



Cuadernos de Estrategia 197

La posverdad. Seguridad y defensa

Instituto
Español
de Estudios
Estratégicos

ieeee.es
Instituto Español de Estudios Estratégicos



MINISTERIO DE DEFENSA



Cuadernos de Estrategia 197

La posverdad. Seguridad y defensa

Instituto
Español
de Estudios
Estratégicos

ieeee.es
Instituto Español de Estudios Estratégicos



MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
<http://publicacionesoficiales.boe.es/>

Edita:



<https://publicaciones.defensa.gob.es/>

© Autores y editor, 2018

NIPO: 083-18-128-4 (edición papel)

ISBN: 978-84-9091-368-0 (edición papel)

Depósito legal: M-16386-2018

Fecha de edición: junio 2018

Maqueta e imprime: Ministerio de Defensa

NIPO: 083-18-129-X (edición libro-e)

Las opiniones emitidas en esta publicación son exclusiva responsabilidad de los autores de la misma. Los derechos de explotación de esta obra están amparados por la Ley de Propiedad Intelectual. Ninguna de las partes de la misma puede ser reproducida, almacenada ni transmitida en ninguna forma ni por medio alguno, electrónico, mecánico o de grabación, incluido fotocopias, o por cualquier otra forma, sin permiso previo, expreso y por escrito de los titulares del © Copyright.

En esta edición se ha utilizado papel 100 % libre de cloro procedente de bosques gestionados de forma sostenible.

ÍNDICE

	Página
Introducción.....	9
<i>Leandro Esteban Villamor</i>	
Capítulo primero	
El mundo de la posverdad	21
<i>Federico Aznar Fernández-Montesinos</i>	
Una época de confusión. Los pos- y los -ismos	23
Los medios y la opinión pública	27
Tecnología y sociedad	41
Verdad, emoción y razón	46
La posverdad	49
Las fake news o noticias falsas	55
La pospolítica	59
La guerra híbrida y la posverdad	64
Superar la posverdad	69
Conclusiones	75
Bibliografía	77
<i>Publicaciones</i>	77
<i>Recursos electrónicos y artículos</i>	79
Capítulo segundo	
Políticas de seguridad y defensa en la era de la posverdad	83
<i>Alfonso Merlos</i>	
Introducción: un futuro de incertidumbre y fragilidad	85
Repensando el concepto de interés nacional	86
Hacia una transición en los modelos de seguridad	89
Nuevos horizontes de la cultura de defensa	92
La Inteligencia: ayer, hoy y mañana	93
El arma de doble filo de las TIC	96

	Página
La metamorfosis en los procesos de comunicación	97
Un escenario de audiencias volátiles y empoderadas	99
Injerencias imprevistas en procesos electorales	100
Realidades y mitos de las operaciones rusas	102
Conclusiones: cómo detener a atacantes invisibles	104
 Capítulo tercero	
Redes sociales y posverdad en el devenir de los Estados.....	107
<i>Eva Moya</i>	
Pero... ¿cómo hemos llegado hasta aquí?.....	109
Globalización, democracia y lobby	110
Del usuario pasivo al «ciudadano interactivo»	111
La pequeña revolución de la movilidad y la evolución de los dispositivos móviles	119
Computación en nube, big data e inteligencia artificial	120
Política, relaciones internacionales y economía a golpe de tuit	123
Propaganda política y posverdad «transparente»	123
Propaganda política y posverdad «enmascarada».....	133
Las redes sociales y la manipulación de la economía	141
El impacto de la posverdad en las redes sociales y en las emergencias:	
seguridad y defensa	144
Catástrofes naturales	144
Crimen, cibercrimen y mercenarios en redes sociales	146
Terrorismo: el Dáesh en las redes sociales y contrapropaganda.....	148
Las Fuerzas Armadas como objetivo	155
Tácticas utilizadas para combatir la propaganda y la manipulación a través de la posverdad.....	157
 Capítulo cuarto	
La disrupción digital en el contexto de las guerras híbridas	159
<i>Javier Lesaca Esquiroz</i>	
La revolución tecnológica y sus implicaciones en la gobernanza	161
La disrupción comunicativa como arma en el contexto de las guerras híbridas	168
Las guerras híbridas de agentes nacionales	175
Las guerras híbridas de agentes no nacionales	182
La metodología de la disrupción comunicativa	183
La disrupción comunicativa del Dáesh	186
La narrativa disruptiva del Dáesh	187
Estrategia de medios y plataformas de difusión propias	192
Distribución automatizada de las campañas	194
Conclusión	195
 Capítulo quinto	
El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato	197
<i>Manuel R. Torres Soriano</i>	
Introducción	199

	Página
Una breve historia del hacktivismo	201
Entre lo individual y lo colectivo	202
La eclosión del hacktivismo antisistema: Anonymous.....	206
Bajo la estela de Anonymous.....	213
Hacktivismo yihadista	216
Conclusiones.....	223
Composición del grupo de trabajo.....	225
Cuadernos de Estrategia	227

Introducción

Leandro Esteban Villamor

Decir que la *posverdad* y las *fake news* o noticias falsas son gran parte de la esencia de la comunicación y de las relaciones sociales de nuestros días quizá sea una de las pocas verdades absolutas que nos queden en pie. Según el informe de la consultora Edelman (Edelman Trust Barometer¹ 2018, que encuestó a más de 33.000 personas en veintiocho países), el 63% de la población mundial no es capaz de distinguir entre noticias verídicas y rumores. En el mismo documento se afirma que un 59% de la población opina que cada vez es más difícil saber si una noticia proviene de un medio respetado o no. Resulta paradójico comprobar cómo la sociedad de la información sufre una auténtica epidemia de desinformación; quizá por ello nace esta publicación. El hecho cierto es que la oportunidad de hacerlo parece innegable, del mismo modo que parece innegable que con la era de la *posverdad* se inicia el reinado del sentimiento, que emerge victorioso sobre la verdad. Esta verdad, la vieja y superada verdad, no representa ya un valor o un modelo, sino que se nos aparece justo como lo contrario. En una imagen, es como si alguien que esgrimiera la verdad frente al sentimiento se nos representase como la fría espada clavándose en el corazón palpitante. Al fin y al cabo, no es nada nuevo, pues el corazón tiene razones que la razón ignora. El ser humano se ha debatido desde sus inicios como especie entre lo que su cabeza le aconseja y lo que su corazón le dicta, y viceversa, en función de qué parte

¹ <https://www.edelman.com/trust-barometer>. © 2018 Edelman.

