



Samuel Álvarez.
Ingeniero de Telecomunicación.

Las **cuatro paradojas** de la ciberseguridad

Uno de los problemas más importantes sin resolver del reto de la ciberseguridad no es el cibercriminal o las ciberamenazas, sino la propia sociedad y **su comportamiento en Internet**.

La hiperconectividad de las personas y las ‘cosas’ (IoT), el 5G, la Inteligencia Artificial (IA) y la falta de cultura y sensibilización en relación al correcto y cauto uso de los datos que se publican y se comparten con el mundo, hacen que el desafío de la ciberseguridad no sea un asunto baladí y que requiera, al menos, de un redundante esfuerzo y reflexión de cómo plantear, en primer lugar, el entendimiento del problema para luego trazar una hoja de ruta tortuosa, lo que se podría llamar ‘la mejor solución’.

El reto de la ciberseguridad intenta cristalizar abriéndose camino en medio de una tormenta de contradicciones y paradojas, de una multitud de elementos muy complicados de alinear, donde la ‘gobernanza’ del ciberespacio y los esfuerzos de las Administraciones por proteger a las personas son vacuos, débiles e ineficaces. Es como si estuviéramos tejiendo una gran red con agujeros grandes para pescar ballenas cuando lo que necesitamos pescar son salmonetes. Estas paradojas o contradicciones son:

Paradoja 1: ¿Es compatible preservar la neutralidad de la red y del ciberespacio y garantizar las libertades de los ciudadanos?

Paradoja 2: ¿Es factible regular la protección de datos a nivel global en relación con los ciudadanos mientras éstos airean y publican sin control hasta sus más íntimos secretos?

Paradoja 3: ¿Cuál es el equilibrio y el código ético que debe establecerse entre el uso y aplicación de la IA para hacernos la vida más útil y fácil sin que a la vez no tome control sobre nuestras vidas y el rumbo del mundo?

Paradoja 4: ¿Cómo de útil y efectivo resultan todas las medidas institucionales y corporativas en ciberseguridad cuando una persona ‘pincha’ en su ordenador del trabajo un USB que le han regalado?

Las paradojas anteriores lo impregnan todo. Nacen a raíz de la persona, del comportamiento de cada ciudadano, pero im-

Procesos para ciberinfluir en la sociedad

El conjunto de medios que existen para influir en la sociedad, ya sea con un fin moral o con un fin inhumano y delictivo, engloba tanto tecnologías sofisticadas como perfiles profesionales especializados en neurociencias, psicología y comunicación. El proceso es conceptualmente sencillo y se compone de tres pasos:

PASO 1

Realizar escucha masiva en Internet, lo que se denomina Social Listening, para lograr una hipersegmentación de la sociedad respecto al tema que se haya investigado.

Por ejemplo: ¿Cuántas familias jóvenes con hijos viven en el sur de Madrid, tienen un poder adquisitivo concreto, su tendencia política es X, son religiosos, tienen un solo vehículo, no tienen estudios universitarios, trabajan en un determinado sector, son de un rango de edad específico, son más de montaña que de playa y les gusta los videojuegos...?

Esta primera acción persigue identificar audiencias susceptibles de ser influidas para algo, identificando perfiles psicológicos en función del comportamiento ante las redes sociales y en las diferentes fuentes abiertas donde publican su vida.

PASO 2

Producir inteligencia sobre la información recogida, lo que se denomina Social Intelligence, con objeto de identificar las principales identidades sobre las cuales un mensaje específico tenga un impacto masivo en Internet, dentro del tipo de perfil psicológico y del comportamiento identificado en el párrafo anterior.

Esta fase es relevante y de alto impacto, pues la orientación, finalidad y uso determinarán si el objetivo es manipular o generar tendencia, dos términos muy diferentes, aunque estén separados por una delgada línea, no sólo legal sino moral.

PASO 3

Producir un mensaje y una información, diseñados milimétricamente para ser consumidos por los grupos sociales y psicológicos identificados en el proceso anterior, dirigidos como un proyectil inteligente sólo y exclusivamente a un puñado de personas, perfectamente estudiadas, cuya reacción provocaría un impacto masivo en decenas de miles de perfiles en Internet. Una intervención quirúrgica, de alto impacto, como una reacción en cadena producida sólo estimulando un átomo, una única molécula. Así se simple, así de sencillo, así de fácil.

