ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

78/2021 24 de junio de 2021

*Francisco Marín Gutiérrez**

Características del ciberespacio que favorecen las actuales acciones de desinformación y decepción

Características del ciberespacio que favorecen las actuales acciones de desinformación y decepción

Resumen:

El ciberespacio resulta especialmente adecuado para la realización de acciones de desinformación —y, en casos más complejos, de decepción— y, por ello, se ha convertido en el ámbito favorito para esta clase de actividades. Se distingue entre desinformación y decepción porque esta última, según el punto de vista militar, puede englobar actividades en un mayor número de ámbitos que la desinformación.

Además de analizar determinadas características del ciberespacio, en el presente documento se abordan por separado las distintas capas que lo componen —humana, lógica y física— para entender como sus respectivas peculiaridades condicionan la generación, difusión, obtención y análisis de la información.

En definitiva, si las características generales del ciberespacio facilitan que distintos actores lo utilicen para llevar a cabo acciones de desinformación y decepción, las peculiaridades de las capas que integran este ámbito favorecen que dichas acciones incrementen sus posibilidades de éxito.

Palabras clave:

Ciberespacio, decepción, desinformación, redes sociales, cámaras de eco.

*__NOTA:__ Las ideas contenidas en los ***Documentos de Opinión*** son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

Cyberspace characteristics that favour current disinformation and deception actions

Abstract:

Cyberspace is particularly suitable for the conduct of disinformation - and, in more complex cases, deception - actions and has therefore become the favourite domain for this type of activities. This work makes a distinction between misinformation and deception as the latter, according to the military point of view, may encompass activities in a greater number of domains than disinformation.

In addition to analysing cyberspace characteristics, the research has addressed separately its different constitutive layers —human, logical and physical— to understand how their respective peculiarities condition the generation, dissemination, collection, and analysis of information.

In short, the general characteristics of cyberspace facilitate its use by different actors to carry out disinformation and deception actions; in addition to that, the peculiarities of the layers that make up this domain increase the chances of success of such actions.

Keywords:

Cyberspace, deception, disinformation, echo chambers.

Cómo citar este documento:

MARÍN GUTIÉRREZ, Francisco. *Características del ciberespacio que favorecen las actuales acciones de desinformación y decepción*. Documento de Opinión IEEE 78/2021. http://www.ieee.es/Galerias/fichero/docs_opinion/2021/DIEEEO78_2021_FRANMAR_Ciber.pdf y/o enlace bie[3] (consultado día/mes/año)

Introducción

«Nosotros configuramos nuestras herramientas,
y después ellas nos configuran a nosotros»
Marshall McLuhan

El rápido desarrollo de las tecnologías y plataformas de comunicación digitales han producido una transformación generalizada de nuestro modo de vida, trabajo y relaciones. El fenómeno ha alcanzado dimensiones sin precedentes e incluso ha generado su propio ámbito, el ciberespacio. Aprovecharemos para explicar que los ámbitos de operaciones son «espacios, físicos y no físicos, dotados de características propias y diferenciadas que condicionan las aptitudes y procedimientos de las fuerzas que deben operar en ellos[1]». Y que frente a los ámbitos de actuación físicos o tradicionales —terrestre, marítimo y aeroespacial— existen otros dos, el ciberespacial y el cognitivo, que guardan una estrecha relación por su carácter transversal y por generar una serie de zonas híbridas comunes a dos o más espacios.

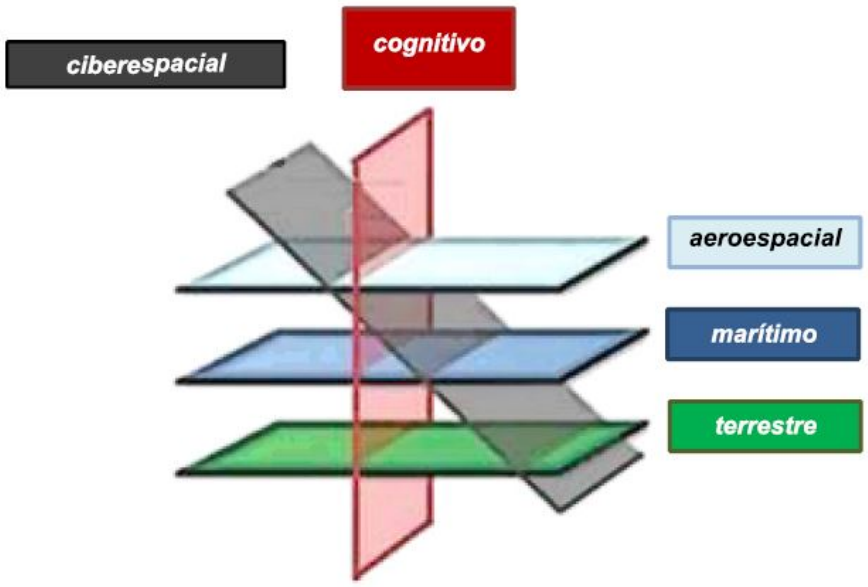

Figura 1. Ámbitos de operaciones. Fuente. PDC-01 (A). Doctrina para el empleo de las Fuerzas Armadas.

[1] También se han denominado a veces como *dominios*, traducción directa de palabra en inglés *domain*.

A su vez, el ciberespacio ha propiciado un incremento del número de actores con capacidad de ejercer influencia, generando igualmente una sobreabundancia de fuentes de información, circunstancias que disminuyen nuestra capacidad de análisis y favorecen la proliferación de fenómenos de manipulación informativa: difusión de bulos, desinformación, decepción, etc. Estos fenómenos no se limitan únicamente a grandes operaciones, como la posible interferencia en los procesos electorales de otras naciones, sino que también suceden en un nivel mucho más cotidiano, con acciones básicas de engaño como, por ejemplo, la suplantación. Según un estudio de ciberseguridad en España, el 64,8 de los usuarios de Internet reconocía haber sufrido algún problema de seguridad y un 12 % de este grupo, —77 760 individuos por cada millón de usuarios— era consciente de que su identidad había sido suplantada[2]. El número de casos resulta lo suficientemente elevado como para reflexionar sobre el tema.

Este trabajo se centra en la desinformación y la decepción por considerar que se trata de los fenómenos más elaborados de manipulación informativa y resulta necesario comprender la diferencia entre ambos. Según la doctrina militar se entiende por decepción «aquellas medidas diseñadas para llevar a error al enemigo mediante la manipulación, distorsión, o falsificación de las evidencias que le induzcan a reaccionar de una manera perjudicial para sus intereses»[3]. Otra acepción más genérica, procedente del ámbito académico, establece que la decepción es «la información diseñada para manipular el comportamiento de otros induciéndoles a aceptar presentación falsa o distorsionada de su entorno físico, social, o político»[4].