predomine sobre ellos y en qué momento. Pero esta disyuntiva siempre se ha incardinado más en el ámbito de las decisiones individuales: las relativas al plano de las relaciones afectivas o a la interpretación de información poco comprensible. Aún hoy sigue vigente; podría decirse, sin duda, que forma parte de la esencia misma del ser humano. Y es quizá en esa esencia natural en la que se basa la posibilidad misma de la *posverdad* y su implantación en nuestra sociedad actual. Sin embargo, hacen falta más elementos para su arraigo y fértil crecimiento, y estos ya no son tan «naturales»: son justamente lo contrario. No nacemos adictos a nada, aunque en nuestra genética llevemos la posibilidad de serlo. Es el entorno el que determina el modo de vida, y esa vida la que lleva a tales adicciones. Si la era de la *posverdad* es la era de la superación de la verdad misma y, a la vez, la supremacía del sentimiento frente al dato objetivo, no sería absurdo decir que la intolerancia a este ha derivado en adicción a aquel. Nos hemos convertido en consumidores compulsivos de sentimientos que, sistemáticamente, digerimos deprisa para poder consumir otros nuevos. Para llegar hasta aquí, como se pregunta Eva Moya en su capítulo en esta publicación, han sucedido muchas cosas en nuestro entorno que seguramente han derivado en esa adicción. Pero, ¿qué ha sucedido? ¿cómo nos afecta? ¿hacia dónde nos lleva? ¿podemos superarlo? y lo que es más importante, ¿cómo podemos hacerlo? son precisamente algunas de las cuestiones que nos hemos propuesto analizar y responder en esta publicación del IEEE (Instituto Español de Estudios Estratégicos).

Para ello, Federico Aznar Fernandez-Montesinos inicia su capítulo, el primero, con una provocación en forma de tango, tomando prestada para la ocasión la letra de *Cambalache* de Enrique Santos Discépolo. Entiéndase provocación en este contexto como la cruda presentación ante nuestros ojos de una letra que pretende, y creo que consigue, describirnos la sociedad como una sucesión de desórdenes, desequilibrios, desmanes, injusticias y carencias de valores con las que más o menos podemos estar de acuerdo, pero que tocándonos el corazón resultaron ser, son y serán, ni más ni menos, ¡verdad! Es precisamente esa «pérdida de horizontes y referencias que implica la posmodernidad», en palabras de Federico Aznar, la que vivimos y la que Santos Discépolo describe, la que ha posibilitado, con el empleo de las redes sociales, la aparición y difusión de noticias no ajustadas a la verdad o simplemente falsas, que han terminado por inundar los canales de comunicación social y que han puesto en grave riesgo tanto la gobernanza de muchos países como el papel de los medios de comunicación clásicos. En este sentido, el referido informe de Edelman afirma que el 78,5% de los países desconfían de los medios. Por su parte, el informe *Authenticity in an Uncertain World*² pone de manifiesto que la media de confianza en los medios

² Authenticity Gap Report – ©FleishmanHillard Inc. <http://cdn.fleishmanhillard.com/wp-content/uploads/meta/resource-file/2017/authenticity-gap-2017-global-executive-summary-1505147721.pdf>. (p. 9).

tradicionales es del 27%, del 23% en los medios de papel y del 19% en redes sociales.

Redes sociales: ya tenemos otro de los elementos indispensables en el mundo posmoderno, en el mundo de las noticias falsas y la *posverdad*. Eva Moya nos contará en su capítulo cómo hemos llegado hasta aquí, y para ello las redes sociales y su evolución son la clave: hemos superado el primer modelo unidireccional de Internet para llegar a uno multidireccional, hemos pasado de las de las .com a los *social media*, de los teléfonos móviles a los *smartphones*, del periodismo clásico al periodismo popular, del boca a boca al «pásalo», etc. En términos generales, podríamos hablar de un cambio radical en el sistema de relación de los seres humanos entre sí. Antes se han citado cambios a modo de ejemplo, pero si se paran a pensar, es vertiginoso lo que nos ha sucedido en una cantidad de tiempo ínfima, y los cambios provocados son inmensos. Quizá, lo más importante en este campo es que la comunicación de masas, que antes estaba reservada a los medios clásicos de comunicación, a las instituciones o grandes empresas y a muy pocas personas a título individual, hoy está completamente abierta a todos los seres humanos. Sin embargo, ese espacio global y abierto, permeable y directo que representan las redes sociales puede ser simultáneamente un lugar de información o servir de plataforma para lanzar cualquier falsedad, e incluso una campaña completa de propaganda o desinformación. Añadan máquinas que, simulando ser seres humanos, envían miles de mensajes, y a esto la posibilidad de que una institución o un Estado este detrás de la campaña: sería el sueño de Göebbels. Pero como toda obra humana es perfectible, ¿qué tal si a todo le añadimos el anonimato? pues sea. Ya tenemos una perfecta *fake*: libre, universal, rápida, sencilla, gratuita, falsa y anónima. Revístanla de auténticos valores (naturalmente falseados) como el pacifismo, la defensa de los derechos y libertades del ser humano, la necesidad de recaudar fondos para falsas enfermedades o causas y demás ingredientes que tocan el corazón y estarán ante la sublimación de una noticia falsa. Ya no es necesario pedir a la puerta de una iglesia, te ingresan la limosna en tu cuenta corriente; ya no es necesario tener razón, solo es preciso que lo parezca; ya no hay que intimidar o agredir para torcer voluntades, basta con engañar impunemente; no se entra en un banco a punta de pistola, se entra en su servidor a punta de virus; no se persigue al malo, sino a su *smartphone*; no tienes que buscar la mejor oferta para encontrar lo que buscas, ella te encuentra a ti; no escribas lo que pienses, piensa dónde puede estar ya escrito. En efecto, estamos en ese cambalache que nos introducía al asunto, pero es un cambalache 2.0. La bondad y la maldad del ser humano no cambian, solo cambia el escenario donde se representa la vida y sus actos se proyectan. Las redes sociales no son ni buenas ni malas, solo las personas lo son. Por tanto, ¿qué ha sucedido para que las personas que utilizamos las redes seamos tan permeables como comunidad a este torbellino de mentira? quizá tenga mucho que ver con la instauración de una «cultura» muy basada en tópicos falsos, en la simplificación de contenidos, en el relativismo y, como no, en lo políticamen-

te correcto. Quizá tenga que ver con la infantilización de nuestra sociedad actual, y no solo en la apariencia física, sino en la esencia del pensamiento. Es muy frecuente aparentar juventud física y mental; la primera tiene que ver únicamente con la estética, pero indisociablemente parece ir unida a la mentalidad. Es como si una especie de efecto Walt Disney se hubiese apoderado del subconsciente colectivo. Esto implica conductas en las que los derechos aniquilan a los deberes, las consignas triunfan sobre los discursos y lo simple es obligado. Se aprecia muy bien en el discurso político; Orwell lo describía de manera premonitoria y sublime en *Palabras nuevas*³. En él queda patente el efecto que la limitación y la redefinición del lenguaje producen sobre la capacidad de pensar, lo que hoy algunos llaman «hechos alternativos» y que no son otra cosa que la capacidad para describir con todo detalle una realidad en términos completamente falsos, apelando al supuesto derecho que cada uno tiene a ver lo que le dé la gana y como le dé la gana e imponérselo al común de los mortales como una verdad absoluta (Kellyane Conway⁴, afirmando que el Gobierno había dado «hechos alternativos» para justificar el número de asistentes a la ceremonia de investidura de Donald Trump).