La escucha masiva en Internet y la generación de mensajes pueden servir para crear tendencias, orientar votos o avivar revueltas sociales

pactan, al no resolverse de forma sencilla, en la continuidad de negocio de cualquier organización, ya sea una empresa, un gobierno, un sistema democrático, una infraestructura crítica... y, por supuesto, impactan de lleno en la economía.

Impactos de las paradojas

Entonces, ¿cómo resolvemos el problema? ¿cerramos Internet? ¿cerramos las redes sociales? ¿prohibimos a la sociedad que publique sus debilidades a troche y moche? ¿metemos en la cárcel a quien utilice una contraseña '1234' para acceder a sus servicios digitales? ¿cómo es posible que nos manipulen en Internet si se supone que tenemos un nivel socio cultural medio-alto, en teoría suficiente para darnos cuenta de que estamos siendo víctimas y corresponsables de un delito siendo ovejas de un gran rebaño que tiene un pastor al que no conocemos ni identificamos y donde simplemente caminamos hacia donde se nos dice?

Lamentablemente, el nivel de exposición de la sociedad en Internet es increíble, es desmesurado, es absurdo. Decimos dónde vivimos, dónde vamos de vacaciones, dónde estamos exactamente en el momento en el que publicamos algo, cuáles son nuestros hobbies, cómo de guapos son nuestros hijos, si tenemos mascotas, dónde tenemos la hipoteca, quiénes de nuestro contactos son vínculos familiares, cuál es nuestro nivel socio-económico, qué coche tenemos, de qué equipo deportivo somos, cuáles son nuestros gustos,

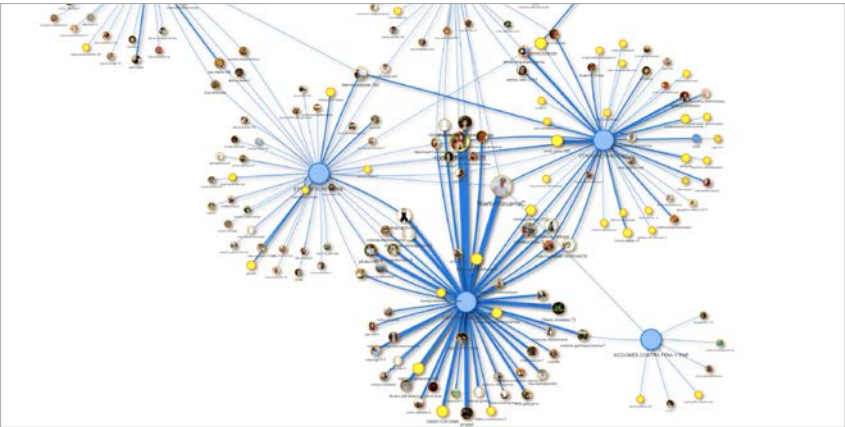
El nivel de exposición de la sociedad en Internet es increíble, es desmesurado, es absurdo

qué deportes practicamos y qué rutas hacemos, a quién votamos, si creemos en Dios, si apoyamos al gobierno o le desprestigiamos, si comemos gambas o somos vegetarianos... lo publicamos todo. Y todo esto lo hacemos de forma abierta, accesible para cualquiera. Ante semejante realidad... ¿cómo vamos a proteger a la sociedad?

¿Cómo se manipula a la sociedad desde el ciberespacio?

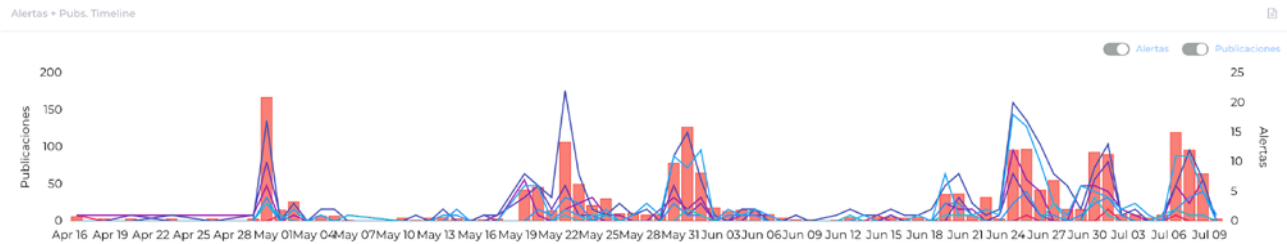
A estas alturas no considero que nadie pueda cuestionar que esto no esté ocurriendo. Basta remontarse al pasado reciente, en 2008, cuando Barack Obama ganó democráticamente su presidencia del Gobierno y se apoyó en la escucha masiva en Internet para dirigir de forma

