CÓMO LAS DEMOCRACIAS PUEDEN SUPERAR LOS DESAFÍOS HÍBRIDOS Y LA DESINFORMACIÓN

La desinformación se ha convertido en una amenaza cotidiana para el mundo interconectado en el que vivimos, aunque sus efectos pueden ser infravalorados debido a la falta de instrumentos con los que medir su impacto. Uno de los problemas centrales de este desafío es, precisamente, que mientras nuestro mundo ha ido cambiando, muchas de las instituciones en cuya protección confiamos han permanecido inalteradas. Este artículo plantea cómo la noción de «democracia» puede sobrevivir en este nuevo mundo digital y formula recomendaciones sobre cómo las instituciones pueden adaptarse y crecer. Además, presenta nuevas ideas en torno a la medición de la desinformación, tanto respecto a su difusión como a su impacto.

John Kelly
Investigador invitado, The German Marshall Fund

CIDOB REPORT
08- 2022

La nueva guerra está en todas partes

En los últimos años, han aparecido nuevos términos para describir la sensación de conflicto permanente que se percibe en todo el mundo: guerra híbrida, guerra cibernética, zona gris, información errónea, desinformación, mala información, operaciones de influencia y agentes malintencionados; son sólo algunas de las expresiones que han ido ganando aceptación en el léxico sobre conflictos y que intentan definir esta nebulosa de distintas tipologías de confrontación entre estados que ha comenzado a ser norma en tiempos de paz. Son conceptos que, en su mayoría, se incluyen en la idea de *guerra híbrida*.

La paz, tal como la conocemos, se define como la ausencia de guerra. Al mismo tiempo, la guerra, en nuestra idea tradicional, es un conflicto cuya naturaleza es cinética, lo que supone ataques armados, envíos de tropas y confrontación bélica. En cambio, la guerra híbrida ha transformado

nuestra noción de la época de paz. Según la OTAN, los conflictos híbridos desdibujan la línea que separa la guerra de la paz, mientras aumenta la opacidad o la ambigüedad sobre el origen de posibles ataques híbridos mediante la fusión de instrumentos convencionales y no convencionales, difuminándose el umbral de la guerra (véase Bargués y Bourekba en este volumen).

Aunque no esté especificado en esos términos, el concepto de guerra híbrida es tan antiguo como las desgastadas páginas de Sunzi que, hace más de dos mil años, ya advirtió que las destrezas bélicas podían incluir la idea de someter «al enemigo sin darle batalla» (véase Arco Escriche en este volumen). Sin embargo, más allá de que este pasaje se interprete, mayoritariamente, como una defensa de que la política y otros medios deberían evitar la guerra, es evidente que la estrategia de declarar o alimentar un conflicto al margen de las batallas cinéticas ha persistido a lo largo del tiempo.

Timothy Snyder (2018), en su libro *El camino hacia la no libertad*, observó que el riesgo de definir una guerra como híbrida es que, en este caso, el conflicto, por su naturaleza no convencional y no cinética, puede percibirse como una «guerra menor» o algo menos que una guerra normal. En cambio, este autor sostiene que ese tipo de conflicto armado debería considerarse como una «guerra aumentada», puesto que crea un ambiente de confrontación permanente, incluso sin la presencia del elemento cinético.

Todas estas nociones de guerra híbrida muestran, en conjunto, sólidos elementos para empezar a precisar un concepto intencionadamente vago. Definida en términos sencillos, la guerra híbrida se podría considerar como la agresión de una entidad (sea un Estado o una facción) hacia otra a través del uso de herramientas de poder no cinéticas con el objetivo de crear un resultado estratégico. Sin embargo, todavía es necesario elaborar más este concepto para aprehender la totalidad de su alcance actual. En concreto, hay que profundizar en los factores que determinan cuándo un Estado se considera a sí mismo *en* una guerra híbrida, qué forma debería adoptar su respuesta, y si existen parámetros que propicien que el arte de gobernar de forma convencional o el ejercicio de poder entre estados se conviertan en una guerra híbrida.