En este orden de cosas, Alfonso Merlos nos presenta la era de la *posverdad* marcada por la difusión estratégica a través de campañas metódicas y de alcance global, de informaciones de dudosa veracidad y de historias falsas que, en determinados procesos políticos y electorales, pueden representar una amenaza para la seguridad de los Estados y de la propia comunidad internacional. Las guerras de información basadas en el uso masivo y estudiado de las nuevas tecnologías de la comunicación exigen de nuevas estrategias de defensa que identifiquen con precisión la fisonomía de estos nuevos riesgos y sean capaces de atacarlos, neutralizarlos, amortiguarlos en sus efectos. Los planes y mecanismos a desarrollar e implementar tendrán forzosamente un carácter, en el corto plazo, dinámico y transformacional.

Existe una máxima en periodismo que dice que las opiniones son libres, pero los hechos son sagrados. Si la opinión como interpretación no puede ni debe ser objetiva, la información ha de ser veraz, y opinión e información deben estar debidamente identificadas y acotadas. Sin embargo, en el contexto actual de sociedad líquida que ya anticipó Bauman (frente a la solidez de los valores de la sociedad moderna), se observa que estas máximas antes señaladas se rompen: la *posverdad* es una amenaza que tiene enorme protagonismo hoy en día. Hay quienes defienden que la *posverdad* es la mentira de toda la vida, y, en esencia, tienen razón, pues toda *posverdad* es mentira, aunque no toda mentira alcance la categoría de *posverdad*. Sin embargo, la cuestión no es esa, no es de esencia, sino de forma y dimensión. La sociedad se precipita cuando las emociones y las opiniones priman sobre los hechos

³ ORWELL, George. *Palabras nuevas*, editorial Godot, 2014. ISBN: 9789871489800.

⁴ Kellyane Conway, Consejera del Presidente de Estados Unidos actualmente en el cargo.

objetivos de forma generalizada. Cuando unos hechos descontextualizados, o simplemente falsos, sirven para generar una opinión (naturalmente falsa de inicio y que se propagará como una epidemia), cuando esta ruptura de principios y valores se produce y sus consecuencias no solo producen el reproche hacia su autor, sino que además le proporcionan un beneficio, sin duda estamos ante un grave problema.

Los elementos que han influido en el desarrollo de este fenómeno son dos, los cuales a su vez están interrelacionados: el desarrollo de las nuevas tecnologías de la información y la comunicación (TIC) y el proceso de globalización. Ambos han llevado a que el alcance de los riesgos de la generalización de la *posverdad* tenga carácter global y casi inmediato.

La *posverdad*, no obstante, es un hecho que alimenta otro de mayor envergadura si cabe, el populismo. A lo largo de la historia, las grandes crisis económicas han venido acompañadas de crisis políticas y sociales: los ciudadanos buscan desesperados las razones de su malestar y casi siempre terminan encontrándolas en los Gobiernos de turno. Esto ha provocado que hoy en Europa haya vuelto el fantasma del populismo (*El retorno de los chamanes*, como señala Víctor Lapuente⁵), lo que impulsa por ende un discurso populista que busca apelar a las emociones y sentimientos del pueblo. Las opiniones son, en estos casos, elevadas a la categoría de verdad fáctica. En el mundo de la *posverdad*, la generación de condiciones previas en el entorno social, cultural o político es el hecho necesario para poder después aplicar las medidas deseadas: descontento social generalizado, anteposición de los sentimientos a la hora de tomar decisiones puramente racionales y Gobiernos sometidos a lo políticamente correcto aparecen en nuestros tiempos de modo generalizado, y son el perfecto caldo de cultivo para la eclosión populista. Podría decirse que se produce una auténtica inversión en el proceso de formación de la opinión y su correlato en la manifestación de la voluntad en la sociedad. Angel Riesgo⁶ afirma:

«Hay gente que piensa que los consumidores siguen la cadena de acción pienso-hago-siento, cuando en realidad el orden es “siento-hago-pienso”. Por eso muchas decisiones de consumo se toman con la emoción, y luego se usa la razón para justificarlas. Es lo mismo que pasa ahora con la decisión de voto».

Este comportamiento generalizado es el que provoca el surgimiento de sociedades polarizadas, divididas en facciones incompatibles, casi irreconciliables. Cas Mudde y Cristóbal Rovira⁷, en su libro *Populismo: una muy breve introducción*, describen que se trata de un tipo de política que ve a la sociedad

⁵ LAPUENTE, Víctor. *El retorno de los chamanes*, ed. Península, 2015. ISBN: 9788499424408.

⁶ <http://angelriesgo.blogspot.com.es/>.

⁷ MUDDE, Cas; ROVIRA, Cristóbal. *Populismo: una muy breve introducción*, 2017.

dividida en dos grupos en pugna, catalogados como «el verdadero pueblo» y «la élite corrupta».

Las causas tienen que ver con el éxito de las redes sociales y la crisis de credibilidad de la prensa tradicional. Eli Pariser⁸, autor de *El filtro burbuja*, indica que los algoritmos de Instagram, Facebook y Twitter ahondan la división creando islas ideológicas cerradas donde los usuarios tienden a recibir solamente opiniones políticas afines y noticias, reales o falsas, que corroboren sus prejuicios. A medida que las empresas suministradoras de contenidos en la Red proponen más contenidos a sus «clientes», estos cada vez son más prisioneros de ellas. Esta constante retroalimentación de las narrativas propias tiende a endurecerse y a protegerse de forma férrea de las de «los otros» subrayando las diferencias y haciéndolas cada vez mayores, a la vez que atacando de modo inmisericorde cualquier disonancia o discrepancia con ellas. Hoy muchos ciudadanos pasan gran parte de su tiempo escrutando las redes en busca de posibles ataques a su «bando» para actuar en contra, e incluso en no pocas ocasiones se ven auténticos linchamientos mediáticos. A este respecto, Juan Soto Ivars⁹ señalaba lo siguiente:

«En esta división aparece una nueva forma de censura, la poscensura. Provocada, sin ser totalmente conscientes de ello, por los dos bandos de la corrección política. Suele escribirse sobre corrección política de izquierdas, pero el otro frente de puritanismo censor se ha vuelto tan poderoso como aquella. Miles de ciudadanos ejercen una vigilancia paranoica del pensamiento y el lenguaje público a través de las redes, desde la izquierda y la derecha. Quien hoy defiende tu libertad de expresión, mañana tratará de castigarte.

[...]

Al calor de la poscensura han brotado empresas como Writing in the Margins, que “corrige” los libros antes de ser publicados para “limpiarlos” de expresiones que puedan ser entendidas como racistas o machistas. Así, una escritora tan poco sospechosa de xenofobia como J.K. Rowling, autora de Harry Potter, decidió someterse a esta censura para ahorrarse posibles linchamientos en Twitter. Su comportamiento respondía a un miedo contemporáneo: ser acusado de algo que no eres por una multitud de pueblerinos digitales. [sic] Ocurrió a Tim Burton, acusado de racista porque sus protagonistas siempre son blancos, o a Scarlett Johansson, que había cometido el pecado de interpretar a la cyborg en la adaptación de un manga japonés.

