

30/2021

9 de marzo de 2021

*Raúl Sampedro Oliver**

**Redes sociales: desinformación,
adicción y seguridad**

Redes sociales: desinformación, adicción y seguridad

Resumen:

Las redes sociales han modificado nuestros patrones de obtención de información, de comunicación y de movilización colectiva. Los mecanismos psicológicos en los que se asientan estas plataformas facilitan su carácter adictivo, y su tendencia a generar polarización social. La comprensión de este fenómeno global implica la síntesis de enfoques desde la psicología y desde las tecnologías de la información y comunicación. El uso que se ha realizado en el pasado reciente de las redes sociales hace patente su potencial como herramienta en las campañas de desinformación. La concienciación social en el marco de la seguridad nacional, a través de iniciativas educativas, y la prevención, en base a la resiliencia extraída del análisis de las lecciones aprendidas, son las estrategias propuestas.

Palabras clave:

Redes sociales, seguridad del Estado, desinformación, extremismo, adicción.

***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.

Social Media: disinformation, addiction, and security

Abstract:

Social networks have modified how people collect information, communicate, and take part in mobilizations. The psychological mechanisms in which these platforms are based facilitate their addictive nature, and their tendency to generate social polarization. The understanding of this global phenomenon implies the synthesis of approaches from the psychology as well as from communication technologies. The way social networks have been used in the recent past show its potential as a tool in disinformation campaigns. The proposed strategies are based on social awareness, through educational initiatives within the framework of National Security, as well as prevention, based on the resilience extracted from the analysis of lessons learned.

Keywords:

Social Media, State security, disinformation, extremism, addiction.

Introducción

El desarrollo vertiginoso en los últimos años de nuevas tecnologías, la llamada *revolución digital*, ha favorecido la implantación a escala mundial de las redes sociales¹. Se trata de herramientas de software para el entretenimiento y la comunicación. No obstante, los efectos buscados y provocados en los usuarios de las redes sociales no se han limitado a estos fines; ni siquiera a favorecer el consumo de los productos promocionados por los anunciantes que contratan los servicios de estas plataformas. También han influido en el modo en que los ciudadanos se informan sobre la actualidad, desplazando a los medios de comunicación tradicionales, como la prensa y televisión. Actualmente, se tiende a valorar más la inmediatez y la transferencia de la noticia desde el punto de vista de los protagonistas que el análisis cualificado y la verificación de fuentes que se hace desde el ámbito periodístico: «Los profesionales de la información han visto suplantada su función social por el llamado *periodismo ciudadano*, es decir, por unos receptores que ejercen de periodistas, pero sin su formación ni su acervo ni sus códigos éticos»².

En el ámbito de la seguridad, merece una atención especial el impacto que las redes sociales han tenido en el desarrollo de movimientos sociales y de campañas electorales. En 2007, el ataque masivo de denegación de acceso contra los servidores informáticos del Gobierno de Estonia³ fue precedido por una campaña de protestas en redes sociales ante la retirada de la estatua del Soldado de Bronce en Tallin. En 2009 se relacionó a la red social Twitter con la revolución verde en Irán en junio de ese año⁴. En 2011, al fenómeno de las revueltas sociales en varios países árabes se las denominó *Primavera Árabe*, pero también como la «Revolución de las redes sociales»⁵. Desde 2014, las redes

¹ Definidas como un servicio de la sociedad de la información que ofrece a los usuarios una plataforma de comunicación a través de Internet para que estos generen un perfil con sus datos personales, facilitando la creación de comunidades con base en criterios comunes y permitiendo la comunicación de sus usuarios, de modo que puedan interactuar mediante mensajes, compartir información, imágenes o vídeos, permitiendo que estas publicaciones sean accesibles de forma inmediata por todos los usuarios del grupo. Disponible en: <https://dpej.rae.es/lema/red-social> [Consultado el 20/1/2021].

² BLANCO ALFONSO, Ignacio. «Reseñas bibliográficas. Verificación digital para periodistas. Manual contra bulos y desinformación Internacional», *Doxa.comunicación*, n.º 27, julio-diciembre 2018. Disponible en: https://www.doxacomunicacion.es/pdf/2_3.pdf [Consultado el 26/1/2021].

³ «Incidentes que afectan a la Seguridad de las TIC», *Centro Criptológico Nacional*, Perspectiva de la AA.PP., n.º 19, febrero de 2008. Disponible en: <https://www.ccn-cert.cni.es/comunicacion-eventos/articulos-y-reportajes/653-incidentes-que-afectan-a-la-seguridad-de-las-tic/file.html>

⁴ KAMINSKY, Ross. «Iran's Twitter Revolution». *Human Events*, June 18, 2009. Disponible en: <https://humanevents.com/2009/06/18/irans-twitter-revolution/> [Consultado el 20/1/2021].