Respecto a la definición de desinformación se ha escogido la propuesta por la Unión Europea, que entiende el concepto como «información verificablemente falsa o engañosa que se crea, presenta y divulga con fines lucrativos o para engañar deliberadamente a la población, y que puede causar un perjuicio público»[5].

[2] "Estudio sobre la ciberseguridad y confianza del ciudadano en la Red. Oleada enero - junio 2020", *Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI)*, Madrid, noviembre de 2020. Disponible en: https://www.ontsi.red.es/sites/ontsi/files/2021-02/EstudioCiberseguridadConfianzaOleadaEneroJunio2020.pdf. Fecha de consulta 01/05/2021.
[3] "NATO Glossary of Terms and Definitions (DLW Edition)". Nov 1997. La misma en *Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms*. 12 April 2001.
[4] WHALEY, B. "Toward a General Theory of Deception. Military Deception and Strategic Surprise", *Frank Cass,* Londres, 1982.
[5] "COM(2018) 236. La lucha contra la desinformación en línea: un enfoque europeo", *Unión Europea*, Bruselas, 4 de abril de 2018. Disponible en: https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018DC0236&from=PL. Fecha de consulta 05/05/2021.

Resumiremos las diferencias entre ambos conceptos diciendo que la desinformación se centra en modificar las opiniones y percepciones del objetivo, desarrollándose en el ámbito cognitivo, mientras que la decepción —que se lleva a cabo en todos los ámbitos, incluidos los físicos— va un paso más allá y tiene por objeto engañar a los responsables de la toma de decisiones para que reaccionen de manera favorable a nuestros intereses.

Regresando al ciberespacio, que no hemos abandonado si estamos leyendo una copia digital del presente trabajo, este resulta un ámbito especialmente adecuado para el desarrollo de las acciones de engaño, y la terminología militar lo define como un «ámbito global y dinámico compuesto por las infraestructuras de tecnología de la información —incluida Internet—, las redes y los sistemas de información y de telecomunicaciones»[6]. Respecto a sus características, según la Estrategia Nacional de Ciberseguridad, el ciberespacio es «un espacio común global caracterizado por su apertura funcional y su dinamismo. La ausencia de soberanía, su débil jurisdicción, la facilidad de acceso y la dificultad de atribución de las acciones»[7]. Estas características motivan que las operaciones que en él se desarrollan destaquen por su:

- Alcance: la ausencia de fronteras posibilita que una acción iniciada en un punto termine afectando de forma casi instantánea a elementos situados en cualquier parte del mundo.
- Asimetría: el acceso al ciberespacio es global, sencillo y económico. Un individuo o pequeña organización pueden, con un mínimo de capacidad técnica y recursos, producir efectos en un oponente con el que se guarda total desproporción.
- Anonimato: la utilización de identidades virtuales facilita la ocultación de la verdadera personalidad e intenciones de individuos o grupos. Son fenómenos frecuentes usurpar la ciberidentidad de terceros para ocultar las actividades propias o llevar a cabo operaciones de decepción mediante acciones de «falsa bandera»[8] o utilizando agentes interpuestos (*proxies*). La atribución de las

[6] "PDC-00 Glosario de Terminología de Uso Conjunto", *Estado Mayor de la Defensa*, Madrid, julio de 2020. Disponible en: https://www.defensa.gob.es/ceseden/Galerias/ccdc/documentos/PDC-00_Ed_2019_FIRMADA.pdf. Fecha de consulta 01/05/2021.
[7] Orden PCI/487/2019, de 26 de abril, por la que se publica la Estrategia Nacional de Ciberseguridad 2019. 26 de abril de 2019. Disponible en: https://www.boe.es/boe/dias/2019/04/30/pdfs/BOE-A-2019-6347.pdf. Fecha de consulta 30/04/2021.
[8] SKOPIK, Florian y PAHI, Timea. "Under false flag: using technical artifacts for cyber-attack attribution", *Cybersecurity, SpringerOpen*, marzo de 2020. Disponible en:

actividades se convierte en un problema fundamental, siendo necesario combinar múltiples disciplinas del área de la Inteligencia y del análisis forense para lograr resultados. El grado de sofisticación del ejecutante incrementa la dificultad de la atribución e incluso puede hacerla imposible.

- Tempo: las acciones en el ciberespacio pueden tener efectos inmediatos, o bien pueden retardarse, según la finalidad a alcanzar. La complejidad del objetivo, las técnicas a utilizar y el grado de anonimato deseado pueden suponer que preparar una acción en el ciberespacio requiera más tiempo que utilizar un arma convencional.

- Versatilidad: resulta interesante reutilizar infraestructuras técnicas o herramientas empleadas previamente. Ello puede reducir la posibilidad de mantener el anonimato o bien potenciarlo al utilizar recursos de otras entidades. Existen casos donde grupos de espionaje vinculados a un país dificultan la atribución empleando elementos asociados previamente a otra nación.

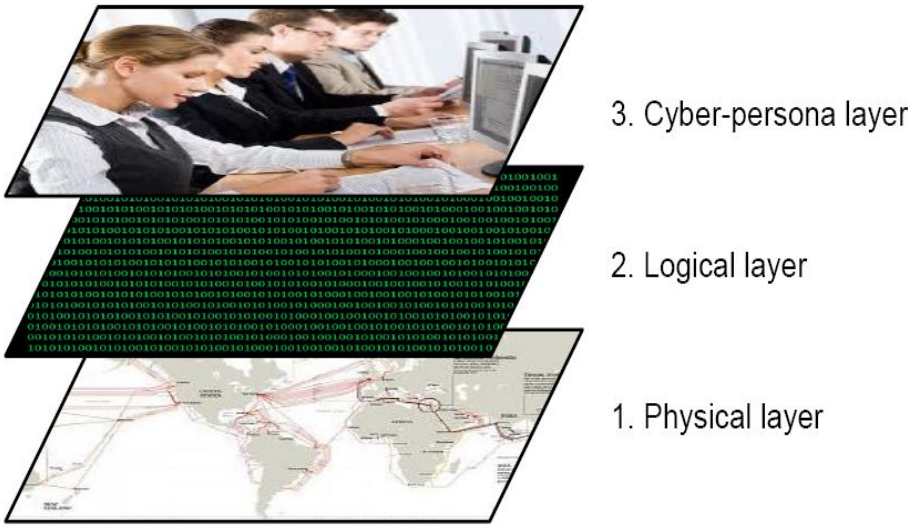

Figura 2. Capas integrantes del ciberespacio. Fuente. NATO STANDARD AJP 3-20 Cyberspace Operations, Ed A Version 1.

https://cybersecurity.springeropen.com/track/pdf/10.1186/s42400-020-00048-4.pdf. Fecha de consulta 06/05/2021.