[...]

⁸ PARISER, Eli. *The Filter Bubble: What the Internet Is Hiding from You Hardcover*, 2011.

⁹ SOTO IVARS, Juan. *Arden las redes* (Debate, Barcelona, 2017). ISBN 978-84-999275-2-7.

La poscensura es un sistema represivo que no requiere leyes ni estado [sic] censor, y que impone sus prohibiciones infundiendo el miedo a ser catalogados como traidores. Bajo la poscensura, los izquierdistas tienen miedo de que una multitud les llame machistas, racistas u homófobos, mientras que los derechistas temen etiquetas como buenista, relativista o progre. En cada bando, son los sinónimos de “traidor”.

La poscensura mata el debate racional y exagera los insultos y las acusaciones. Explica por qué engordan las posiciones radicales y se achica el espacio para la sutileza [...]».

Manuel Torres profundiza en estas conductas particulares de esos «ciudadanos» que actúan en las redes, a veces de modo individual y en otras ocasiones agrupados y con objetivos comunes. Un ejemplo de los muchos que pueden encontrarse aparece en el número de febrero de este año en *Le Monde Diplomatique*, que se hacía eco de los *netizens* chinos: ciudadanos jóvenes, entorno a los veinte años, que, frente a los comentarios críticos hacia China, contestan y explican al mundo las bondades de su país de manera gratuita, fruto de la educación recibida. Sin duda *hacktivistas* al servicio de una causa. Pero el propósito de este capítulo pretende abordar dos fenómenos de *hacktivismo* muy concretos y orientados hacia dos realidades que amenazan el mundo actual: el terrorismo yihadista y el movimiento antisistema. Su objetivo, en palabras del autor, es:

«Analizar como [sic] el hacktivismo ha sido empleado por individuos y organizaciones como una eficaz estrategia de comunicación. El propósito de ambos estudios de caso es analizar las dinámicas organizativas de estos movimientos. Se parte de la tesis de que el principal reto al que tiene que enfrentarse el hacktivismo (particularmente el de carácter delictivo), no es tanto la viabilidad de sus operaciones, sino cómo conciliar su vertiente colectiva, con la individualidad de sus miembros».

El mundo de la *posverdad*, en suma, no solo ha cambiado los procesos de relación y comunicación de nuestra sociedad, sino que, para ello, también ha afectado gravemente al reconocimiento y al ejercicio de algunos derechos fundamentales y libertades públicas dentro de un marco constitucional garantista, al menos al modo en que estos se han entendido en los Estados democráticos durante gran parte del siglo xx. Como se ha dicho, quizá los más afectados sean el derecho a la libertad de opinión y el derecho a la información, elementos esenciales para la construcción de una democracia liberal. Y no solo se ven afectados, sino que además representan una debilidad utilizada por personas, grupos y agentes estatales para atentar contra los sistemas en los que se incardinan. Hannah Arendt, sin embargo, ya apuntaba cómo esto podría ser un gran farsa si, paralelamente, no se garantiza la información objetiva y no se aceptan los hechos mismos. En el siglo xx, en sentido contrario, esto podía verse de forma patente en regímenes autoritarios, que se valían de elementos como la propaganda para engañar y

manipular a la población. Elocuente es la frase de Iván Agayants¹⁰, responsable de operaciones de desinformación del KGB, 1965: «algunas veces me sorprende de lo fácil que es jugar a este juego. Si ellos no tuviesen libertad de prensa, deberíamos inventársela».

El mundo de la *posverdad* no solo impacta de lleno en la formación de la opinión pública, sino que, como consecuencia de ello, lo hace como se dijo en el ejercicio de derechos «sagrados» hasta hoy, y con ello, de paso, afecta a otro de los pilares básicos de nuestras sociedades: la economía. Eva Moya cita un clarísimo ejemplo (de los muchos que pueden encontrarse) que sucintamente viene a explicar cómo por medio de campañas basadas en falsedades flagrantes se puede engañar durante el tiempo necesario a todo un mercado de valores para «hacer temblar» ni más ni menos que a Wall Street. Si James Carville espetaba aquel «Es la economía, estúpido» para hacer entender que en aquella campaña que llevó a Clinton a la Casa Blanca la economía era lo verdaderamente importante y seguro para los ciudadanos-electores, hoy podríamos seguir diciendo que la economía, no cosa baladí, sigue siendo un pilar esencial de nuestro modelo de sociedad. Pero hoy, sin perder su vigencia, la frase debería ser completada: hoy es la economía y es la nueva comunicación de la era de la *posverdad*. Sin duda, la economía es y será siempre un factor clave, hoy por hoy incluso un factor esencial para desencadenar guerras (por supuesto no declaradas y alejadas de cualquier formalismo clásico). Sin embargo, se apoyan en potentes aparatos y campañas comunicativas de enorme simplicidad y basadas en lo pasional o en lo emocional, si se quiere (*America first*). Está por demostrarse que este eslogan vaya a proporcionar mejores condiciones de vida a los ciudadanos de Estados Unidos. Es más, a juicio de no pocos analistas, el encierro en sí misma de la economía de Estados Unidos probablemente obtenga resultados opuestos a los que persigue; sin embargo, ya consiguió de inicio el beneplácito de millones de ciudadanos a los que no se propuso ninguna solución concreta a sus problemas, sino que simplemente se sintieron escuchados. Esta es la política de la *posverdad*: ya no es necesario aportar soluciones por medio de programas sólidos dirigidos a los ciudadanos, solo es necesario que estos se sientan escuchados. De nuevo, el corazón sobre la mente.

Hoy, resulta más que evidente, no se declara la guerra; es más el empleo legítimo de la fuerza por parte del Estado lo que se pone constantemente en cuestión. No es políticamente correcto su empleo aunque responda a situaciones o provocaciones racionalmente claras, aunque trate de evitar abusos e ilegalidades flagrantes que se escudan precisamente en un supuesto pacifismo articulado en una narrativa *ad hoc*. El concepto clásico de legitimación en el empleo de la violencia por parte del Estado, tal y como lo definía Weber, está en cuestión para muchos ciudadanos. Sin embargo, el hecho de

¹⁰ Ivan Ivanovich Agayants (28 de agosto de 1911 – 12 de mayo de 1968). KGB oficial de inteligencia.