⁵ CARLINI, Agnese. *Las redes sociales como factor de desestabilización*. Documento de Opinión IEEE 79/2018. Disponible en: http://www.ieeee.es/Galerias/fichero/docs_opinion/2018/DIEEE079-2018_RRSS_FactorDesestabilizacion_ACarlini.pdf [Consultado el 20/1/2021].

sociales han sido usadas como una capacidad militar más en el conflicto entre Ucrania y Rusia⁶, utilizándolas en campañas de amplio espectro, combinando ataques kinésicos, tecnológicos y cognitivos⁷.

Entre 2014 y finales de 2017, la guerra contra el Dáesh evidenció el poder de las narrativas y su difusión a través de redes en el seno de las sociedades occidentales⁸. En 2016, en el referéndum del *brexit*⁹ y en las elecciones presidenciales de Estados Unidos de América, la consultora Cambridge Analytica adquirió notoriedad internacional, tras las filtraciones que revelaron que había comprado a la red social Facebook los perfiles de más de 78 millones de usuarios, que los había usado para identificar aspectos de su personalidad, sus tendencias políticas, su predisposición a votar e incluso su colegio electoral, y que había personalizado anuncios de nuevo en Facebook para dichos usuarios, con objeto de motivarles para votar o, en su caso, no votar (según el interés del partido político contratante)¹⁰. En 2017, las redes sociales tuvieron un papel muy activo en la difusión de los correos electrónicos del aspirante al Eliseo, Emmanuel Macron, en su disputa electoral con Marine Le Pen¹¹. Ese mismo año Facebook estuvo en el punto de mira internacional por la difusión, a través de perfiles de usuarios en Myanmar, de una campaña de odio racial contra la minoría musulmana de los rohinyás¹², que desembocó en un genocidio. Durante los disturbios sociales de Cataluña a finales de 2018 hubo una gran campaña en redes sociales con repercusiones internacionales,

⁶ TREGUBOV, Victor. «Ukraine raised the alarm over weaponized social media long before Trump's twitter ban», *Atlantic Council*, January 14, 2021. Disponible en:

<https://www.atlanticcouncil.org/blogs/ukrainealert/ukraine-raised-the-alarm-over-weaponized-social-media-long-before-trumps-twitter-ban/> [Consultado el 26/1/2021].

⁷ JAITNER, Margarita. «Russian Information Warfare: Lessons from Ukraine». En: GEERS, Kenneth (ed.). *Cyber War in Perspective: Russian Aggression Against Ukraine*, Tallinn: NATO CCD COE Publications 2015. Disponible en:

https://www.researchgate.net/publication/291086368_Russian_Information_Warfare_Lessons_from_Ukraine [Consultado el 13/02/2021].

⁸ BARRANCOS LARRÁYOZ, David. *Los Community Managers del terror: la propaganda online de ISIS y su ofensiva sobre Irak*. Documento de Opinión IEEE 82bis/2014. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2014/DIEEO82bis-2014_ISS_DavidBarrancos.pdf [Consultado el el 14/1/2021].

⁹ *Brexit* es un acrónimo de dos palabras en inglés: *Britain* (Gran Bretaña) y *exit* (salida), y hace referencia al proceso de salida de Reino Unido de la Unión Europea. Disponible en: <https://www.lamoncloa.gob.es/brexit/acercadelbrexit2/Paginas/index.aspx> [Consultado el 14/1/2021].

¹⁰ PEIRANO, Marta. *El enemigo conoce el sistema: manipulación de ideas, personas e influencias después de la economía de la atención*. Barcelona: Debate 2019.

¹¹ MOHAN, Megha. «Macron Leaks: the anatomy of a hack», *BBC Trending*, 9 May 2017. Disponible en: <https://www.bbc.com/news/blogs-trending-39845105> [Consultado el 23/1/2021].

¹² MOZUR, Paul. «A Genocide Incited on Facebook, With Posts From Myanmar's Military», *The New York Times*, oct. 15, 2018. Disponible en: <https://www.nytimes.com/2018/10/15/technology/myanmar-facebook-genocide.html> [Consultado el 14/1/2021].

en la que una parte de la información fue intencionalmente distorsionada¹³. En 2020, las redes sociales tuvieron un papel importante en las campañas de desinformación relativas a la pandemia de la COVID-19¹⁴. El ataque al Capitolio de Washington, el 6 de enero de 2021, ha evidenciado el efecto que las redes sociales ejercen en la movilización política. El controvertido bloqueo de las cuentas en redes sociales del todavía presidente Donald Trump por parte de los gestores de estas¹⁵, con objeto de evitar la movilización social antes de la proclamación del presidente electo Biden, ha supuesto un hito en el papel de las redes sociales en el ámbito político¹⁶. La última movilización social a través de las redes ha tenido como protagonista el ataque a los fondos de inversión bajistas que operan en Wall Street. La plataforma utilizada fue Reddit¹⁷, un agregador de noticias sociales. En enero de 2021 consiguieron más de dos millones de suscriptores nuevos, en base a una estrategia coordinada de inversión particular pero masiva en valores bursátiles de bajo valor hasta el momento de su intervención: tal fue el caso de las acciones de GameStop, o la cotización de la criptomoneda Dogecoin¹⁸.