Para entender determinados fenómenos, a las características reseñadas debemos añadir las particularidades de las partes componentes del ciberespacio. La estructura de este ámbito se suele explicar mediante un modelo de capas, y aquí se utilizará la versión sancionada por la OTAN. Según dicho modelo, el ciberespacio está constituido por tres capas o redes interrelacionadas: física, lógica y humana o de «ciberpersonas»[9].

La capa física la integran los dispositivos de las tecnologías de la información y la infraestructura física que proporciona almacenamiento, transporte y procesamiento de información, incluyendo los repositorios de datos y las conexiones para transferir datos. La capa lógica se compone de elementos expresados mediante código, tales como sistemas operativos, protocolos y otros componentes de *software* o conjunto de aplicaciones que hacen posible la realización de tareas específicas. Finalmente tenemos la capa humana, que no contiene personas u organizaciones reales, sino representaciones de identidades virtuales como direcciones de correo electrónico, nombres de usuario o cuentas en redes sociales. En consecuencia, cada persona puede tener simultáneamente varias personalidades cibernéticas y, por otro lado, varias personas u organizaciones pueden compartir una misma personalidad, como el correo corporativo de una organización. Esta realidad también dificulta el citado proceso de atribución.

El conjunto de características citado explica la proliferación de actividades informativas hostiles en el ciberespacio pues, con un coste reducido y mínimo riesgo para el atacante, proporcionan elevada efectividad. Analizaremos a continuación las peculiaridades de las capas componentes de este ámbito para determinar cómo favorecen la difusión e incrementan las posibilidades de éxito de las acciones de desinformación y decepción.

Elementos de la capa física

A medida que avanza la tecnología los aparatos se hacen más útiles y atractivos para que los usuarios les dediquemos cada vez más tiempo y atención. Así, dispositivos como los teléfonos móviles inteligentes —*smartphones*— no solo se han convertido en elementos insustituibles de comunicación sino en una de las principales herramientas de

[9] NATO STANDARD AJP 3-20 Cyberspace Operations, Edition A Version 1. NATO STANDARDIZATION OFFICE, 2020. Disponible en: https://nso.nato.int/nso/nsdd/_CommonList.html Fecha de consulta 02/05/2021.

acceso a fuentes de información cuando no la única (en 2020 un 94,3 % de los españoles accedía a Internet a través de ellos[10]). La necesidad de optimizar la interacción entre usuarios y dispositivos ha adquirido especial relevancia y constituye un nuevo campo de actuación. De hecho, el diccionario incluye ya un término que materializa dicha interacción, el «interfaz, definido como la conexión, física o lógica, entre una computadora y el usuario, un dispositivo periférico o un enlace de comunicaciones». En el caso del *smartphone*, el interfaz es la pantalla y, según su diseño y el de las aplicaciones concebidas para su sistema operativo, podemos obtener experiencias positivas o absolutamente frustrantes. Una mala experiencia puede llevarnos a rechazar una aplicación o un modelo concreto de terminal telefónico, lo que obliga a las empresas a ofrecer servicios atractivos y utilizables por el mayor número posible de usuarios. Aparece así el concepto de Diseño de Experiencia de Usuario (UX Design), actividad que «se encarga de que la percepción y sensaciones que el uso de un producto o servicio deja en la mente de las personas sean las óptimas bajo cualquier punto de vista: ergonomía, facilidad de uso, eficiencia, etc.»[11]. Cuanto más satisfactoria sea la experiencia, más utilizaremos el dispositivo digital en detrimento de otras fuentes de información, como la prensa escrita.

Por su diseño y construcción los dispositivos cibernéticos disfrutan de ventajas sobre los humanos y otras tecnologías a la hora de difundir información, verdadera o falsa, e influenciar. Los ordenadores resultan más eficaces respecto a los medios de comunicación tradicionales y según algunos autores resultan más eficaces que las personas a la hora de ejercer la persuasión debido a varios motivos[12]:

- Persistencia: ningún humano es tan perseverante como una máquina, un ordenador no se cansa ni se desconcentra, repetirá el mismo mensaje las veces que sea necesario.
- Anonimato: nos resulta más sencillo proporcionar datos a una plataforma aparentemente anónima que a una persona real, y de igual forma se aceptan

[10] "Marco General de los Medios en España 2021*", Asociación para la Investigación de Medios de Comunicación*. Madrid, 2021. Disponible en: https://www.aimc.es/a1mc-c0nt3nt/uploads/2021/02/marco2021.pdf. Fecha de consulta 02/05/2021.
[11] HUERTA, Eduardo. "Introducción al Diseño de Interfaces y de Experiencia de Usuario (UI/UX Design)", *Educaweb*, 9 de junio de 2014. Disponible en: https://www.educaweb.com/noticia/2014/06/09/introduccion-diseno-interfaces-experiencia-usuario-ui-ux-design-8275/. Fecha de consulta 05/05/2021.
[12] FOGG, B.J. "Persuasive Technology. Using Computers to Change What We Think and Do", *Morgan Kaufmann Publishers*, San Francisco, 2003.

mejor los consejos de una máquina que de una persona con la que nos relacionamos presencialmente.

- Gestión de datos: los ordenadores manejan, almacenan e interrelacionan enormes cantidades de datos y, con las herramientas adecuadas, realizan predicciones sobre nuestras respuestas y reacciones.
- Múltiples modalidades para influenciar: pueden utilizar textos, imágenes, audio, vídeos, etc., según las preferencias del grupo objetivo.
- Capacidad de escalada: pueden crecer rápidamente según se incrementen las necesidades, es decir, según aumente la audiencia.
- Ubicuidad: los ordenadores llegan hasta donde los humanos no pueden o no son bienvenidos y pueden estar en cualquier lugar, incluso dentro de nuestros espacios de mayor privacidad como dormitorios o cuartos de baño.