no reaccionar a esta situación puede llevar a la parálisis o cuanto menos a una enorme dificultad del Estado a la hora de actuar frente a la proliferación de narrativas que están intoxicando la opinión pública y lo ponen en riesgo. Es verdad que en el plano defensivo han proliferado diversas iniciativas —entre ellas el East Stratcom de la UE— para detectar, seguir y denunciar las noticias falsas, aislarlas y ofrecer información veraz. Pero esto no deja de ser una respuesta, como se dijo, puramente defensiva; es un escudo puesto sobre la población para tratar de evitar los embates de la mentira como arma. Sin embargo, ahí queda todo. Como sociedad, nos declaramos «pacifistas» ante los relatos que tratan de debilitar e incluso destruir nuestros Eobiernos, nuestras instituciones e inevitablemente nuestra sociedad tal y como la conocemos, queremos y por cuya construcción hemos trabajado. Si las guerras, o eufemísticamente los conflictos, hoy no responden al modelo clásico, no es lógico combatirlos con medios clásicos. Hoy es el tiempo de las guerras híbridas, que se han convertido en la principal amenaza para la estabilidad de los Estados, y su procedencia, en muchas ocasiones poco clara, puede tener su origen en la acción de otros Estados, de grupos de naturaleza subnacional y, como también se dijo, de actores no estatales. El interés por condicionar y manipular la opinión pública constituye una amenaza cada vez más importante, y las armas o herramientas para conseguirlo son cada vez más poderosas. Son las llamadas «armas de seducción masiva» en palabras de Javier Lesaca¹¹; los objetivos de quienes las esgrimen se centran en destruir la cohesión y el pacto social que une a los ciudadanos con sus instituciones públicas. En el capítulo final de esta publicación, nos pone de manifiesto como:

«En los últimos cinco años, las operaciones ofensivas de disrupción comunicativa por parte de gobiernos [sic] y de grupos violentos y extremistas han aumentado, en cantidad y en complejidad. La investigación y monitorización de estos intentos de desestabilización de la opinión pública demuestra que existe una metodología de la disrupción que consiste en los siguientes procesos: a) detección de las vulnerabilidades sociales de un país; b) creación de una narrativa que fomente estas vulnerabilidades en la opinión pública; c) implementación de una red de medios de comunicación propios; d) utilización automatizada y trampa de las plataformas de comunicación social. Los estados [sic] deben entender la naturaleza de esta amenaza y construir capacidades que permitan hacerla [sic] frente con eficacia».

Se trata de actuar tanto en el campo de la legislación como en el campo de la comunicación estratégica. En el primero, en las reformas legislativas, Francia, uno de los países que ha sufrido injerencias en sus procesos electorales, está en pleno debate sobre el asunto. El presidente de la Repúbli-

¹¹ LESACA, Javier. *Armas de seducción masiva*, Haz clic para votar Eliminar voto ed.: Península, 2017. ISBN: 9788499426143.

ca, Emmanuel Macron, ha anunciado la presentación de un proyecto de ley que impide la desinformación a los ciudadanos en los periodos electorales con el fin de «luchar contra toda tentativa de desestabilización dirigida por servicios especiales controlados o influenciados por potencias extranjeras». Sugiere una posible legislación que pudiera permitir el recurso ante un juez de instrucción para intervenir con rapidez y, llegado el caso, suprimir los contenidos falsos, cerrar o bloquear los accesos a Internet de los medios que propaguen *fake news*¹².

Por su parte, la Comisión Europea propone un Código de Buenas Prácticas. Se trataría inicialmente de un conjunto de medidas para combatir la desinformación a través de las redes por medio de la promulgación de un Código de Buenas Prácticas sobre Desinformación, que pretende fomentar el periodismo de calidad y promover la alfabetización mediática. En febrero de 2018, la Comisión promovió unas recomendaciones con la vista puesta en las elecciones de 2019 al Parlamento Europeo en las que «Se anima a las autoridades nacionales competentes a determinar, basándose en las experiencias de los Estados miembros, las mejores prácticas para detectar, mitigar y gestionar los riesgos que suponen para los procesos electorales los ciberataques y la desinformación».

El 12 de marzo de 2018 se publicaron las conclusiones y recomendaciones del grupo. En concreto fueron las siguientes:

- «1. Mejorar la transparencia de las noticias en línea, involucrando un intercambio adecuado y conforme a la privacidad de los datos sobre los sistemas que permiten su circulación en línea;
2. Promover la alfabetización mediática e informativa para contrarrestar la desinformación y ayudar a los usuarios a navegar en el entorno de los medios digitales;
3. Desarrollar herramientas para empoderar a usuarios y periodistas para abordar la desinformación y fomentar un compromiso positivo con las tecnologías de la información en rápida evolución;
4. Salvaguardar la diversidad y la sostenibilidad del ecosistema de los medios de comunicación europeos, y;
5. Promover la investigación continua sobre el impacto de la desinformación en Europa para evaluar las medidas tomadas por los diferentes actores y ajustar constantemente las respuestas necesarias».

En lo que a comunicación estratégica se refiere, la UE, como se dijo, ha puesto en marcha la iniciativa East Stratcom Task Force, pero su di-

¹² ABC internacional. JUAN PEDRO QUIÑONERO. Corresponsal en París. Actualizado:04/01/2018 11:49h.

mención, inicialmente al menos, y sus capacidades parecen reducidas frente a las que debe combatir.

Estamos, como ha podido verse, ante un nuevo panorama que afecta a la gobernanza de los Estados y al derecho a la información veraz de los ciudadanos, que basa su poder disruptivo en la horizontalidad y la democratización de la comunicación mediante el empleo de las redes sociales. Y estamos a la vez ante un horizonte difícilmente predecible, en el que todo ejercicio de prospectiva queda obsoleto casi al momento de nacer. Su desenlace se presenta incierto, si bien en esto tampoco puede aventurarse nada positivo o negativo. Lo cierto es que tras la superación de la era de la posverdad, las noticias falsas, las campañas de desinformación... el nuevo orden mundial no parece que vaya a ser el mismo que hoy tenemos.

Pues bien, este es el mundo que hoy nos toca vivir, aunque la realidad que proyecta sobre nosotros no parezca ser la que colectivamente queremos afrontar. Ese «cambalache» que da inicio a esta publicación debería encontrar respuestas y, paradójicamente, en el ámbito musical al menos hay una: «Nunca es triste la verdad, lo que no tiene es remedio»¹³:

«Cuéntale a tu corazón
que existe siempre una razón
escondida en cada gesto.
Del derecho y del revés
uno es siempre lo que es
y anda siempre con lo puesto.
Nunca es triste la verdad
lo que no tiene es remedio».

Dicho de otro modo, la verdad y los hechos siempre estarán ahí, por mucho que se intente esconderlos o deformarlos. Sin embargo, para reconocerlos hace falta resiliencia ante lo adverso y juicio crítico ante lo que se nos muestra porque, en efecto, nunca es triste la verdad, lo que no tiene es remedio.

¹³ JOAN MANUEL SERRAT. Título: "Sinceramente Tuyo".

Capítulo primero

El mundo de la posverdad

Federico Aznar Fernández-Montesinos

Resumen

La pérdida de horizontes y referencias que implica la posmodernidad se ha visto acentuada con la globalización. El surgimiento de redes sociales en el contexto de la crisis de la política y del periodismo ha posibilitado la aparición y circulación de noticias e informaciones que no se atienen completamente a la verdad, y en no pocas ocasiones de un modo intencionado. Este fenómeno precisa ser superado, pues daña a la cohesión de la comunidad y promueve el desorden. Tal cosa ha de hacerse de un modo calmado y acorde a los valores propios, buscando la actuación concertada de la comunidad democrática internacional en tal empeño.