Modalidades y patrones de uso de las redes sociales

Según las estadísticas facilitadas por la web Data Reportal¹⁹, con datos acumulados hasta el mes de julio de 2020, más de la mitad de la población mundial usa redes sociales: 3960 millones de personas. Se ha producido un incremento del 10 % de usuarios desde julio de 2019. La mayoría de los usuarios se conecta a través de

¹³ ANDERSON, Paul. «'Independence 2.0': Digital activism, social media and the Catalan independence movement», *Catalan Journal of Communication & Cultural Studies*, Volume 11, Number 2, 1 October 2019, pp. 191-207(17). Disponible en: https://doi.org/10.1386/cjcs_00003_1 [Consultado el 23/1/2021].

¹⁴ PORTERO ALFÉREZ, Nuria. *Las redes sociales y la COVID-19: herramientas para la infodemia*. Documento de Opinión IEEE 163/2020. Disponible en: http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEO163_2020NURPOR_infodemia_Covid.pdf [Consultado el 23/1/2021].

¹⁵ CLAYTON, James, KELION, Leo; MOLLOY, David. «Asalto al Capitolio: Facebook e Instagram bloquean a Donald Trump al menos hasta que se complete el traspaso de poder», *BBC news*, 7 de enero de 2021. Disponible en: <https://www.bbc.com/mundo/noticias-internacional-55575310> [Consultado el 2/2/2021].

¹⁶ «Rusia compara el bloqueo de las cuentas de Trump en redes sociales con 'una explosión nuclear' en el ciberespacio», *Europa Press*, 14 de enero de 2021. Disponible en: <https://www.europapress.es/internacional/noticia-rusia-compara-bloqueo-cuentas-trump-redes-sociales-explosion-nuclear-ciberespacio-20210114151007.html> [Consultado el 2/2/2021].

¹⁷ Disponible en: <https://www.reddit.com/r/wallstreetbets/> [Consultado el 10/2/2021].

¹⁸ GANDEL, Stephen. «How Reddit posters made millions as Wall Street lost billions on GameStop's wild stock ride», *CBSNEWS*, 29/1/2021. Disponible en: <https://www.cbsnews.com/news/gamestop-reddit-wallstreetbets-short-squeeze-2021-01-28/> [Consultado el 10/2/2021].

¹⁹ Disponible en: <https://datareportal.com/reports/more-than-half-the-world-now-uses-social-media?rq=social%20media> [Consultado el 10/1/2021].

dispositivos de telefonía móvil. Las regiones mundiales con menor porcentaje de acceso a las redes sociales son África central, con un 12 %; seguida de África oriental y occidental, con un 14 % y un 23 %, respectivamente; y Asia central, con un 31 %. En España, el acceso a Internet cuenta con una penetración del 91 % de la población, y una tasa de uso de redes sociales del 61 %.

Los usuarios pasan como media 2 horas y 10 minutos consultando las redes sociales. En el grupo de menor edad, de 16 a 24 años, el tiempo invertido es de 2 horas y 53 minutos, y las mujeres pasan como media conectadas unos 35 minutos más que los hombres.

Facebook ha marcado un antes y un después en cuanto al impacto de las redes sociales, y también en cuanto a su papel protagonista en múltiples movilizaciones sociales²⁰. Es la red social de más éxito e implantación a nivel mundial, con 2600 millones de usuarios; es decir, más que los habitantes de cualquier país del mundo. Factor clave para este desarrollo fue la iniciativa de Mark Zuckerberg de extender el acceso a la red a países de África, Asia y América Latina con una fórmula aparentemente altruista: Internet.org en 2013 y su evolución en Free Basics a partir de septiembre de 2015²¹. Esta fórmula ha dejado de aplicarse en algunos países, después del mencionado escándalo del uso de cuentas de Facebook contra la minoría musulmana de los rohinyás en Myanmar, en 2017.

Bases psicológicas de la adicción a las redes sociales

Peirano²² advierte sobre los poderosos mecanismos psicológicos que sostienen los patrones de comportamiento de los usuarios habituales de las redes sociales. El modelo de negocio de las redes sociales se basa en la venta de nuestros datos a terceros: nosotros somos el producto. Cuanto más nos enganchen los contenidos que nos ofrecen,

²⁰ LA ROSA, Amaro. «Movimientos sociales, redes sociales y recursos simbólicos», *Correspondencia & Análisis*, n.º 6, 2016.

²¹ Se trata de una asociación entre Facebook y proveedores de servicio de Internet móvil. Aunque se anuncia como un Internet gratis, en realidad solo da acceso a Facebook y a otras aplicaciones concertadas, como Bing, el buscador de Microsoft. Incluso en estas plataformas el acceso no es ilimitado: solo permite leer los titulares de vídeos y noticias, pero no da acceso al contenido de estas (ello conlleva el consumo de datos).