Podemos afirmar que el objetivo del diseñador es que, al interactuar con un dispositivo, el usuario obtenga resultados o experiencias acorde a sus expectativas. El problema se presenta cuando la experiencia resulta tan satisfactoria que el uso del dispositivo se convierte en adictivo y va acaparando mayor proporción del tiempo del usuario. Sin llegar al extremo de los *hikikomori* en Japón —jóvenes aislados de la sociedad que viven recluidos en su mundo virtual al que acceden a través de diferentes terminales—, existe una crecente tendencia a convertir los dispositivos con acceso a Internet en la principal ventana al mundo exterior y en única fuente de noticias e información. Un estudio de abril de 2020 recoge que, en España, un 79 % de los entrevistados accedía a las noticias a través de medios online, y un 56 % utilizaba las redes sociales para ello[13].

Esta facilidad de acceso a través de terminales extremadamente atractivos y adictivos, unido al hecho de que vivimos en la era de la sobreabundancia de información[14], tienen como consecuencia que somos incapaces de prestar atención y carecemos de tiempo para comparar fuentes y comprobar la veracidad de la información, disminuyendo nuestra capacidad de análisis. Un escenario perfecto para el éxito de la desinformación.

[13] NEWMAN, Nic; FLETCHER, Richard; SCHULZ, Anne; ANDI, Simge y NIELSEN KLEIS R. "Digital News Report 2020", *Reuters Institute*, 2020. Disponible en: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf Fecha de consulta 01/05/2021.
[14] LEVITIN, Daniel. J. "The organized mind: Thinking straight in the age of information overload", *Dutton*, Penguin Group. Nueva York, 2014.

Elementos de la capa lógica

Aunque se trata de una parte eminentemente técnica relativa a los programas que hacen funcionar a los ordenadores, esta capa también está relacionada con los condicionamientos del receptor de la información, de los que también hablaremos posteriormente. Veremos a continuación como las aplicaciones informáticas y su utilización son capaces de influir en las decisiones y opiniones de los usuarios, bien propiciando que solo utilicemos información filtrada o bien proponiendo directamente respuestas o modos de comportamiento.

La propensión para encontrar solo aquello que nos gusta

Los cambios tecnológicos, especialmente el auge de las redes sociales como fuente de información primordial, han creado dos fenómenos que predisponen la aceptación de información falsa, son los denominados «filtros burbuja y cámaras de resonancia».

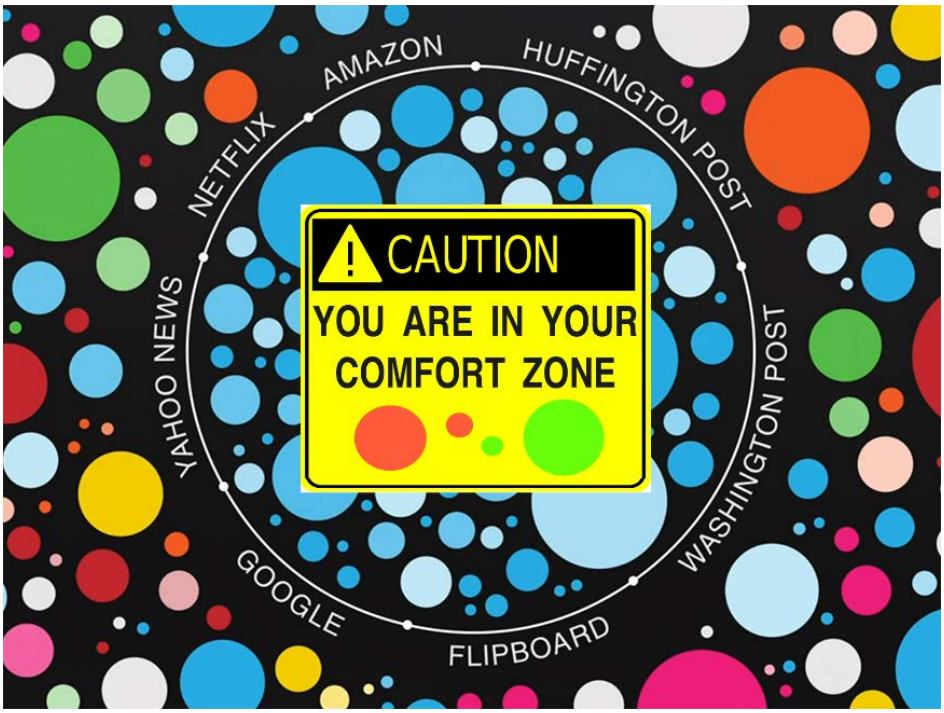

Figura 3. Concepto de filtro burbuja. Fuente. Disponible en: https://ucm.teleshuttle.com/2016/12/

Los «filtros burbuja» son resultado de las búsquedas personalizadas que determina el algoritmo de un motor de búsqueda (abreviadamente, «buscador») en Internet. Estos programas seleccionan, mediante estimaciones basadas en parámetros como el historial

de búsquedas previas, la información que se supone que al usuario le gustaría ver, filtrando aquella que discrepa de sus puntos de vista y aislándolo en una especie de burbuja ideológica y cultural. Edi Pariser, creador del concepto, explica que actualmente Internet se adapta a cada usuario y que plataformas como Facebook o Google filtran de forma individualizada la información que nos ofrecen. Y esto es algo que los propios buscadores como Google reconocen, que en 2009 ya anunciaba que para obtener mejores resultados iba a «personalizar los resultados de búsqueda en función de 180 días de actividad de búsqueda vinculada a una cookie anónima de su navegador»[15]. Esto implica que, salvo que desconectemos la personalización —opción que muchos desconocen—, el buscador utilizará el historial de los últimos seis meses para mostrarnos lo que opina deberíamos ver. No obstante, también según Pariser, un motor de búsqueda como Google utiliza realmente 57 características para determinar los resultados de las preguntas de cada usuario[16]. Además del historial, se incluye el idioma, versiones del navegador y sistema operativo utilizados, tiempo entre búsquedas y tiempo invertido en cada página visitada, frecuencia con la que se seleccionan anuncios, etc., todo para presentar únicamente lo que se supone le gusta al usuario, que no tiene que coincidir con lo que realmente le puede interesar ver. Según el creador del concepto, «estos motores de búsqueda crean un universo único de información para cada uno de nosotros que altera fundamentalmente la forma en que encontramos ideas e información»[17].

En cuanto a las «cámaras de resonancia», son el resultado del diseño y uso selectivo de las plataformas sociales, y describen un entorno en el que alguien solo encuentra opiniones y creencias similares a las suyas, donde no tiene que considerar alternativas pues no existe ningún debate, siendo especialmente eficaces para reforzar puntos de vista extremos. Están directamente relacionadas con el concepto de «sesgo de confirmación», que describe la tendencia humana para buscar información que confirme las creencias preexistentes y rechazar información contradictoria con dichas creencias evitando así la «disonancia cognitiva».