Palabras clave

Posverdad, fake news, posmodernidad, guerra híbrida, censura, periodismo.

Abstract

The loss of horizons and references that imply postmodernity has been increased with globalization. The emergence of social networks in the crisis of journalism and politics has made easier the appearance and circulation of news and

information that does not fully adhere to the truth, often in an intentional manner. This phenomenon needs to be overcome because it damages the cohesion of community and promotes disorder. Such a thing needs to be done calmly and in accordance with our values, seeking the concerted action of the international democratic community in this endeavour.

Keywords

Post truth, fake news, postmodernity, hybrid warfare, censorship, journalism.

Que el mundo fue y será
una porquería, ya lo sé.
En el quinientos seis
y en el dos mil, también.
Que siempre ha habido
chorros,
maquiavelos y estafaos,
contentos y amargaos,
barones y dublés.
Pero que el siglo veinte
es un despliegue
de maldá insolente,
ya no hay quien lo nie-
gue.
Vivimos revolcaos en un
merengue
y en el mismo lodo
todos manoseados.
Hoy resulta que es lo
mismo
ser derecho que traidor,
ignorante, sabio o chorro,
generoso o estafador...
¡Todo es igual!
¡Nada es mejor!

Lo mismo un burro
que un gran profesor.
No hay aplazaos ni esca-
lafón,
los ignorantes nos han
igualao.
Si uno vive en la impostura
y otro roba en su ambición,
da lo mismo que sea cura,
colchonero, Rey de Bastos,
caradura o polizón.
¡Qué falta de respeto,
qué atropello a la razón!
Cualquiera es un señor,
cualquiera es un ladrón...
Mezclao con Stravisky
va Don Bosco y La Mignon,
Don Chicho y Napoleón,
Carnera y San Martín...
Igual que en la vidriera
irrespetuosa
de los cambalaches

se ha mezclao la vida,
y herida por un sable sin
remache
ves llorar la Biblia
junto a un calefón.
Siglo veinte, cambala-
che
problemático y febril...
El que no llora no mama
y el que no afana es un
gil.
¡Dale, nomás...!
¡Dale, que va...!
¡Que allá en el Horno
nos vamo'a encontrar...!
No pienses más; sentate
a un lao,
que ha nadie importa si
naciste honrao...
Es lo mismo el que
labura
noche y día como un
buey,
que el que vive de los
otros,
que el que mata, que el
que cura,
o está fuera de la ley...

Cambalache, Enrique Santos Discépolo.

Una época de confusión. Los *pos-* y los *-ismos*

Para gestionar un conflicto, y más aún para resolverlo, es preciso comprenderlo; ello requiere, a su vez, entender el entorno cultural en que se desarrolla, las claves psicosociales que inciden en él. La guerra es un hecho social: no es la misma la guerra que emprende un pueblo pastor que un pueblo agricultor. La cultura marca sus formas. Sin entender un conflicto, sin comprenderlo y acotarlo, no hay modo de ganarlo. Por eso los primeros debates son, o deben ser, metacognitivos; definir el marco en que se dan y su naturaleza es lo primero. Como Clausewitz decía, cada tiempo tiene su propia teoría de la guerra.

En fin, el tiempo que nos ocupa no termina aún de encontrar su lugar, y como resultado ha resurgido una suerte de neodecadentismo; es un tiempo que se define en torno o contra algo, de prefijos (los *pos-*) y de sufijos (los *-ismo*). La acotación aúna un marco de superación (aunque no de desaparición) junto con otro que implica un sesgo, una tendencia y hasta una radicalidad. Se da

cumplimiento así a la admonición de Gramsci: «lo nuevo no acaba de nacer, lo viejo no acaba de morir y en estos claroscuros surgen los monstruos»¹.

En esta lógica, ambos términos, «pos-» e «-ismos», han renovado palabras viejas y difusas que se vienen utilizando con diferentes significados y cronologías; también han servido para designar a distintos movimientos en diferentes ámbitos. En esta lógica, el antropólogo Roger Bartra² considera que con el prefijo *pos* no se alude a un tiempo «transcurrido después de una situación o un acontecimiento determinado», sino a cuando los acontecimientos pertenecen «a un tiempo en el cual el concepto especificado (la verdad, en el caso que nos ocupa) se ha vuelto insignificante o irrelevante».

Estamos ante un cajón de sastre en el que se apilan, desordenadamente, distintos movimientos y corrientes, en el que caben desde el fanatismo hasta el relativismo mientras se discute quienes, si la sociedad o los terroristas, son o dejan de ser nihilistas. Todo puede defenderse, pues no hay árbitro ni pretor con legitimidad suficiente para dictar una resolución en tan crucial asunto.

Al final, la posmodernidad viene a ser, ante todo, un estado mental, una actitud de negación y hasta de rechazo de todo lo anterior en la que lo efímero se vuelve norma por la falta de principios últimos. Por eso se cita ese tiempo, para confirmar su muerte y definitiva superación. Estamos por ello en una época de confusión y conceptos débiles que, necesariamente, rechaza cualquier forma de sacralización. Es la «sociedad ligera» de la que habla Braudillard o «líquida», como la definía Bauman.

Las instituciones que hacen posible la existencia de una verdad compartida —la educación, los medios de comunicación social y el propio marco normativo— se encuentran muy debilitadas, y el binomio sociedad-Estado de las que estas son juntura, también.

Como consecuencia, se priva al grupo de las necesarias referencias y, con ello, hasta de la idea de perfección y, subsecuentemente, de cualquier forma de legitimidad; aparece, por el contrario, un caos nebuloso y una sensación de deriva. El hombre queda una vez más, tal y como apuntaba Protágoras de Samos, investido de todo poder y consignado como la medida de todas las cosas, lo que acaba por generar, esta vez sí, una suerte de nihilismo. Una época por lo demás similar a la que dio origen a los sofistas en la Antigua Grecia.

Los tiempos ayudan a ello. Por ejemplo, los miembros de la llamada «Generación Z» (los nacidos entre 1995 y 2015) han vivido en un periodo de cambio

¹ «La crisi consiste appunto nel fatto che il vecchio muore e il nuovo non può nascere: in questo interregno si verificano i fenomeni morbosi più svariati». GRAMSCI, Antonio. *Quaderni del Carcere*. Volumen I Quaderni 1-5, Giulio Einaudi, 1977.

² ORTEGA, Octavio. *Favorece ignorancia posverdad en México*. [en línea]. Revista Reforma, 26 de marzo de 2017. Universidad Nacional de México. Disponible en web: http://www.iis.unam.mx/pdfs/iismedios/marzo2017/02_reforma.

permanente, en el que un paradigma sin solución de continuidad sigue a otro, y en el que lo último que ha sido superado se construye contra lo anterior que, además, se rechaza. Es lo que Paul Valéry calificó como «régimen de sustituciones rápido».