²² PEIRANO, Marta, *op. cit.*

mejor para sus intereses. En esta línea, Gómez de Agreda²³ apunta: «Facebook no es la plaza pública en la que nos sentábamos a charlar de nuestras cosas, es más bien un club privado en el que algunos pagan para que nos sentemos a compartir con ellos nuestros datos».

Somos consumistas por naturaleza, posiblemente porque en nuestra evolución como especie era una garantía de éxito frente a periodos de escasez. A nivel fisiológico, estos comportamientos tienen su reflejo en nuestra corteza cerebral: es el mecanismo de recompensa basado en el neurotransmisor dopamina²⁴. La dopamina se libera cuando realizamos actividades placenteras: practicar sexo, comer algo delicioso, tomar drogas estimulantes o comprar. Si los niveles de dopamina están bajos, nos encontramos incómodos, nerviosos. Podemos mitigar esta sensación desagradable si retomamos los comportamientos que liberan de nuevo dopamina.

Fogg²⁵ teorizó en 2009 sobre un modelo de comportamiento al que dio su nombre. Describe tres condiciones necesarias para que un comportamiento se manifieste: la motivación, la habilidad y la oportunidad. La persona, antes de actuar, tiene que querer hacer algo, tiene que saber hacerlo, y tiene que sentir que es el momento adecuado para ello (que haya un desencadenante o señal). Si utilizamos las señales idóneas, como los sonidos y las luces en las máquinas tragaperras, la persona se verá impulsada a realizar repetidamente esa conducta que conoce y que en el pasado le ha reportado sensaciones placenteras, como ganar un premio. Estas señales son las que activan también las redes sociales, con estímulos como recibir *likes*²⁶ o recomendaciones de nuestros amigos. Un *like* o un emoticono pueden generar una potente descarga de dopamina en nuestro cerebro²⁷. Una vez iniciada la conducta, si los estímulos señal se presentan con frecuencia, se acaba convirtiendo en un hábito o en una adicción. Y no hay estímulos

²³ GÓMEZ DE AGREDA, Ángel. *Mundo Orwell. Manual de supervivencia para un mundo hiperconectado*. Barcelona: Ariel 2019, p. 117.

²⁴ Adjunto se incluye una web con amplia información sobre la dopamina, los mecanismos de recompensa y las adicciones. Disponible en: <https://neuro-class.com/sistema-de-recompensa-cerebralcomo-funcionan-las-adicciones/> [Consultado el 11/1/2021].

²⁵ Fogg fue uno de los gurús de manipulación del comportamiento de Silicon Valley. Sus cursos basados en la aplicación de la persuasión en la programación de aplicaciones en Facebook hizo a más de un alumno suyo millonario. Fuente: FOGG, B. J., *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann Publishers, 2003.

²⁶ Facebook o Instagram no dan la posibilidad de *don't likes*. Así se potencia el efecto reforzante de publicar en estas plataformas.

²⁷ Véase esta interesante publicación sobre el efecto de los móviles en los jóvenes y las dificultades asociadas a su capacidad de mantener la atención: ANGUIANO LUNA, H.; CISNEROS, J. L.; MARÍN ORNELAS, A. R. «Las redes sociales, telefonía celular y el efecto phubbing». *Veredas. Revista del Pensamiento Sociológico*, n.º 35 «Sociología y comunicación», 2018.

señal más efectivos que las notificaciones, o tecnología *push*, empleadas en cada una de las aplicaciones de nuestros dispositivos digitales, y que vienen activadas por defecto. Los *likes* y el chequeo regular de nuestras notificaciones se basan en una motivación humana tan relevante como la de sentirse aceptado o reconocido por el grupo, o en su reverso, el miedo a sentirse rechazado²⁸.

Un estudio²⁹ con más de 80 000 voluntarios sobre la capacidad predictiva de Facebook mostraba que el algoritmo de la plataforma, teniendo en cuenta los *likes* que los participantes habían dado a contenidos de Facebook en el pasado, era capaz de predecir con más acierto que las personas allegadas los comportamientos futuros de los usuarios. La precisión predictiva del algoritmo superaba con 10 *likes* analizados sobre un tema en particular (por ejemplo, publicaciones del usuario sobre política) a las estimaciones de los compañeros de trabajo relativas a posibles comportamientos de los sujetos del estudio en esa área (por ejemplo, sobre si acudiría a un mitin político), con 70 *likes* a los amigos, con 150 a los familiares y ¡con 300 a los cónyuges!

Otro elemento de impacto en la efectividad de las redes para la movilización social son los denominados *memes*. Se identifican con el concepto formulado por Richard Dawkins³⁰, que consideraba que el mandato biológico de reproducción y transmisión de la carga genética, que los humanos compartimos con el resto de los animales, lo habíamos ampliado a la transmisión de ideas, historias o cultura entre generaciones. La revolución digital ha personificado estos «memes» en imágenes o vídeos de muy corta duración, que bien por su contenido humorístico, o bien por su enganche emocional, son reenviados de modo masivo entre los usuarios que comparten una o varias redes sociales. No hay nada más efectivo para deteriorar la imagen pública de una autoridad o una institución, o bien para conseguir la identificación con una causa³¹, que un meme ampliamente virilizado.

