Su uso sistemático y la facilidad para su diseminación la han convertido en uno de los principales vectores de la amenaza híbrida

DESINFORMACIÓN y Unión Europea

Teniente coronel Vicente Diaz de Villegas Roig
Gabinete del SEGENPOL

LA primera víctima en los conflictos es la verdad. El deber de toda sociedad civil es desarrollar su propia resiliencia y proteger la información como un bien común. Si uno no ocupa su lugar en el entorno de la información, otros lo harán. Durante la guerra fría, la potencial destrucción mutua que garantizaba un conflicto con armas nucleares actuó como elemento disuasorio en el entorno físico. Sin embargo, internet y la posterior eclosión de las redes sociales han facilitado que el entorno de la información se convierta en un campo de batalla. Las agencias gubernamentales, organizaciones privadas y otros grupos de presión luchan en una batalla por el relato las 24 horas del día, donde el gap tecnológico ya no supone un *game changer*.

La desinformación ha pasado a ocupar un lugar preferente en las crisis actuales. Si bien no es un fenómeno nuevo, su uso sistemático y la facilidad para su diseminación que ofrecen las nuevas tecnologías, la ha convertido en uno de los principales vectores de la amenaza híbrida. A este respecto, el Marco conjunto para contrarrestar las amenazas híbridas publicado por la Unión Europea en 2016 indica que «las campañas masivas de desinformación, que utilizan las redes sociales para controlar la narrativa política o para radicalizar, reclutar y representar directamente a los actores, pueden ser vehículos para amenazas híbridas».

OTRA VÍCTIMA: EL PENSAMIENTO CRÍTICO

En la batalla por el relato, la desinformación busca generar dudas sobre la veracidad de los hechos, para lo cual, se relativiza la verdad devaluando el discurso público con el objeto de generar desconfianza en las instituciones que gobiernan la sociedad. La principal herramienta para lograr ese efecto no es tanto la mentira frontal, como la utilización interesada de información sacada de contexto y de mensajes que apelan más a las emociones que a la razón. Un individuo que duda y desconfía, sometido permanentemente a una saturación de información (*infosaturation*), posee una opinión voluble, una situación ideal para transformar una opinión pasiva en una convicción activa.

Valorar la efectividad de la desinformación no es tarea sencilla, la pregunta que surge es si la desinformación puede lograr nuevas opiniones o simplemente refuerza las existentes. Para ello hay que considerar los factores de vulnerabilidad de la sociedad como son la existencia de divisiones externas e internas, la presencia de minorías, instituciones débiles y una cultura débil de los medios de comunicación. Además, los medios empleados juegan un rol fundamental. Las narrativas a medida, en algunos casos muy reducida (*microtargeting* e, incluso, *targeting* individualizado), las interferencias en procesos democráticos, las filtraciones interesadas, la falsificación de documentos…, son solo algunos ejemplos.

ECLOSIÓN DE LAS REDES SOCIALES

Los responsables de las campañas de desinformación han encontrado un lugar ideal para enmascarar su huella: el ciberespacio. En otras palabras, la red dificulta la atribución de las acciones, al menos, con la normativa tradicional.

La horizontalidad de las redes sociales permite a cualquier ciudadano convertirse en periodista sin pasar por ningún filtro editorial. La saturación de comunidades y la presencia de granjas de troles (personas que realizan comentarios provocadores buscando crear controversia o

Consejo Europeo

desviar la atención de una temática) han transformado las dinámicas de generación y difusión de la información. A estos últimos se han incorporado sistemas semiautomáticos y automáticos de difusión como los *bots* (programas informáticos que efectúan automáticamente tareas repetitivas a través de internet) y los *servidores zombis*.

¿CÓMO LO HACEN?

Para aumentar el tiempo de conexión a la red, las plataformas utilizan algoritmos de personalización que encierran a los internautas en una caja de resonancia (*filter bubbles)* de contenidos afines al historial de búsqueda de los usuarios, reduciendo el acceso a información que permita contrastar noticias. Las comunidades de troles realizan una labor similar, generan una gran cantidad de identidades falsas (*sockpuppets*) que trasladan una misma idea con mensajes similares. En muchos casos, esos mensajes vienen apoyados por contenidos falsos creados con las, cada vez más desarrolladas, herramientas informáticas de edición de sonido, fotografía y video.

El humor ha cobrado protagonismo en las campañas de manipulación de la información, para las que, los *memes* han resultado ser una herramienta muy eficaz; una imagen con un texto corto que apela a la emoción y es fácil de retrasmitir.

Lo correcto es correcto si todo el mundo lo hace. En 2006, Cialdini postuló los 6 principios de influencia que se encuentran detrás de cualquier intento de persuasión. Uno de ellos, el principio de la conformidad social, afirma que «descubrimos lo correcto enterándonos de la opinión de los demás sobre lo correcto». Este principio tiene plena validez en las redes sociales, ya que, una vez en nuestra caja de resonancia, la información será más atractiva cuanto mayor número de *likes* tenga. En la red se pueden comprar *likes* y una de las principales actividades de las comunidades de troles es la de introducir comentarios a las noticias para dar la impresión de que la mayoría de las personas están de acuerdo con las ideas que promueven.