[15] "Personalized Search for everyone", *Google Official Blog*, 4 de diciembre de 2009. Disponible en: https://googleblog.blogspot.com/2009/12/personalized-search-for-everyone.html. Fecha de consulta 02/05/2021.
[16] PARISER, Eli. "Beware inline filter bubbles", *TED Talks*, 2014. Disponible en: https://tedsummaries.com/tag/eli-pariser/. Fecha de consulta 05/05/2021.
[17] PARISER, Eli. "The Filter Bubble: What the Internet Is Hiding from You", *The Penguin Press*, Nueva York, 2011.

Algunos plantean el fenómeno de la cámara de resonancia a dos niveles: por un lado, una cámara cognitiva individual creada por los usuarios como resultado de un «sesgo de confirmación» y, por otro, una red de individuos que postulan unas ideas y narrativas similares en cuanto a su forma de ver el mundo[18].

Como consecuencia de los fenómenos anteriores se consigue que únicamente se compartan y amplifiquen conjuntos parciales de información. Esta tendencia está adquiriendo una importancia significativa y supone un serio desafío para la difusión de información veraz. El problema fue reconocido por el Grupo de Alto Nivel sobre Libertad en los Medios y el Pluralismo, constituido en 2011 por el Consejo Europeo para formular recomendaciones que fomenten la libertad de los medios de comunicación en Europa. Su informe final afirmaba que: «Los crecientes mecanismos de filtrado hacen que sea más probable que las personas sólo reciban noticias acerca de temas que les interesan y con la perspectiva con la que se identifican. […] Estos acontecimientos, sin duda, tienen un impacto potencialmente negativo en la democracia. De esta manera podemos llegar a leer y escuchar lo que queremos, y nada más que lo que queremos»[19].

También en otros foros internacionales como la Munich Security Conference en 2017, se ha afirmado en relación con estos fenómenos que «todo ello crea una estructura a la espera de ser explotada, tanto por los populistas dentro de nuestras sociedades como por actores externos interesados»[20].

Persuasión tecnológica

Abordamos aquí un conjunto de principios básicos de persuasión propios de entornos digitales. Diversas fuentes denominan «tecnología persuasiva» *(persuasive technology)* a cualquier sistema informático interactivo diseñado para modificar las actitudes o comportamientos de las personas. Inicialmente, los ordenadores no fueron diseñados

[18] SCHLEGEL, Linda. "¿Cámaras de los secretos? Cámaras de eco cognitivas y el rol de las redes sociales para facilitarlas", *European Eye on Radicalization*, 19 de septiembre de 2019. Disponible en: https://eeradicalization.com/es/camaras-de-los-secretos-camaras-de-eco-cognitivas-y-el-rol-de-las-redes-sociales-para-facilitarlas/. Fecha de consulta 05/05/2021.

[19] VAIRA VĪKE-FREIBERGA et al., "A Free and Pluralistic Media to Sustain European Democracy", *Report of the High Level Group on Media Freedom and Pluralism*, enero de 2013. Disponible en: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/HLG%20Final%20Report.pdf. Fecha de consulta 05/05/2021.

[20] "Munich Security Report 2017: Post-Truth, Post-West, Post-Order?". Disponible en: https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/MunichSecurityReport2017.pdf. Fecha de consulta 02/05/2021.

para influir en los comportamientos sino para realizar operaciones y manejar datos, pero estos ingenios se han convertido en herramientas imprescindibles que desarrollan acciones de influencia anteriormente llevadas a cabo por profesores, asesores y vendedores. Este papel comenzó a desarrollarse en la década de los 80 con los primeros sistemas destinados a promover mayor productividad en los puestos de trabajo y a mejorar nuestra salud, siendo pionero el Body Awareness Resource Network (BARN), desarrollado para promover específicamente un estilo de vida saludable entre los adolescentes del ámbito rural, ofreciendo consejos acerca de todo tipo de aspectos del comportamiento[21].

La popularización del uso de Internet incrementó el grado de persuasión e intervención de los ordenadores en nuestras vidas: cada buscador pretende que le otorguemos la exclusividad y lo utilicemos por defecto, las plataformas de ventas intentan que escojamos los productos que nos sugieren según sus propios acuerdos económicos, etc. Y todos intentan obtener nuestros datos con el pretexto de personalizar las experiencias y poder ofrecernos los bienes, servicios y contenidos que se estima nos deben gustan en función de la información proporcionada. Una nueva dimensión es la alcanzada mediante las aplicaciones —*apps*— desarrolladas para dispositivos móviles, que no solo orientan nuestro consumo, sino que prometen ayudarnos a mejorar todos los aspectos de nuestras vidas, desde los físicos a los espirituales. Conviene resaltar que los nuevos medios digitales cuentan con una ventaja frente a las plataformas tradicionales, la interactividad, que proporciona a quien persuade de retroalimentación para corregir sus acciones según las respuestas recibidas.

Una de las condiciones necesarias para que aceptemos los mensajes enviados en el marco de una actividad de desinformación o decepción es que las fuentes sean consideradas creíbles. El análisis de los elementos que dan credibilidad a los medios informáticos llevó a B. J. Fogg a crear el término *captology* —acrónimo de *computers as persuasive technologies* (ordenadores como tecnologías persuasivas)— para designar la actividad que tiene como objetivo «el diseño, investigación y análisis de productos

[21] MARSON, Stephen M. "Body Awareness Resource Network (BARN): Software Review", *Journal of Technology in Human Services*, vol. 21(3), 2003. Disponible en: https://libres.uncg.edu/ir/uncp/f/Body%20Awareness%20Resource%20Network_Software%20Review.pdf Fecha de consulta 05/05/2021.

informáticos interactivos creados con el propósito de cambiar las actitudes o comportamientos de las personas»[22].