²⁸ El concepto de *fear of missing out* (FOMO) refleja el hábito de consultar las redes sociales varias veces al día, para no dejar de responder un mensaje, corresponder a un *like* o dejar de estar al tanto de la actualidad.

²⁹ YOUYOU, Wu; KOSINSKI, Michal; STILLWELL, David. «Computer-based personality judgments are more accurate than those made by humans», *PNAS*, vol. 112, January 27, 2015. Disponible en: <https://doi.org/10.1073/PNAS.1418680112> [Consultado el 23/1/2021].

³⁰ DAWKINS, Richard. *El gen egoísta: las bases biológicas de nuestra conducta*. Barcelona: Salvat Ciencia 1990.

³¹ MARTÍNEZ PONTIJAS, Juan. *#Boogaloo, un meme para el conflicto armado*. Documento de Opinión IEEE 100/2020. Disponible en: http://www.ieeee.es/Galerias/fichero/docs_opinion/2020/DIEEEO100_2020JUAMAR_boogaloo.pdf [Consultado el 14/1/2021]

El reverso del uso de las redes para la movilización social deviene en los mecanismos de control colectivo. El caso paradigmático es el sistema chino de «crédito social³²». Se basa en un sistema de puntuación que identifica el nivel de cumplimiento del ciudadano con la ley y con las normas comunitarias. Hasta la fecha, no se ha implantado *de facto* en el nivel estatal, al estilo del Gran Hermano de Orwell; más bien se trata de sistemas locales. Por ejemplo, la ciudad de Rongcheng³³, en el noreste de China, da 1000 puntos iniciales a sus ciudadanos. Infracciones comunitarias como una multa de tráfico, resta puntos; acciones de apoyo a la comunidad, como donaciones, suma puntos. Estos puntos se pueden combinar con los sistemas de puntos de empresas privadas, como Ant Financial's Zhina Credit, conocida popularmente como «Sesamo Credit». Su sistema de puntos es voluntario, pero la particularidad de sus algoritmos es que no solo puntúa en función del historial de créditos solicitados y devengados a la financiera, sino también en función del comportamiento de los clientes. Así, por ejemplo, gastar dinero en juegos *online* de apuestas o similares reduciría la puntuación en Sesamo Credit. La puntuación de esta plataforma ha sido utilizada en algunos hoteles para aceptar reservas sin depósito o para prestar paraguas. El hecho de que el sistema no incluya mecanismos de queja o corrección de los puntos, las posibles consecuencias que este tendría a nivel económico y social para estigmatizar a una persona y la espiral de caída de puntos en la que podrían caer muchos ciudadanos, la convertiría en una herramienta propia de una ficción distópica³⁴. Y no se trata de especulaciones: en 2014, el Gobierno chino publicó un plan para la puesta en marcha de este sistema con la fecha de término de 2020, con el propósito de incrementar los niveles de confianza en la sociedad china. A fecha de hoy no se ha implementado a nivel nacional, pero sí en grandes ciudades como Pekín, Shanghái, Guangzhou, Shenzhen, Hangzhou, Nanjing o Suzhóu.

Polarización y procesos de influencia

En contra de lo que se suele pensar en la cultura popular, el objetivo de las campañas de influencia más exitosas no ha sido el cambiar lo que la gente pensaba, sino más

³² BACH, Jonathan. «The red and the black: China's social credit experiment as a total test environment», *The British Journal of Sociology*, Volume 71, Issue 3, 2020, p. 489-502.

³³ Disponible en: <https://www.wired.co.uk/article/china-social-credit-system-explained> [Consultado el 14/1/2021].

³⁴ Es el caso de Nosedive, el primer episodio de la tercera temporada de *Black Mirror* en la plataforma Netflix, que muestra una sociedad obsesionada con calificar a las personas.

confirmar lo que la gente ya creía³⁵. Una vez que las audiencias objetivo han visto validadas sus creencias, valores y actitudes en torno a la narrativa buscada, el paso para la movilización social está muy cerca.

La mayoría de las redes sociales incorporan las *news feed*³⁶ que implementó Facebook en 2006. Son noticias relacionadas con los gustos y las publicaciones en que ha mostrado interés anteriormente el usuario. Este cree que las noticias que lee en sus redes sociales son las mismas que puede leer cualquier otro usuario, y eso no es así. Están personalizadas en función de sus búsquedas previas, del tiempo que ha dedicado a cada noticia y de las interacciones al respecto con sus contactos. Estos contenidos pueden ser contratados por los partidos políticos en las campañas electorales. De este modo consiguen acceso directo a los votantes, según el perfil de tendencias políticas identificado por la plataforma u otras empresas de gestión de datos en la red³⁷.