Como señala Zygmunt Bauman: «Hoy únicamente podemos albergar dos certezas: que hay pocas esperanzas de que los sufrimientos que nos produce la incertidumbre actual sean aliviados y que solo nos aguarda más incertidumbre»³. Las viejas soluciones ya no sirven, y las nuevas no terminan de adecuarse a los problemas a los que pretenden responder. La palabra futuro evoca, en estas circunstancias, algo cercano en el tiempo. Como apuntaba Baudrillard, en parte alineado con el pensamiento de Nietzsche: «Es el fin de la linealidad. En esta perspectiva, el futuro ya no existe. Pero si ya no hay futuro, tampoco hay fin. Por lo tanto ni siquiera se trata del fin de la historia»⁴. La sensación es la de un permanente interregno.

La ausencia de una propuesta de futuro —las ideologías constituían una atalaya desde la que se contemplaba el mundo y que obliga a su concreción en lo venidero— concentra sobre el presente cualquier solución: puede concluirse que es la gestión del presente, la inmediatez, una sensación de urgencia, la clave de una actitud posmoderna. *Carpe diem, carpe horam*⁵ frase manida y citada las más de las veces de forma incompleta.

Atender solo al presente, a su vez, impide el desarrollo de proyectos a largo plazo. El compromiso también pierde valor, ya que a cada instante es un nuevo punto de partida: no se mira hacia un pasado que ni existe, ni se comprende ni compromete. La cuestión es que, al moverse exclusivamente en el plano temporal y en el corto plazo, lleva a sus postulados a la contradicción, la incongruencia y el absurdo en otros planos y, con ello, a una suerte de hedonismo cortoplacista. En esta tesitura, el esfuerzo realizado parece serlo en arabesco y puede resultar baldío por incoherente y contradictorio.

La falta de horizontes es causa de un sentimiento de deriva, pues faltan las referencias necesarias para apoyar las decisiones y, al carecerse de certezas, todo es posible. Ese cuestionamiento del modelo vigente es el que subyace en la idea de la *posverdad*. El mundo postmoderno ha desechado encontrar una justificación general de la realidad que le dé sentido. Sin metarrelatos tampoco es posible la utopía: la realidad se fragmenta y la utopía también. Una utopía fragmentada para un mundo fragmentado, que se ha

³ BAUMAN, Zygmunt. *En busca de la política*. Fondo de Cultura Económica. Buenos Aires, 2001.

⁴ BAUDRILLARD Jean 1995 *La ilusión del fin. La huelga de los acontecimientos*. Barcelona, Anagrama.

⁵ El verso completo de *Las Odas* de Horacio es «*Carpe diem, quam minimum credula postero*», esto es, «*aprovecha el día, no confíes en el mañana*». La segunda parte del verso no suele ser referida.

convertido en el dominio de la interpretación y son estas las que, a la postre, dan de sentido a los hechos⁶.

El crepúsculo de las ideologías que marcó la llegada del nuevo siglo trajo un nuevo antropocentrismo del que se dedujo a su vez un cuestionamiento, un ablandamiento y una reformulación de muchas de las ideas imperantes hasta ese momento. Todo esto es lo que Gianni Vattimo denomina «pensamiento débil». Es el terreno del hombre *light*, del ciudadano conforme, sin valores ni pensamientos fijos, que vive en una realidad que ha configurado a su medida, por eso la sociedad del siglo xxi es conformista y acrítica. *Es la época del horroridens de Sartori*.

El posmodernismo también es posheróico. La muerte, las ideas negativas, pesarasas y aun hasta el mismo esfuerzo desaparecen. Es este un tiempo líquido, sin certezas ni relatos; no reconoce nada valioso detrás del esfuerzo, se desecha a los héroes por innecesarios o incluso por peligrosos (el ejemplo condena la inacción); los héroes, a lo mucho, son personajes genéricos o carcasas. Los restauradores y otras profesiones, incorporadas al mundo de la cultura, parecen haber ocupado su lugar en la divinización del hombre común, su apoteosis. Por eso, en pro de la horizontalidad, es preciso que los héroes sean personajes de ficción y se sepa. En todo hay un punto de falsedad reconocida y exculpatoria que sirve a la igualdad, por eso el término *posverdad* ha tenido tanta aceptación: vivimos en una época secularizada y posmítica.

Max Weber ya había profetizado que la desaparición de los valores, víctimas de los procesos de racionalización; era el destino de nuestro tiempo. Modernidad y nihilismo, entonces, se dan la mano en la posmodernidad liquidando los elementos cohesionadores (y también legitimadores) de la sociedad —entre ellos el patriotismo o la religión— en la medida en que ponían al individuo al servicio de esta.

La posmodernidad es adaptativa: los valores se acoplan como los líquidos a cualquier formato beneficiándose de su naturaleza amorfa. Como consecuencia, al no encontrarse vertebrados tampoco pueden direccionarse, por lo que no cabe esperar ningún beneficio de semejante capacidad adaptativa. Por eso es estática, pertenece al presente; volvemos otra vez sobre el conformismo y la falta de futuro. La emoción y el sentimiento imperan en este contexto y trasladan una sensación de movimiento.

No obstante, aunque ya no existen ideologías totalizadoras, sí se dan algunos debates que sirven para la fijación del marco sociológico de las sociedades y cuyas respuestas suponen la existencia de un cierto marco ideológico preferente por más que abierto y evolutivo.

⁶ BIANCO, Gabriella. «Desde el post-modernismo a la post-verdad» [en línea], en CECIES: Pensamiento latinoamericano y alternativo [ref. del 20 de marzo de 2018]. Disponible en web: <http://www.cecies.org/articulo.asp?id=582>.

Y es que no todo es malo en la posmodernidad, ni mucho menos. Es, en primer término, una reevaluación del hombre y una puesta en cuestión del sistema vigente, de sus clisés y dogmas. Uno de los grandes méritos y de las claves del pensamiento posmoderno es su visión antidualista y la puesta en valor de nuevas perspectivas (género, medioambiente, colectivos desfavorecidos), al tiempo que favorece el pluralismo y la diversidad. Además, el relativismo implícito al fenómeno sirve para desactivar los conflictos en la medida en que contribuye al cuestionamiento de sus causas. Y no es un movimiento necesariamente de derechas ni de izquierdas.

Los medios y la opinión pública

Según el dictado de Carl Von Clausewitz, la naturaleza de la guerra, en su acepción total, reside sobre una trilogía formada por el pueblo, que es su parte pasional, la actividad de las fuerzas armadas, que son su parte volitiva, y el campo racional, que queda reservado para los Gobiernos. El parecer del pueblo puede atribuirse a la opinión pública (discutible por anónima), y conviene, dicho esto, distinguir opinión pública y opinión publicada.

«La opinión pública difícilmente tomaba parte alguna en las guerras del XVIII; los soldados profesionales, reclutados en las clases más bajas de la sociedad, no sentían necesidad de saber porque *[sic]* luchaban. En el siglo XX, el soldado y el ciudadano han llegado a ser intercambiables y, el público en general, sintiéndose pacíficamente dispuesto, exige cuentas a sus dirigentes»⁷.