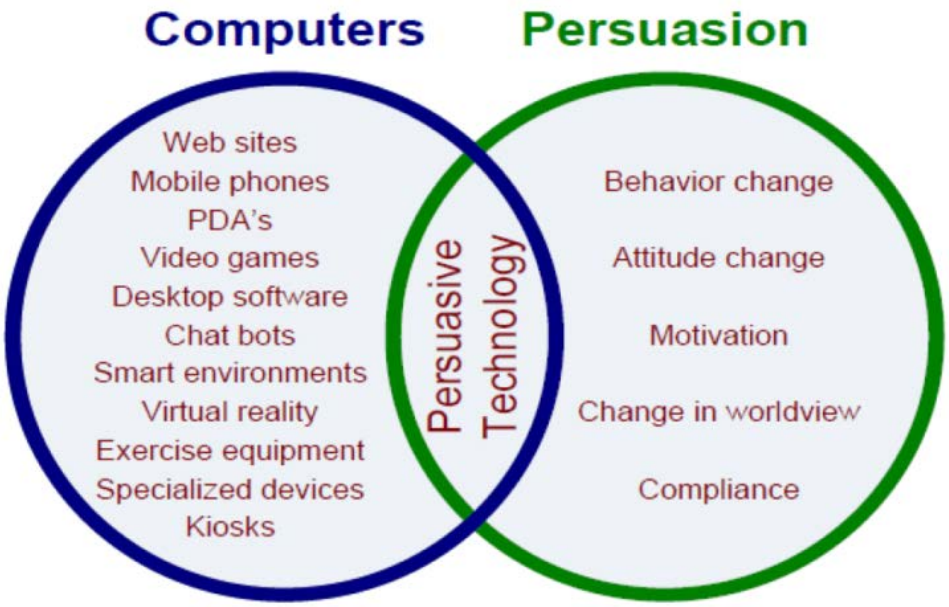

Figura 4. Concepto de captología. Fuente. Disponible en: https://tofasakademi.com/tr/persuasive-tech/

Este estudio se centra en la relación persona-ordenador para comprender cómo los individuos somos persuadidos al interactuar con la tecnología informática, en como el producto se diseña para convertirse en origen de los intentos de persuasión. En este ámbito, Fogg propuso los siguientes tipos de credibilidad para las plataformas en Internet:

- Supuesta: basada únicamente en las suposiciones generales realizadas por el usuario, que incluyen todo tipo de estereotipos. Contribuye mucho que el sitio pertenezca a una organización supuestamente sin ánimo de lucro o que el dominio acabe en .org
- Reconocida: derivada u obtenida en base a informaciones o referencias de terceros. Se incrementa si el sitio ha sido recomendado por alguien de nuestro círculo de amistades.

[22] FOGG, B.J; TSENG, Hsiang. "The Elements of Computer Credibility", *CHI 99*, Proceedings of the SIGCHI conference on Human Factors in Computing Systems. Pittsburgh, mayo de 1999. Disponible en: https://dl.acm.org/doi/10.1145/302979.303001 Fecha de consulta 03/05/2021.

- Superficial: nivel de interacción limitado a la parte estética, basado en las primeras impresiones y en la simple inspección de la apariencia. Influyen fundamentalmente los factores de su diseño.
- Experimentada: derivada de la experiencia de primera mano obtenida por el usuario con el sitio web durante un cierto período de tiempo.

El mismo autor y otros investigadores del Stanford Persuasive Technology Lab determinaron que los principales elementos que transmiten y refuerzan la credibilidad de un sitio web evocando fiabilidad y experiencia son[23]:

- profesionalidad del diseño
- profundidad del contenido: se pueden buscar contenidos publicados en el pasado, se citan las credenciales de los autores de los artículos
- el sitio se actualiza periódicamente
- se proporcionan datos de contacto como una dirección física, direcciones de correo electrónico o teléfonos
- incluye contenidos con referencias que se pueden verificar
- contiene enlaces a materiales y fuentes externas creíbles

Por el contrario, la credibilidad de una página es afectada negativamente si existen errores tipográficos, contenidos no actualizados o confusos —anuncios que no se distinguen del verdadero contenido—, o si carece de datos de contacto. La primera impresión resulta fundamental, y cuando un usuario abre una página web, la decisión sobre su fiabilidad se toma en segundos. Así, si un atacante quiere diseñar una página para difundir informaciones falsas deberá prestar especial atención no solo a hacerla atractiva sino a que también transmita credibilidad.

Pero la ética de los quienes elaboran una página web puede ser discutible, y en este sentido muchas empresas o individuos desean no solo atraer sino incitar a quienes las visitan a realizar una acción concreta. Nace así el concepto de *dark pattern* (diseño confuso), opciones de diseño de interfaz de usuario que benefician a un servicio al coaccionar, direccionar, o engañar a los usuarios en la adopción de decisiones que, si estuvieran plenamente informados, podrían no tomar. Harry Brignull acuñó el neologismo en 2010 y fundó *darkpatterns.org*, una biblioteca de ejemplos de interfaces de usuario

[23] FOGG, B.J. “Persuasive Technology Using Computers to Change What We Think and Do”, *Morgan Kaufmann Publishers*, San Francisco, 2003.

engañosas. El autor afirma que «cuando se usan sitios web y aplicaciones, no se lee cada palabra en cada página: lees y haces suposiciones. Si una empresa quiere engañarte para que hagas algo, pueden aprovechar esto haciendo que una página parezca que está diciendo una cosa cuando en realidad está diciendo otra»[24]: En cuanto a la clasificación de este tipo de prácticas engañosas en páginas web, estudios académicos han englobado los casos definidos inicialmente por Brignull junto a otros más recientes en cuatro grandes categorías[25]:

- Persistencia: redirección de la funcionalidad esperada que puede persistir durante varias interacciones. Se manifiesta como una intrusión repetida durante la interacción normal, donde la tarea en la que se centra el usuario es interrumpida por otras no relacionadas (anuncios en ventanas emergentes, mensajes de audio, etc.)
- Obstrucción: convertir un proceso en algo más difícil de lo que debe ser, con la intención de disuadir al usuario de realizar ciertas acciones. Por ejemplo, dificultar la cancelación de una suscripción tipo Premium a determinados servicios.
- Escabullirse: ocultar, disfrazar o retrasar la divulgación de información relevante para el usuario, sobre todo si dicha información pudiera llevar a realizar una acción contraria a la deseada por el diseñador de la página.
- Interferencia en el interfaz: manipulación de la interfaz de usuario que privilegia ciertas acciones sobre otras. Se manifiesta mediante diversos tipos de engaño y se subdivide en tres subtipos: información oculta (opciones relevantes para el usuario no aparecen de forma inmediata —costes adicionales que solo aparecen al final de un proceso de compra— o no resultan fácilmente accesibles), preselección (la opción favorable al diseñador se selecciona de forma predeterminada antes de la interacción del usuario) y manipulación estética (opciones que tratan de distraer la atención del usuario)
- Acción forzada: exige realizar una determinada acción para acceder a ciertas funciones. Puede manifestarse como un paso necesario para completar un proceso, o aparecer disfrazado como una opción beneficiosa para el usuario (por