Los contenidos más extremos son los que llaman más la atención de las personas que comparten puntos de vistas similares, así que le dan al *like* o lo reenvían a sus amigos, formando las llamadas *echo chambers*³⁸. Pero eso es lo que hacen también los que opinan lo contrario: comentan la noticia, burlándose o contraargumentando, pero, en todo caso, contribuyendo a que se difunda. De este modo, el algoritmo de la red social tenderá a presentar ese contenido más frecuentemente en los *news feed*, al considerarlo como tendencia en el momento. Además, a diferencia de un periódico, una red social no puede ser demandada porque haya divulgado una noticia falsa.

Internet ha cambiado las reglas de juego. La capacidad de control que los Gobiernos democráticos —no digamos los autoritarios— pudieran tener sobre los medios de comunicación se ha difuminado. Cuando alguien inicia una campaña de influencia en las redes, el coste es tan reducido y las consecuencias de los errores son tan pequeñas que el potencial de la herramienta es enorme. En ocasiones, el objetivo ni siquiera es

³⁵ TORRES SORIANO, M. R. «La tormenta perfecta». En: TORRES, M. R. (coord.). # *Desinformación. Poder y manipulación en la era digital*. Granada: Comares 2019.

³⁶ Se trata de una presentación continua, y aparentemente sin fin, de noticias intercaladas con actualizaciones, fotos y comentarios de amigos de Facebook, junto con anuncios.

³⁷ Tal y como ocurrió con Cambridge Analytica en las campañas del *brexít* y las elecciones norteamericanas de 2016.

³⁸ Una *echo chamber* se puede definir como un entorno donde una persona solo encuentra información u opiniones que reflejan o refuerzan las propias. Suelen generar desinformación y distorsionar la perspectiva de los implicados, al dificultar su capacidad de considerar puntos de vista contrapuestos o de diferenciar los matices de un problema complejo. Se alimenta en base al sesgo de confirmación, que es la tendencia a dar preminencia a la información externa que confirma nuestras creencias previas. Disponible en: <https://edu.gcfglobal.org/en/digital-media-literacy/what-is-an-echo-chamber/1/> [Consultado el 7/1/2021].

conseguir cambios en el comportamiento de audiencias: con generar ruido o crispación en el debate público consiguen cumplir con su agenda de desinformación.

Un ejemplo paradigmático de la utilización de las redes sociales en los procesos de influencia fue la denominada injerencia rusa en las elecciones presidenciales estadounidenses en noviembre de 2016. La hipotética estrategia de actores provenientes de las inmediaciones de Rusia para debilitar a los países occidentales, alentando las posiciones polarizadas, sean de derechas o izquierdas, supremacistas blancos o del Black Lives Matter, adquiere en este caso tintes de éxito rotundo. Uno de los documentos más significativos en este sentido fue la investigación realizada por la Fiscalía General de los Estados Unidos, denominada *Informe Mueller*³⁹: «The Russian government interfered in the 2016 presidential election in sweeping and systematic fashion».

El elemento más activo en la campaña de desinformación, en 2016, fue achacado a la granja de *bots* situada en el número 55 de la calle Savushkina, en San Petersburgo, conocida como Internet Research Agency. Su metodología, según Vallés⁴⁰, consiste en el siguiente protocolo: observar las situaciones internas en los países occidentales, detectar qué problemas políticos y sociales tienen y alimentarlos mediante medidas activas de desinformación. No buscan crear nuevos problemas, sino amplificar los ya existentes.

Como respuesta institucional a la amenaza desestabilizadora de las campañas de desinformación, la Comisión Europea decidió crear, en 2016, un Grupo de Expertos de Alto Nivel⁴¹. Entre las medidas propuestas, destacaba la promoción de las agencias de verificación de noticias independientes.

Las fuerzas armadas y el reto de la gestión de la desinformación en las redes sociales

La preocupación por los vertiginosos cambios sociales, culturales y políticos de la sociedad motivó en 2017 que el entonces jefe del Estado Mayor de la Defensa (JEMAD),

³⁹ US Department of Justice. *Informe Mueller*, 2019, p. 38.

⁴⁰ VALLÉS, Vicente. «La injerencia rusa. Putin contra Occidente». En: TORRES, M. R., *op. cit.*, pp. 23-24.

⁴¹ ROJAS CAJA, Fernando. *El fact checking. Las agencias de verificación de noticias en España*. Documento de Opinión IEEE 89/2020. Disponible en:

http://www.ieee.es/Galerias/fichero/docs_opinion/2020/DIEEEE089_2020FERROJ_agencias.pdf

[Consultado el 10/2/2021].

general de Ejército D. Fernando Alejandro Martínez, pusiera en marcha un Programa de Futuros en el Centro Superior de Estudios de la Defensa Nacional. A finales de 2018, el proyecto culminó en la publicación de sendos manuales. Por un lado, el documento *Panorama de Tendencias Geopolíticas. Horizonte 2040*, dirigido por el Instituto de Estudios Estratégicos (IEEE); y, por otro lado, el documento *Entorno Operativo 2035*, dirigido por el Centro Conjunto de Desarrollo de Conceptos (CCDC).