GRÁFICO DE RELACIONES DE GRUPO DE PERSONAS POR AFINIDAD EN COMPORTAMIENTO SOCIAL



Este grafo representa el descubrimiento de la fortaleza entre las relaciones de identidades digitales en función de comportamientos sociales y gustos o preferencias de los usuarios. Las intersecciones manifiestan un mayor nivel de afinidad y el grosor de las uniones quién ostenta el liderazgo o es más efectivo en la comunicación para impactar en el total del colectivo.

EVOLUCIÓN DE TENDENCIA DE REACCIÓN DE GRUPO SOCIAL EN INTERNET



Línea de tiempo basada en alertas predeterminadas a comportamientos que se puedan producir en Internet, junto con la identificación de niveles de sentimiento respecto a una temática. En la gráfica se aprecian los picos y evolución de la tendencia y relevancia de temáticas dentro de un colectivo específico y para una temática concreta.

¿La solución? Básicamente, tan solo necesitamos alimentar y diseminar el cbersentido común

más efectiva su mensaje a determinados grupos sociales. Según han pasado los años se han producido en el mundo otros acontecimientos relacionados con la escucha masiva en Internet y la generación de mensajes para la creación de tendencia, orientación de voto o encendido de la mecha a una revuelta social. Traigo a colación acontecimien-

tos como la 'Primavera Árabe', el 'Brexit', el proceso electoral de Donald Trump y la supuesta injerencia rusa, las revueltas indígenas en Latinoamérica o los 'chalecos amarillos' en Francia.

Aunque no es lo mismo 'manipular' que 'potenciar una tendencia', la realidad es que la tecnología y el equipo humano

necesarios para realizar todo lo anterior es la doble cara de la misma moneda. Este tipo de tecnologías pueden utilizarse para el bien, para mitigar la temperatura de movimientos hostiles en Internet o para perseguir a cibercriminales, pero también para producir injerencias de información (desinformación), las archiconocidas 'fake news', para ejecutar una estrategia de manipulación, para orientar la intención de voto o para diseminar un mensaje de odio o de exacerbación social.

El 'troll center'

Medición de sentimiento; influencia en tendencias; geolocalización masiva de identidades en Internet; agrupación por afinidad social, política o económica, por perfil psicológico, por gustos, por creencias, por factores emocionales (como el nivel de sensibilidad, de violencia o de nivel cultural)... un sinfín de información aglutinada en sistemas y tecnologías basadas en Big Data e Inteligencia Artificial capaces de ofrecer y brindar en qué puntos debe actuarse para lograr maximizar el objetivo deseado.

A todo este sistema, de forma elegante, se le domina CPI, Centro de Producción de Información. La acepción negativa cuando esta capacidad se utiliza para la injerencia y la desestabilización es más conocida como 'troll center'.

No podemos permanecer ajenos a esta realidad, puesto que constituye la piedra angular, el factor fundamental sobre el cual, si no se actúa de forma eficaz, la ciberseguridad seguirá siendo lo que es, una quimera y entelequia matemática, una red demasiado amplia como para atrapar aquellas amenazas que han demostrado ser eficaces derrocando gobiernos.

¿La solución? Aunque pueda parecer que debería ser difícil de encontrar no lo es. La solución es educación, concienciación, priorización de verdad de este gran problema a todos los niveles de la sociedad. Básicamente, tan solo necesitamos alimentar y diseminar el cbersentido común. ■

GEOLOCALIZACIÓN REAL DE GRUPO DE INTERÉS PARA INFLUENCIA



Mapa global de geolocalización de las identidades o colectivo en seguimiento, identificando por colores dónde se concentran los mayores niveles de incumbencia sobre la temática escuchada. La geolocalización se basa en parámetros de la información pública en los perfiles en seguimiento pero también en geolocalización de las propias publicaciones.

GEOLOCALIZACIÓN REAL DE UNA IDENTIDAD DIGITAL ELEGIDA PARA INFLUIR



Cuando las geolocalizaciones se captan a través de los parámetros de una publicación es posible identificar, con exactitud GPS (latitud, longitud), dónde se encontraba esa identidad cuando realizó la publicación que se está monitorizando.