[24] BRIGNULL, Harry. "Types of dark pattern". Accesible en https://www.darkpatterns.org/types-of-dark-pattern Fecha de consulta 05/05/2021.
[25] GRAY, Colin M; KOU, Yubo; BATTLES, Bryan; HOGGATT, Joseph y. TOOMBS, Austin L. "The Dark (Patterns) Side of UX Design", *CHI 2018 Paper*, Conference on Human Factors in Computing Systems 2018, pp. 21-26, abril 2018, Montréal, Canadá. Disponible en: https://dl.acm.org/doi/pdf/10.1145/3173574.3174108. Fecha de consulta 05/05/2021

ejemplo, juegos en red que sugieren al usuario que invite a sus amigos a participar, recibiendo a cambio beneficios en dicho juego)

Este tipo de manipulación mediante el diseño de la plataforma ha sido reconocido en muy diversos ámbitos. El Consejo Noruego de Consumidores (Forbruckerrådet) analizó la configuración de Facebook, Google y Windows 10 para comprobar si era respetuosa con el nuevo Reglamento General de Protección de Datos (RGPD) europeo, llegando a interesantes resultados directamente relacionados con los «patrones confusos»[26]. El estudio concluyó que tanto la configuración predeterminada como las características del diseño de interfaz están concebidas para manipular a los usuarios y empujarlos a escoger las opciones menos respetuosas con la privacidad. Los hallazgos incluyen ajustes por defecto intrusivos en la privacidad, opciones redactadas de forma que inciten a los usuarios a realizar determinadas elecciones, la ocultación de las opciones más favorables para el consumidor y la utilización de arquitecturas de elección donde seleccionar la opción que más respeta la privacidad requiere un esfuerzo mayor.

Añadir que la preocupación por los patrones confusos no se limita al escenario europeo, donde el RGPD es de obligado cumplimiento, sino que se ha incorporado a otras legislaciones, como la Ley de Protección de la Privacidad de California, cuya modificación entrará en vigor en enero de 2023, que define un patrón confuso como «un interfaz de usuario diseñado o manipulado con el efecto sustancial de subvertir o afectar la autonomía, proceso de toma de decisiones o elección del usuario» y se afirma que, «de igual manera, el acuerdo obtenido mediante el empleo de patrones oscuros no constituye consentimiento»[27].

En definitiva, determinadas peculiaridades de la capa lógica se utilizan para tratar de modificar las actitudes de los usuarios y orientar sus opiniones, convirtiéndose en herramientas para obstaculizar nuestra capacidad de análisis.

[26] "Deceived by Design", *Forbruckerrådet*. 27 de junio de 2018. Disponible en: https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf. Fecha de consulta 05/05/2021.

[27] "Submission of Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021". Disponible en: https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1%20%28Consumer%20Privacy%20-%20Version%203%29_1.pdf Fecha de consulta 05/05/2021.

Elementos de la capa humana

Actualmente las personas trabajamos y desarrollamos vidas virtuales en el ciberespacio y en estas nuevas relaciones influyen aquellos factores que condicionan nuestro razonamiento. Estas peculiaridades, que se han tratado de resumir en dos grandes bloques, convierten a las personas en los elementos que más favorecen la desinformación en el ciberespacio.

La propensión para creer

Una de las principales peculiaridades de los bulos es la propensión por parte de quien los recibe a creerlos y asimilarlos como si de información verdadera se tratase. El actual ritmo de vida acelerado implica que no se evalúan ni analizan los estímulos que recibimos por falta de tiempo. No obstante, existen otros motivos que favorecen dicha propensión, íntimamente ligados a la psicología humana. Se trata de los denominados *sesgos cognitivos*, que son efectos psicológicos que producen una distorsión en el procesamiento e interpretación de la información captada, dando lugar a juicios inexactos o interpretaciones ilógicas. Es un tema amplísimo, especialmente estudiado en los procesos de toma de decisiones, que considera un gran número de tales efectos. Además del ya citado sesgo de confirmación podríamos mencionar otros como el anclaje —la tendencia juzgar una situación basándonos en la información que se acaba de recibir— o la percepción selectiva. No obstante, para limitar la extensión del presente trabajo se ha optado por destacar dos por considerar que son los que más se ajustan al tema analizado.

Por un lado, tenemos el autoengaño, conocido también como teoría del razonamiento motivado. Se basa en el hecho de que las motivaciones de los receptores configuran las informaciones recibidas para que se ajusten a sus creencias y opiniones, es decir, que nuestras emociones nos llevan a otorgar mayor importancia a la información acorde a los puntos de vista propios y a ignorar aquellos hechos que los contradicen. Por eso, si las informaciones que recibimos se acomodan a nuestra visión del mundo, somos menos escrupulosos a la hora de verificarlas y analizarlas. Es uno de los principios en los que tradicionalmente se han basado las grandes operaciones militares de decepción.

Por otro lado, existe el denominado efecto arrastre o efecto Bandwagon, referido al hecho de que los individuos pensamos y nos comportamos en función de la opinión

predominante que existe en nuestro entorno. Dicho efecto está detrás de lo que en marketing se denomina *social proof* —prueba social— según la cual, ante la falta de información o experiencias acerca de un tema, un sujeto adopta el comportamiento de un colectivo bajo la presunción de que este tiene un mayor conocimiento. Esto se plasma en la realidad cuando una empresa crea la percepción de que la mayoría del mercado consume determinado producto, de forma que los demás consumidores se sentirán más inclinados a seguir la tendencia.

Del mismo modo, si sólo leemos noticias de la misma orientación o estamos rodeados de personas que piensan igual, nos resultará mucho más difícil ser críticos y opinar lo contrario, especialmente por el miedo a no ser aceptados por el grupo al que se supone pertenecemos. Además, recibir información que no concuerda con los puntos de vista propia genera —en mayor o menor medida— lo que conoce como disonancia cognitiva, un estado mental de incomodidad del que se sale fácilmente seleccionando la información que queremos consumir.

Comportamientos que amplifican la difusión

Abordaremos aquí la desinhibición en internet. Cualquiera puede observar como en el ciberespacio muchas personas dicen y hacen cosas que en el mundo real nunca se atreverían a decir o hacer. Este fenómeno puede funcionar en sentidos opuestos: por un lado, puede dar lugar a compartir experiencias personales acompañadas de comportamientos altruistas; por otro lado, puede originar comportamientos realmente tóxicos donde se expresan opiniones extremas en términos groseros o violentos que pueden ser explotados por una campaña de desinformación. El psicólogo norteamericano John Suler denominó a este fenómeno el efecto de desinhibición online, y cita seis factores específicos del uso del ciberespacio que contribuyen al mismo[28]:

- Anonimato disociativo: estar detrás de una pantalla proporciona una sensación de anonimato que posibilita separar las acciones realizadas en el ciberespacio de las de la vida real.