El *Entorno Operativo 2035* establece el contexto operativo de la defensa, disuasión, vigilancia, prevención y respuesta, como el ámbito más adecuado para la actuación de las Fuerzas Armadas frente a la amenaza de potenciales campañas de desinformación. No obstante, se deja abierta la vía de colaboración con otras Administraciones públicas para hacer frente a ciberataques que afecten a la seguridad nacional.

Los retos identificados por el *Panorama de Tendencias Geopolíticas. Horizonte 2040* son múltiples. En relación con el factor físico, se hace referencia al ciberespacio con tres vectores de desarrollo futuro: la computación en la nube, el *big data* y el Internet de las cosas. Tal y como indica el coronel Calvo⁴², a la amenaza del ciberespacio hay que aunar el nuevo espacio de la gestión de la información, que incluye: la información pública, la propaganda, la acción psicológica y la influencia sobre la toma de decisiones de líderes políticos y militares. La sociedad española debe prepararse para este reto, en base a la educación en la materia y la generación de resiliencia⁴³, como las armas más prometedoras contra la desinformación. La receta de Peirano⁴⁴ para hacerle frente es: un análisis detallado, una vez identificada la campaña; detección de los resortes emocionales y narrativos en los que la campaña se centra; sustitución de la desinformación con información veraz y satisfactoria, reconociendo los errores cometidos (la credibilidad es clave); y búsqueda del apoyo de expertos que aporten información objetiva, veraz y, a ser posible, con base científica.

El factor humano del *Horizonte 2040* incide en los retos sociales de los próximos años: cambios demográficos y fenómenos migratorios, aumento de la religiosidad y educación

⁴² CALVO ALBERO, José Luis. «Conflicto, información e influencia». En: *Implicaciones del ámbito cognitivo en las Operaciones Militares*. Instituto Español de Estudios Estratégicos. Documento de Trabajo 01/2020.

⁴³ La definición de *resiliencia* de la RAE combina el significado que se le da al término desde el punto de vista psicológico. Es la capacidad de adaptación de un ser vivo frente a un agente perturbador o un estado o situación adversos. Pero, al igual que los materiales, se busca que el individuo haya recuperado su estado inicial cuando haya cesado la perturbación a la que había estado sometido. O, más bien, que haya crecido como persona u organización en base a la superación de la experiencia estresante.

⁴⁴ PEIRANO, Marta. «Medios de comunicación». En: *Implicaciones del ámbito... op. cit.*

e igualdad de género en auge. Estos cambios son un caldo de cultivo perfecto para aquellos agentes que quieran aumentar la conflictividad social a través de campañas de desinformación. Donoso⁴⁵ advierte sobre el incremento de la probabilidad y potencial daño de estas campañas, fundamentado en: la sobreinformación (multitud de fuentes a las que se recurre de forma reiterada), la sobredifusión (rapidez de la transmisión de la información), la sobreconexión (en base a los dispositivos móviles) y la sobremovilización social (a través de las redes sociales).

El factor económico y sociopolítico del *Horizonte 2040* plantea el conflicto inherente al proceso de globalización mundial. La tecnología está más cerca de todos y en todo el mundo, aparentemente, se vive en la «aldea global», pero las tensiones de la regionalización y la exacerbación nacionalistas surgen como fuerzas antagónicas. La democracia es cuestionada por los ciudadanos que la disfrutaban, y surgen mecanismos para escapar al control del Estado, como la *dark web*⁴⁶ o las criptomonedas⁴⁷, porque los ciudadanos dudan de las intenciones de sus gobernantes.

El factor militar, que cierra el análisis del *Horizonte 2040*, plantea el conflicto en la «zona gris»⁴⁸, con la ciberguerra y la guerra híbrida como modalidades presentes y futuras más probables. Las campañas de desinformación son el ingrediente adicional para provocar la tormenta perfecta.

El Gobierno del Reino de España promulgó a finales de este año pasado la Orden PCM/1030/2020, de 30 de octubre, por la que se publica el procedimiento de actuación contra la desinformación aprobado por el Consejo de Seguridad Nacional. Su objetivo consiste en garantizar el acceso a la información veraz para todos los ciudadanos. Para ello, se constituye una comisión permanente contra la desinformación, con la participación de autoridades públicas, el sector privado y la sociedad civil, que velarán,

⁴⁵ DONOSO RODRÍGUEZ, Daniel. «Aspectos psicológicos en el ámbito de las operaciones militares», En: Implicaciones del..., *op. cit.*

⁴⁶ La *dark web* es una parte de la *deep web* (el Internet que no está indexado y no aparece en los buscadores), pero en este caso intencionalmente oculta a los motores de búsqueda, con direcciones IP enmascaradas y accesibles solo con un navegador web especial. Si la *deep web* es el 90 % de Internet, la *dark web* ocuparía únicamente el 0,1 % de ella.