Otro de los métodos utilizados para aumentar la polarización social aprovechando temas controvertidos como la inmigración o las tensiones raciales, es el de participar activamente tomando parte en ambos bandos. Se han detectado numerosos casos en los que, desde un mismo servidor, se han creado sitios y perfiles activos que generaban contenido emocional para cada una de las posturas enfrentadas, buscando una mayor división social.

Las campañas de desinformación encuentran en el ciberespacio un lugar ideal para enmascararse

En este sentido, el coronavirus no se ha librado de la controversia, una de las teorías más habituales que circula por la red es que el virus es un arma biológica estadounidense que ha sido propagada intencionalmente por orden de Trump para aislar a China. Otra atribuye su creación a un supuesto laboratorio británico que también envenenó al disidente ruso Skripal en Salisbury, y

Lecoustier/Comisión Europea

alguna aventura que fue robado de un laboratorio canadiense por espías chinos.

LEAKS: ¿DÓNDE NACE MI OPINIÓN?

Uno de los vectores más potentes de difusión son las filtraciones de información (*information leaks*). Es un método muy efectivo porque la audiencia a la que va dirigido tiene la percepción de tener acceso a la verdad por haber sido obtenida directamente de la fuente. Sin embargo, en la mayoría de los casos forman parte de una campaña de desinformación, ya que, la difusión se produce de manera interesada, se descontextualiza, se añaden datos (*tainted leaks*) que, a menudo, pasan desapercibidos pero que producen alteraciones intencionadas.

El pasado 9 de marzo, comenzó en la Haya el juicio contra cuatro sospechosos del derribo del vuelo MH17 de *Malaysian Airlines* mediante un misil antiaéreo. Un mes antes, varios medios de comunicación publicaron noticias que apuntaban a «nuevos documentos filtrados» que supuestamente demostraban que en el área del accidente no había ningún sistema de misiles *BUK* (identificado por los investigadores como causante de la catástrofe).

¿CÓMO SE PROTEGE LA UNIÓN EUROPEA?

Las interferencias en los procesos electorales pueden estar dirigidas a los votantes, mediante campañas para influenciar el sentido de voto, o a los sistemas electrónicos, con el fin de modificar bases de datos que alimentan el censo, el recuento de votos o, simplemente, robar datos. La simple sospecha de que haya una intención de manipular los resultados de una votación genera una sensación de desconfianza en el electorado que puede restar legitimidad al proceso.

La Unión Europea se ha visto movida a actuar dado el aumento de los casos de interferencia en procesos electorales, destacando el *brexit*, las elecciones presidenciales de Estados Unidos y las elecciones francesas.

La *Estrategia de Seguridad Global* de 2016, año del referéndum sobre el *brexit*, estableció una serie de prioridades entre las que destacan la seguridad de la Unión ante las amenazas actuales. Para hacer frente a las amenazas nos plantea una serie de mejoras de las capacidades de defensa, cibernéticas, de lucha contra el terrorismo, energía y de comunicación estratégica. Esta última, debe de ser capaz, entre otros, de ofrecer refutaciones rápidas y objetivas a la desinformación, fomentar un entorno mediático abierto y de investigación dentro y fuera de la Unión y desarrollar su capacidad de actuación a través de las redes sociales.

El Plan de Acción Contra la Desinformación de la Unión Europea define la desinformación cómo «la información verificablemente falsa o engañosa que se crea, presenta y difunde para obtener beneficios económicos o para engañar intencionalmente al público, y puede causar daño público. El daño público incluye amenazas a los procesos democráticos, así como a los bienes públicos, como la salud, el medio ambiente o la seguridad de los ciudadanos de la Unión. La desinformación no incluye errores involuntarios, sátira y parodia, ni noticias y comentarios partidistas claramente identificados».

El plan plantea cuatro pilares sobre los que se debe asentar la respuesta coordinada de la Unión:

• Mejorar las capacidades de las instituciones de la Unión para detectar, analizar y exponer la desinformación.
El aumento de capacidades que propone se consigue reforzando con personal especializado, servicios de monitorización y *software* de análisis de *big data* los Grupos de Trabajo de Comunicación Estratégica del Servicio Europeo de Acción Exterior, las Delegaciones y la Célula de Fusión Híbrida.

• Fortalecer las respuestas coordinadas y conjuntas a la desinformación.
El plan parte de la base de que la pronta reacción a través de una comunicación efectiva basada en hechos es esencial para contrarrestar y disuadir la desinformación, incluso en los casos de desinformación sobre asuntos y políticas de la Unión. Por este motivo, en marzo de

2019, desde Bruselas se creó un *Sistema de Alerta Rápida* para facilitar a los Estados Miembro y a las instituciones de la UE el intercambio de datos con el objeto de permitir una visión común con la que facilitar el desarrollo de respuestas consensuadas, garantizando la eficiencia en tiempo y recursos.

