digital Activism Data Set. http://www.icpsr.umich.edu/icpsrweb/ICPSR/studies/34625/version/2.

Kazeem, Yomi. 2018. Cambridge Analytica Tried to Sway Nigeria's Last Elections with Buhari's Hacked Emails. Quartz. https://qz.com/1234916/cambridge-analytica-tried-to-sway-nigerias-last-elections-with-buharishacked-emails/.

Lee Myers, Steven y Paul Mozur. 2019. China Is Waging a Disinformation War Against Hong Kong Protesters. New York Times. https://www.nytimes.com/2019/08/13/world/asia/hong-kong-protestschina.html (Setiembre 3, 2019).

Mahtani, Shibani y Regine Cabato. 2019. Why Crafty Internet Trolls in the Philippines May Be Coming to a Website near You. Washington Post. https://www.washingtonpost.com/world/asia_pacific/why-craftyinternet-trolls-in-the-philippines-may-be-coming-to-a-website-nearyou/2019/07/25/c5d42ee2-5c53-11e9-98d4-844088d135f2_story.html (Setiembre 4, 2019).

Mozur, Paul. 2018. A Genocide Incited on Facebook, With Posts From Myanmar's Military. The New York Times. https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html (Julio 24, 2019).

Nunu. 2018. Leaked Documents Show That Ethiopia's Ruling Elites Are Hiring Social Media Trolls (And Watching Porn) · Global Voices. Global Voices. https://globalvoices.org/2018/01/20/leaked-documents-showthat-ethiopias-ruling-elites-are-hiring-social-media-trolls-and-watching porn/ (Julio 24, 2019).

Rio, I. T. S. 2018. Computational Power: Automated Use of WhatsApp in the Elections. ITS FEED. https://feed.itsrio.org/computational-powerautomated-use-of-whatsapp-in-the-elections-59f62b857033 (Marzo 2, 2019).

Rolfe, John. 2013. Fake Twitter Followers for Tony Abbott Being Investigated by Liberal Party. Perth Now. https://www.perthnow.com.au/politics/federal-politics/fake-twitter-followers-for-tony-abbott-beinginvestigated-by-liberal-party-ng-90b331e9e3ca2542ec9cbdf6d994f986.

Strange, Austin et al. 2013. China's Development Finance to Africa: A Media-Based Approach to Data Collection. Working Paper. https://www.cgdev.org/publication/chinas-development-finance-africa-mediabased-approach-data-collection (Mayo 17, 2017).

York, Jillian C. 2011. Syria's Twitter Spambots. The Guardian. https://www.theguardian.com/commentisfree/2011/apr/21/syria-twitterspambots-pro-revolution (Abril 10, 2017).

AGRADECIMIENTOS

Los autores agradecen el apoyo del European Research Council para el proyecto de investigación, “Propaganda Computacional: Investigando el Impacto de Algoritmos y Bots en el Discurso Político en Europa,” Proyecto 648311, 2015–2020, Philip N. Howard, Investigador Principal. La Fundación Hewlette Foundation, Luminate y la Fundación Adessium brindaron apoyo adicional para este estudio. Cualquier opinión, hallazgo y conclusión, o las recomendaciones expresadas en este material, son las de los autores y no reflejan necesariamente la opinión de los patrocinadores, el Oxford Internet Institute o la Universidad de Oxford.

Por su asesoramiento y apoyo en la investigación, agradecemos a Ualan Campbell-Smith, Amelie Henle, Caio Machado y Cailean Osborne, que recopilaron información preliminar y elaboraron perfiles de país en relación con la manipulación de las redes sociales señaladas en este informe. También estamos profundamente agradecidos con Akin Unver, Alberto Lalama, Alexi Abrahams, Angelina Huyun, Arzu Geybulla, Ben Nimmo, Bence Kollanyi, Chris Roper, Darko Brkan, Didac Fabregas-Badosa, Gabby Lim, Ingrid Grodnig, Iva Nenedic, Lisa-Maria Neudert, Marc Owen Jones, Martin Becerra, Mimie Liotsiou, Monika Kaminska, Nahema Marchal, Nick Monaco, Niki Cheong, Olivier Milland, Philip Di Salvo, Ralph Schroeder, Rosemary Ajayi, Sabine Niederer, Sanjana Hattotuwa, Vidya Narayanan, Tamar Kintsurashvili y Tom Sear, así como con los expertos anónimos consultados para este proyecto. Sus conocimientos especializados de países y redes sociales fueron fundamentales para garantizar la fiabilidad y validez de nuestra información. A todos ellos, nuestro agradecimiento por el tiempo y apoyo brindados para la revisión de los perfiles de país y por ofrecernos fuentes, referencias y datos adicionales para ser incluidos en este informe.

BIOGRAFÍA

Samantha Bradshaw es una experta destacada en el ámbito de la tecnología y la democracia. Su investigación doctoral analiza los generadores e impulsores de la desinformación y cómo la tecnología –inteligencia artificial, automatización y análisis de big data– favorecen y constriñen la diseminación de la desinformación en línea. A la vanguardia de aproximaciones teóricas y metodológicas para estudiar, analizar y explicar la compleja relación entre las redes sociales y la democracia, la investigación de Samantha ha ayudado a promover el debate académico, el conocimiento del público y la discusión de políticas en torno al impacto de la tecnología en el plano político y la privacidad. Samantha está terminando su doctorado en el Oxford Internet Institute, en la Universidad de Oxford, y es investigadora en el Proyecto de Propaganda Computacional.
Samantha tuitea desde @sbradshaww.

Philip N. Howard es catedrático y escritor. Enseña en la Universidad de Oxford, dirige el Oxford Internet Institute y es profesor en Balliol College. Escribe sobre políticas de la información y asuntos internacionales, y es autor de ocho libros, incluyendo The Managed Citizen, Pax Technica: How the Internet of Things May Set Us Free or Lock Us Up y, más recientemente, Computational Propaganda. Ha ganado varios premios al 'mejor libro’, y sus artículos sobre investigación han sido publicados en el New York Times, Washington Post y muchos medios de comunicación internacionales. La revista Foreign Policy lo nombró 'Pensador Global’ en 2018 y el Instituto Nacional Demócrata le entregó el 'Premio a la Democracia’ por su trabajo pionero en el campo de la ciencia social de las noticias falsas. Su próximo libro, Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations and Political Operatives será publicado por Yale University Press a comienzos de 2020. Publica en www.philhoward.org y tuitea desde @pnhoward

The Computational Propaganda Project
at the Oxford Internet Institute
University of Oxford
1 St Giles • Oxford OX1 3JS

Website: www.oii.ox.ac.uk