La desinformación como amenaza

La guerra híbrida es como un pulpo en el que cada tentáculo representa una táctica de guerra nueva, no convencional. De todos ellos, el tentáculo más fuerte sería el uso de la información como arma de desestabilización: a medida que la guerra híbrida se ha ido haciendo más común,

ha aumentado notablemente la propagación de lo que se clasifica como información errónea, desinformación y mala información (MDM, por su sigla en inglés). Según la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de Estados Unidos (CISA), aunque las diferencias entre estos términos sean sutiles, es fundamental entenderlas. Así, la *desinformación* sería la información creada deliberadamente para perjudicar o manipular a una persona, grupo social, organización o país; la *información errónea*, la información falsa elaborada sin la intención de hacer daño y, finalmente, la *mala información* el uso de información veraz fuera de contexto con la finalidad de engañar. La protagonista de estas tácticas híbridas es, sin duda, la desinformación.

La desinformación es una amenaza en auge surgida al amparo de unas plataformas digitales y redes sociales que han crecido prácticamente sin ningún tipo de control, dominando los flujos de información. No obstante, a medida que ha ido creciendo la desinformación, también lo han hecho las tácticas para cuantificarla y luchar contra ella, por lo que ya se pueden tomar medidas para mitigar los efectos de sus contenidos.

LA DESINFORMACIÓN ES UNA AMENAZA EN AUGE SURGIDA AL AMPARO DE UNAS PLATAFORMAS DIGITALES Y REDES SOCIALES QUE HAN CRECIDO PRÁCTICAMENTE SIN NINGÚN TIPO DE CONTROL, DOMINANDO LOS FLUJOS DE INFORMACIÓN. NO OBSTANTE, A MEDIDA QUE HA IDO CRECIENDO LA DESINFORMACIÓN, TAMBIÉN LO HAN HECHO LAS TÁCTICAS PARA CUANTIFICARLA Y LUCHAR CONTRA ELLA, POR LO QUE YA SE PUEDEN TOMAR MEDIDAS PARA MITIGAR LOS EFECTOS DE SUS CONTENIDOS.

Tradicionalmente, se ha identificado y considerado la desinformación poniendo el foco en la producción de contenido falso, en la cantidad de contenido creado «publicado, compartido o visualizado», o en indicadores tales como el número de *bots* que se pueden identificar en Twitter. Si bien estas medidas son eficaces para calcular el número de fuentes de desinformación, no miden el impacto del contenido –veraz, o no– diseminado. Aunque es importante considerar ambos indicadores, es crucial comprender la eficacia de estas campañas desinformativas.

En este ámbito de la producción de contenidos, la Unión Europea (UE) aprobó en abril de 2022 un nuevo paquete legislativo digital para reforzar la respuesta de la Unión a la desinformación: la Ley de Mercados Digitales (DMA, por sus siglas en inglés) y la Ley de Servicios Digitales (DSA, por sus

siglas en inglés), que incluyen un actualizado Código de Buenas Prácticas en materia de Desinformación cuyo objetivo es detener la propagación de la desinformación en las plataformas tecnológicas haciendo responsable al propietario de la plataforma (Meta, Twitter, etc.) de la difusión de contenido falso. Dicho Código aborda esta cuestión aumentando las obligaciones en materia de presentación de informes por parte de estos gigantes digitales sobre las acciones emprendidas para luchar contra la desinformación, exhortándoles a promover la verificación de datos y a aumentar la transparencia en la publicidad política, entre otras medidas. Las sanciones por no cumplir con estas normas caen dentro del ámbito de la DSA que, por primera vez, impone multas de hasta el 6% de los ingresos anuales a nivel global de estas empresas en caso de inacción.