• Movilizar al sector privado para abordar la desinformación.
Google y *Facebook* representan aproximadamente el 70 por 100 del tráfico web, es decir, la audiencia de la gran mayoría de páginas de internet, incluidas las de noticas, proviene de esas plataformas. Bruselas tomó conciencia de este hecho y, alrededor de un año antes de las elecciones al Parlamento Europeo, publicó un Código de Buenas prácticas de la UE contra la desinformación.

Las principales plataformas *on line* (*Facebook*, *Google* y *Twitter*) se adhirieron al citado código comprometiéndose a desarrollar, antes de la fecha de las elecciones al Parlamento, capacidades de inteligencia interna que permitieran detectar, analizar y bloquear actividades maliciosas en sus servicios. La Comisión y el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual (ERGA), se encargaría de supervisar mensualmente el avance de los compromisos adquiridos.

• Sensibilización y mejora de la resiliencia social.
«Una mayor concienciación pública es esencial para mejorar la resiliencia social frente a la amenaza que representa la desinformación». El punto de partida es una mejor comprensión de las fuentes, intenciones, herramientas y objetivos detrás de la desinformación, pero también de nuestra propia vulnerabilidad.

¿QUIÉN CERTIFICA LA IMPARCIALIDAD DE LA *POLICÍA DIGITAL*?

El código de prácticas de la Unión Europea contra la desinformación se benefició de un gran impulso inicial cuando las grandes plataformas de redes sociales implementaron herramientas de autorregulación, fundamentalmente filtros y moderadores, contra las denominadas «actividades maliciosas». Sin embargo, ambas herramientas pueden ser objeto de manipulación por lo que su neutralidad es discutible y su poder de conformar la opinión innegable. Entonces, para poder contestar a la pregunta, hay que tener presente que bajo un aparente interés por identificar la manipulación de información se corre el riesgo de crear «ministerios de la verdad», que, en aras de reforzar una determinada corriente política, deterioran uno de los grandes logros de la democracia, la libertad.

OTRAS INICIATIVAS

En los últimos años han surgido numerosas iniciativas con el objeto de analizar y detectar la manipulación de información. En el seno de la Unión Europea, la *East StratCom Force*, bajo el programa *EUvsDisinfo*, analiza los casos provenientes del este de Europa. Sus principales productos son la *Disinformation review*, que semanalmente analiza los casos detectados, y la *Disinformation digest*, donde analiza los datos obtenidos para identificar los objetivos que hay detrás de las campañas de desinformación.

El Centro de Excelencia StratCom de la OTAN en Riga proporciona análisis, asesoramiento, apoya el desarrollo de doctrina y realiza investigaciones y experimentos para encontrar soluciones prácticas en la comunicación estratégica, incluyendo la desinformación.

Además existen otras organizaciones de carácter privado o semiprivado como el *Digital Forensic Research Lab* (DFRLab), el Bellingcat…, cuya actividad consiste en analizar fuentes abiertas y redes sociales con el objeto de identificar y exponer los casos de desinformación.

Por último, los medios tradicionales de comunicación social, también presentes en la red, pueden tener un papel significativo como guardianes de las buenas prácticas periodísticas. Son una pieza fundamental en la detección y denuncia de acciones de manipulación de la información provenientes del exterior y también tienen un rol en el pilar formativo de la sociedad. Ya son bastantes los medios que dedican esfuerzos a desenmascarar manipulaciones de información. Así, por ejemplo, están los casos de la agencia *France Presse* con su *Fact Check*, la BBC que produce el *Reality Check*, *Le Monde* que publica el *Decodex*,…

La sociedad puede beneficiarse de un ambiente colaborativo entre gobierno, instituciones, periodistas, asociaciones especializadas, basado en un entendimiento común de las dinámicas de desinformación. ■

Respuesta OTAN a la desinformación sobre el COVID-19

LA OTAN se ha visto afectada por campañas de desinformación sobre el COVID-19 enfocadas en resaltar la falta de solidaridad entre los aliados, la irrelevancia de las medidas adoptadas desde Bruselas y el perjuicio que el virus ha causado a la capacidad de respuesta.

En este sentido, durante la videoconferencia extraordinaria de los aliados de la OTAN del pasado 15 de abril, la ministra de Defensa, Margarita Robles, puso en valor todo el trabajo que está realizando la organización atlántica para combatir la desinformación, tanto en el ámbito de la información pública, como en el de la diplomacia. Esta actuación de la Alianza se basa en un proceso de análisis del entorno de la información que incluye los medios tradicionales, redes y audiencias y permite una respuesta oportuna, coherente y basada en datos.

Además, en una crisis que no conoce fronteras, la coordinación con otras organizaciones internacionales juega un papel muy importante, de ahí que la OTAN haya incrementado su relación con la UE en el esfuerzo común para contrarrestar la manipulación de información ligada a esta crisis sanitaria.