[28] SULER, John. “The Online Disinhibition Effect”, *CyberPsychology & Behavior*, julio 2004. Disponible en: https://www.researchgate.net/publication/8451443_The_Online_Disinhibition_Effect/link/5552544608aeaaff3befe87d/download Fecha de consulta 05/05/2021.

- Invisibilidad: la certeza de que los interlocutores no los pueden ver relaja a los usuarios y los lleva a realizar acciones que nunca harían en otra situación.
- Solipsismo: forma radical de subjetivismo según la cual solo existe aquello de lo que es consciente el propio yo. En este caso, los usuarios no conocen a los individuos que encuentran en la red y se forman una imagen de ellos basada en sus propios prejuicios y expectativas.
- Asincronismo: Internet es un medio que permite construir y enviar mensajes complejos sin que sea necesario esperar una respuesta inmediata.
- Imaginación disociativa: los usuarios de Internet se liberan de sus complejos y problemas desarrollando personalidades completamente diferentes a la real, creando un mundo paralelo.
- Minimización de la autoridad: este factor tiene un impacto significativo pues el usuario pierde las referencias del estatus y el poder, considerando que se encuentra en los mismos términos que sus interlocutores, aunque estos sean las Fuerzas y Cuerpos de Seguridad del Estado.

Otro elemento que debemos considerar es la manera en que actualmente se utilizan las redes sociales. Este medio es utilizando según diversas motivaciones, pero en los últimos tiempos ha ganado importancia la tendencia a intercambiar contenidos para obtener una mayor consideración social pues se supone que, cuanto más se lee o comparte un contenido, mayor es la notoriedad de quien lo publica. Esta búsqueda de la popularidad y por conseguir un mayor número de seguidores es un campo excelente para la difusión de noticias no contrastadas, o completamente falsas, todo vale para destacar entre los perfiles de una red.

Prácticas derivadas del ansia de popularidad es la compra de falsos seguidores y de interacciones simuladas[29] o el *like-farming*, que consiste en crear un perfil en una red social con contenidos llamativos —dentro de la legalidad— para recopilar el mayor número de interacciones con otros usuarios. El algoritmo aplicado por la red determina la popularidad en función del número de «me gusta» y los comentarios que recibe una publicación, y aquella noticia que alcance altas puntuaciones será promocionada y sugerida en los *feeds* de noticias de otros usuarios, incrementando la visibilidad del perfil original. Es una práctica habitual para mejorar la visibilidad de una empresa o la

[29] "Massive Instagram Click Farm Uncovered", *vpnMentor blog*, 9 de diciembre de 2020. Disponible en: https://www.vpnmentor.com/blog/report-instagram-scam/ Fecha de consulta 05/05/2021.

popularidad de una persona. Pero en caso de que la página haya sido creada por un potencial atacante, una vez alcanzado un nivel de popularidad suficientemente alto, se sustituye el contenido inicial por otro que puede incluir anuncios fraudulentos, enlaces a programas maliciosos o, simplemente, información falsa dentro de una campaña de desinformación[30].

Los métodos de ciberataque más extendidos actualmente se centran preferentemente en la utilización de las vulnerabilidades psicológicas para comprometer a los componentes de la capa humana de una red. En definitiva, las personas somos el vector de entrada más eficaz pues no existen parches de *software* para las vulnerabilidades y condicionamientos psicológicos.

Conclusiones

Hemos entrado en un periodo de la historia humana ligado al desarrollo y expansión de las tecnologías de la información, y una de las singularidades de esta época es que ha traído consigo un nuevo dominio para el desarrollo de las actividades, el ciberespacio. Debido a características como la sencillez, rentabilidad y dificultad de atribución, este nuevo ámbito se ha convertido en el preferido por los distintos agentes de la amenaza para llevar a cabo acciones de desinformación y decepción. Y a esta predilección debemos añadir que ciertas peculiaridades de los elementos constitutivos del ciberespacio, en especial las vulnerabilidades de los usuarios favorecen una mayor difusión de esas acciones de engaño y garantizan su éxito.

Pero no podemos culpar a la tecnología de las consecuencias que genera, estas dependen del uso que las personas hagamos de ella. Lo que ha hecho Internet y las plataformas digitales es proporcionarnos nuevas herramientas, de manera que ahora resulta más sencillo hacer pública una información y, a la vez, resulta más difícil mantenerla en el ámbito privado.

Según análisis realizados sobre la difusión de las noticias falsas, las estrategias de contención de la desinformación deben prestar especial atención a aquellos factores del comportamiento humano que la propician y no limitarse a aspectos técnicos como, por ejemplo, eliminar los sistemas automatizados que operan en las redes sociales. Por ello,

[30] ARNTZ, Pieter. “Explained: like-farming”, *Malwarebytes Labs blog*, 18 de abril de 2019. Disponible en: https://blog.malwarebytes.com/101/2019/04/explained-like-farming/ Fecha de consulta 05/05/2021.

comprender las sinergias originadas en la relación entre personas y tecnología tiene importantes consecuencias en el ámbito informativo, resultando fundamental en el desarrollo de estrategias que ayuden a anticipar y prevenir las amenazas cibernéticas emergentes.

Debemos resaltar la paradoja de que, aunque hoy día disponemos de una inaudita cantidad de canales de información, parte de la población conforma sus opiniones sobre los temas más complejos a partir de los mensajes recibidos a través de sus redes de conocidos, convirtiéndose la afinidad con el remitente en garantía de veracidad. Ante este y otros fenómenos que paralizan la reflexión, la principal defensa es la aplicación de algo tan sencillo como el sentido común. Nada mejor que utilizar nuestra capacidad de juicio y análisis, comparando la información y acudiendo a fuentes acreditadas, para comprobar la veracidad de las noticias de fiabilidad desconocida o incierta. Si no lo hacemos seremos presa fácil del engaño y de las acciones que se basan en él, como la desinformación y la decepción. Por ello, para finalizar, puede que resulte útil citar a un clásico como Baltasar Gracián que en su día nos recordaba que: «La confianza es madre del descuido».

*Francisco Marín Gutiérrez**
Teniente coronel del Ejército de Tierra
SHAPE, Strategic Employment Directorate