Más allá de este esfuerzo por crear un marco normativo que ponga ciertos límites al fenómeno, avanzan también nuevas medidas analíticas para aumentar el conocimiento sobre cómo se propaga la desinformación, así como sus efectos sociales y políticos. Una propuesta eficaz para medir el impacto de las campañas desinformativas consiste en analizar si, a la larga, la desinformación conduce a la acción, o si el contenido se reproduce también más allá de la plataforma donde se origina. El analista Ben Nimmo (2020), en un estudio para la Brookings, propuso la creación de una «escala de disrupción» que midiese el impacto de una campaña de desinformación. Esta escala va del uno al seis, calculando si el contenido se origina en una única plataforma, si se mueve a través de diversas fuentes (ya sean redes sociales o medios de comunicación tradicionales), si es amplificada por celebridades o personajes conocidos y, finalmente, si llama a la acción, a la violencia o provoca respuestas políticas. Esta escala, usada juntamente con los indicadores identificativos de la fuente original de la desinformación, puede ayudar a los investigadores a entender el qué, el dónde, el quién y el cómo de la desinformación y sus tácticas para arraigarse y proliferarse. Sin embargo, todas estas mediciones son inútiles si, paralelamente, no se consigue restablecer la confianza en la democracia. La desinformación contribuye a la polarización y a la erosión institucional y de los procesos democráticos. Hay formas de luchar contra eso.

¿Cómo sobrevive la democracia a las amenazas híbridas?

La guerra híbrida y la desinformación debilitan los pilares sobre los cuales descansan nuestras democracias, violando los principios y los derechos sobre los cuales fueron fundadas. Sin duda, aunque ese es el objetivo de estas tácticas, estas amenazas se han vuelto tan complejas que dan lugar a una pregunta: ¿habrá que replantearse el concepto de democracia? La respues-

ta simple es no; sin embargo, será necesario que la democracia, sus instituciones y normativa sigan progresando para mantenerse relevantes en la era digital. De la misma forma que se interpretan los textos religiosos para los tiempos modernos, hay que interpretar y desarrollar las democracias para que sigan siendo entidades poderosas capaces de proteger a sus ciudadanos. En este sentido, referente a la regulación de la industria tecnológica, se pueden dar fácilmente pasos en varias direcciones para generar cambios desde este mismo momento.

Hasta 2014, el famoso mantra de Mark Zuckerberg para Facebook era el bien conocido «muévete rápido y rompe cosas». Esta frase, que significaba dar vía libre a los desarrolladores y directores de Facebook para probar, crear y fracasar, se convirtió en la lógica del Silicon Valley. Muchas empresas tecnológicas –como Uber y WeWork– fueron pioneras en el llamado capitalismo de plataforma con resultados dispares. Sin embargo, lo que faltó en el esfuerzo para «avanzar rápidamente y romper cosas» fue, a menudo, la vigilancia o la capacidad de anticiparse a los posibles usos indebidos de estas tecnologías. Así, si bien el mantra de Zuckerberg quizá haya tenido éxito en la industria tecnológica, su respuesta no ha podido ser más radicalmente opuesta en los lentos, metódicos y deliberativos ideales de la democracia. Desde el principio, las democracias se concibieron incorporando mecanismos de control, cuya finalidad era la moderación de sus acciones para adoptar decisiones bien fundadas al servicio de la ciudadanía. No pretendía ser un proceso rápido o disruptivo, por lo que, ante el desafío arrollador de una industria que puede crear tecnologías completamente nuevas en cuestión de días, la democracia se encuentra en una confrontación muy desigual.

Las democracias son tan relevantes hoy como cuando nació la primera democracia en Atenas hace más de 2.500 años. Sin embargo, muchas de ellas han seguido funcionando bajo las rigurosas pretensiones de sus documentos constitutivos, sin haberse actualizado para adaptarse a un mundo en constante cambio. En Estados Unidos, por ejemplo, la Constitución con la que se fundó el país fue concebida como una «Constitución viva», para poder irse actualizando a medida que el mundo evolucionaba. En la práctica, sin embargo, esto ha demostrado ser falso, tanto en Estados Unidos como en otros países. Tal como ya escribió Walter Lippmann en 1919, las democracias son influenciadas por la información de la que disponen, y estas deben esforzarse por «controlar su entorno» cuando trabajan en nuevos espacios informativos. Es facultad de las democracias progresar para controlar este nuevo entorno. Sin embargo, las democracias tienden a ser reactivas en lugar de proactivas, por lo que han tardado casi tres décadas en crear un marco que regule este nuevo mundo tecnológico.