⁴⁷ Criptomoneda es un medio digital de intercambio que utiliza criptografía fuerte para asegurar las transacciones, controlar la creación de unidades adicionales y verificar la transferencia de activos usando tecnologías de registro distribuido.

⁴⁸ «Zona gris» se refiere a un estado de tensión y hostilidad entre las partes en conflicto, con acciones de provocación y agresión mutua, pero al mismo tiempo tratando de evitar un *casus belli* que lleve al conflicto armado abierto.

a través de cuatro niveles de activación, por la identificación y desactivación de las campañas de información que atenten contra nuestra seguridad nacional.

La lucha contra la desinformación es una responsabilidad política en el marco de la Ley 36/2015, de 28 de septiembre, de Seguridad Nacional. Las Fuerzas Armadas actuarán cuando se determine y siempre bajo estricto control político. La actuación eficaz de las Fuerzas Armadas requiere fortalecer los mecanismos de comunicación estratégica. La coordinación de las operaciones de información y las operaciones en el ciberespacio es clave para fortalecer las capacidades de las Fuerzas Armadas. La *Estrategia Nacional de Ciberseguridad de 2019*⁴⁹ enfatiza el papel que la conectividad digital tiene en los movimientos sociales globales. Los principios rectores en los que se inspira son: la unidad de acción, la anticipación, la eficiencia y la resiliencia.

La doctrina para el empleo de las Fuerzas Armadas, PDC-01 (A)⁵⁰, a los tradicionales espacios físicos para las operaciones (terrestre, marítimo y aeroespacial) ha sumado dos espacios no físicos: el ciberespacial y el cognitivo. El novedoso ámbito cognitivo se ha definido en el apartado 308 como: «Un ámbito intangible inherente al ser humano, considerado de forma individual, socializada u organizada... consustancial a su capacidad de juicio y de toma de decisiones. Este ámbito alcanza a las voluntades de todas las personas afectadas por el conflicto y a los sistemas de inteligencia artificial, por lo que impregna al resto de ámbitos. Su principal limitación es que para operar en él se manejan aspectos intangibles y de difícil evaluación, como los valores, las percepciones, la conciencia, las actitudes y los prejuicios».

Las disciplinas que se identifican como adecuadas para que las Fuerzas Armadas puedan alcanzar sus objetivos en este ámbito son: las tecnologías de la comunicación, la ciencia psicológica y otras ciencias sociales.

Conclusiones

La influencia y la manipulación, como elementos inherentes al ser humano y su necesidad de vivir en sociedad, han existido siempre. El reto en la actualidad reside en

⁴⁹ Disponible en: <https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019> [Consultado el 23/01/2021].

⁵⁰ Disponible en: <https://publicaciones.defensa.gob.es/pdc-01-a-doctrina-para-el-empleo-de-las-fas-libros-papel.html> [Consultado el 11/02/2021].

el alcance global y su potencial desestabilizador, producto de las potencialidades que la revolución digital ha generado.

La desinformación apela a lo emocional. La acción de los Gobiernos frente a estas campañas debe apelar también a las emociones, actitudes y valores. Pero, especialmente, al sentimiento de identificación y pertenencia de los ciudadanos con sus sistemas democráticos. Una estrategia de éxito frente a la desinformación no puede ser reactiva. La educación de la sociedad, y la potenciación de su capacidad resiliente, son herramientas clave. Consideramos a este respecto que las lecciones aprendidas de una campaña de desinformación deben ser conocidas y debatidas en el ámbito público. Detectar e informar sobre las emociones y los sesgos con los que se ha pretendido distorsionar la información, las motivaciones que hay detrás de las campañas, es vital para su prevención.

La revolución digital ha convertido a nuestra psique en el eslabón débil de una cadena de efectos, cuya magnitud alcanza la difusión internacional. La proactividad para salvaguardar las sociedades democráticas debe aunar un profundo conocimiento de la psicología y la tecnología, a partes iguales.

Las Fuerzas Armadas cuentan con la capacidad tecnológica de acción en el ciberespacio, a través del Mando Conjunto del Ciberespacio (MCCE). La capacidad de intervención psicológica en el ámbito cognitivo queda respaldada por la Sección de Influencia del Mando de Operaciones, por el Centro de Inteligencia de las Fuerzas Armadas, pero también por el colectivo de 200 psicólogos militares del que dispone Defensa. El potencial de la psicología militar, como fuente de analistas y en el desarrollo de proyectos de protección de los intereses del Estado en el ámbito cognitivo, es amplio. Los retos, riesgos y amenazas que nos depara el futuro próximo harán cada vez más acuciante el aprovechamiento de todos los recursos humanos disponibles para hacerles frente.

*Raúl Sampedro Oliver**

Teniente coronel psicólogo, DEM
Sección de Acción Tutorial de la ESFAS