En general, las democracias solo intervienen cuando una nueva esfera de influencia se vuelve peligrosa. Ello ocurrió en Estados Unidos, cuando la industria automovilística empezó a crecer sin limitaciones y se acabó creando la Administración Nacional de Seguridad del Tráfico en las Carreteras en 1970; o cuando la contaminación empezó a extenderse sin restricciones por todo el país y se estableció la Agencia de Protección Ambiental, también en 1970. En la actualidad, ante la capacidad disruptiva de la desinformación, amplificada por la industria tecnológica, ha llegado el momento de tomar medidas para eliminar riesgos. Mark Zuckerberg, el defensor original del moverse rápido y romper cosas (que posteriormente transformó en «muévete rápido con una infraestructura estable»), afirma que el Gobierno debe desempeñar un papel más activo en la regulación de Internet, y ha propuesto cuatro simples medidas que contribuirían a hacer de las redes sociales e Internet un lugar más seguro: a) la regulación de contenidos nocivos, b) la garantía de la integridad electoral, c) los controles de privacidad y c) la portabilidad de datos.

Por su parte, la UE está abriendo un camino en la creación de un entorno digital más seguro con las mencionadas DMA y DSA. La adopción, por parte de los principales aliados de la UE, de este marco legislativo garantizaría una regulación internacional coherente para prevenir «agujeros digitales» donde agentes maliciosos puedan operar. Asimismo, 61 países ya han firmado un documento titulado «Declaración sobre el futuro de internet», propuesto por la administración Biden, que establece una visión global de Internet en la que se protegen los derechos humanos, se modera la competencia, se asegura la infraestructura y se garantiza el acceso universal a la conectividad, entre otros temas (Engler, 2022). Este documento podría representar también un primer paso firme para alcanzar estos objetivos si los firmantes garantizasen el cumplimiento de las normas en cuestión y, sobre todo, si se consensuase este acuerdo como marco jurídico en lugar de su condición actual de documento no vinculante.

Como se ha mencionado, existen muchos caminos para hacer que las instituciones democráticas sobrevivan y se desarrollen en el entorno digital actual. En primer lugar, la existencia de unas definiciones más firmes de lo que es una guerra híbrida, junto con los parámetros que especifiquen qué significa *estar* en un conflicto híbrido, contribuirían a sortear los espacios grises que estas tácticas pretenden crear. En segundo lugar, el uso de datos para medir la eficacia de los actos dentro de un conflicto, como la difusión de la desinformación, nos puede ayudar a evaluar el riesgo y la reacción. Finalmente, la implementación de normas y reglamentos actualizados puede contribuir a proteger a la ciudadanía y brindar a las instituciones la libertad necesaria para trabajar dentro del nuevo contexto de amenazas. Las democracias fueron creadas para crecer y adaptarse: ha llegado el momento de que ello se lleve a cabo.

Referencias

Bilal, Arsalan. «Hybrid Warfare – New Threats, Complexity, And 'Trust' As the Antidote». *NATO Review* (30 de noviembre de 2021) (en línea) [Fecha de consulta: 6.7.2022] https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Sunzi. *El arte de la guerra,* Alianza editorial, 2022.

Snyder, Timothy. *El camino hacia la no libertad.* Barcelona: Galaxia Gutenberg, 2018.

Nimmo, Ben. «The Breakout Scale: Measuring the Impact Of Influence Operations». *Brookings Foreign Policy* (septiembre de 2020) (en línea) [Fecha de consulta: 6.7.2022] https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf

Lippmann, Walter. «The Basic Problem of Democracy». *The Atlantic* (noviembre de 1919) (en línea) [Fecha de consulta: 6.7.2022] https://www.theatlantic.com/magazine/archive/1919/11/the-basic-problem-of-democracy/569095/

Engler, Alex. «The Declaration for the Future of the Internet is for Wavering Democracies, not China and Russia». *Brookings* (6 de mayo de 2022) (en línea) [Fecha de consulta: 6.7.2022] https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/