Y es que la opinión pública, es decir, el parecer del pueblo, siempre ha sido importante en los conflictos. No en vano, este tiene profundas implicaciones sociales por más que se desarrolle en tierras lejanas. Es la «dimensión social de la estrategia»⁸; como ejemplos de esta podemos considerar el papel de la televisión serbia o de la radio ruandesas, que han sido muy relevantes a la hora de instigar a la limpieza étnica⁹. El problema es que la opinión pública es volátil y se haya muy afectada por la emocionalidad.

La guerra se desarrolla simultáneamente en una pluralidad de planos tan importantes como el militar. Y toda vez que, según el principio de incertidumbre de Heisenberg, a la realidad se incorpora la percepción que se tiene de ella, los medios están llamados a ser uno de los aspectos más significativos de los conflictos, en tanto que afectan directamente a los soportes del esfuerzo bélico de las partes (pues influyen en la conciencia emocional de millones de personas). De hecho, pueden hasta otorgar la victoria a una de ellas, porque la victoria es también una cuestión de percepción y opinión.

⁷ ARON, Raymond. *Un siglo de guerra total*, París: Hispano Europea, 1958, p. 7.

⁸ TERNON, Yves. *El Estado criminal*. Barcelona: Península, 1995, p. 373.

⁹ Sáez ORTEGA, Pedro. *Guerra y paz en el comienzo del siglo XXI*. Madrid: Fundación del hogar del empleado, 2002, p. 67.

Se convierten así en un flanco que debe defenderse y también por el que resulta posible atacar, como bien nos va a detallar el concepto de guerra híbrida que trataremos más adelante.

La imagen de un conflicto, sus motivos, su gestión y su desarrollo es la generada por los medios y, no pocas veces, su parecer resulta más trascendente que la propia realidad. Nada existe que no sea publicado en un mundo mediatizado, y hace falta inteligencia para producir imágenes y para utilizarlas. Como Aron señala: «Los odios abstractos que asolan nuestro siglo son la obra de las masas urbanas, no de los soldados en el frente. Lo que Ely Havely llamó el “entusiasmo organizado” forma un capítulo en la historia de la movilización»¹⁰.

Pero fue a partir del siglo XIX, con la Revolución Industrial y el aumento de la tasa de escolarización, cuando se generalizaron los medios escritos (prensa y libros) como forma de negocio (con unos intereses específicos) y también como mecanismo de transmisión de noticias y de ideas. De hecho, se han convertido en objeto de interés empresarial con vistas a poder influir a nivel político.

Aunque las intervenciones coloniales británicas del XIX se vieron apoyadas desde los medios de comunicación social, fue en la guerra hispano-norteamericana cuando tuvieron un carácter capital para movilizar a la opinión pública, convirtiéndose en un factor polemológico de primer orden al contribuir a la legitimación del conflicto. La frase de Hearst a su dibujante Remigton «Por favor, permanezca allí. Usted suministre los dibujos que yo pondré a la guerra»¹¹ marca un hito en este sentido.

M. Ángel Ballesteros recuerda que los usos diplomáticos evolucionaron desde una diplomacia secreta resultado del «limitado entendimiento de los súbditos» cuyo último gran paradigma será Metternich, hasta una opinión pública elevada actualmente a la categoría de dogma, en combinación con unas políticas públicas por debajo de las cuales corren, y no siempre en la misma dirección, las políticas ordinarias¹²; con ello se vuelve a corroborar el *dictum* del austríaco: «la única verdad es la realidad y la única realidad son las apariencias».

Esta entrada de la opinión pública en los conflictos ha tenido una notable incidencia política y doctrinal. Y es que «la cámara (fotográfica o cinematográfica) tiene un campo de visión todavía más limitado que el hombre que la maneja y la cámara siempre utiliza lo particular para expresar lo general»¹³.

¹⁰ ARON, Raymond. *Op. cit.*, p. 23.

¹¹ COMPAYNS MONCLÚS, Julián. *España en 1898: entre la diplomacia y la guerra*. Madrid: Biblioteca Diplomática española, 1991, p. 188.

¹² BALLESTEROS, Ángel. *Diplomacia y Relaciones Internacionales*. Ministerio de Asuntos Exteriores, 1995, p. 180.

¹³ NIXON, Richard M. *La verdadera guerra*. Barcelona: Planeta, 1980, p. 121.

La cámara se transforma de este modo en una herramienta de la política. No obstante, y como apunta Ignatieff, «las imágenes televisivas son más eficaces expresando consecuencias que analizando intenciones, más adecuadas para señalar los cadáveres que para explicar porque *[sic]* resulta provechosa en ciertos lugares»¹⁴.

Las primeras fotografías de guerra se tomaron en la década de 1850 durante la guerra de Crimea¹⁵. La idea primigenia se basaba en que si el pueblo sostenía un conflicto con recursos humanos y materiales, no debía de mantener una opinión muy diferente de la propia de los Estados Mayores. Los medios de comunicación serían utilizados para sostener precisamente la opinión de una de las partes. La guerra será presentada como una sucesión de victorias. Por eso, no pocos alemanes, en la víspera de la capitulación de la Primera Guerra Mundial, estaban convencidos de estar a las puertas de París.

En esta línea, y coincidiendo con Clausewitz, Lord Palmerston afirmaba «las opiniones son más poderosas que los Ejércitos *[sic]*». Por eso, tanto Cavour como Bülow eran expertos en crear incidentes al objeto de conseguir la «exaltación nacional»¹⁶, con lo que la opinión pública pasa a formar parte del frente bélico.

Ya durante la Primera Guerra Mundial, el presidente Wilson¹⁷ consiguió mediante la propaganda activar al país para hacerlo participar en la guerra. Hitler, detalla Chomsky, atribuyó la victoria aliada en esa guerra a su superioridad en el frente propagandístico. De hecho, la palabra propaganda no era inicialmente peyorativa; uno de los ministerios de Hitler era el Ministerio de Ilustración Pública y Propaganda, dirigido por el doctor Joseph Goebbels. La ilustración y la propaganda se encontraban así al mismo nivel.

Un caso particular fue el abuso de la propaganda por parte de los japoneses a partir de las batallas de las Marianas (junio de 1944); la distorsión fue tal que se generó una atmósfera de irrealidad con importantes consecuencias logísticas y estrategias, ya que afectó a la evaluación de la situación por parte de los mandos subordinados, que desconocían por completo su estadio real¹⁸.

Como ejemplos más cercanos están las imágenes del ahorcamiento de dos sargentos británicos en Palestina a cargo de terroristas judíos, o de la muerte de soldados norteamericanos en Somalia, cuyo impacto en la opinión pú-

¹⁴ IGNATIEFF, Michael. *El honor del guerrero*. Madrid: Taurus, 1999, p. 29.

¹⁵ RAMONET, Ignacio. «Los Conflictos Armados» en VV.AA. *Seminario de Investigación Para la paz*. Diputación General De Aragón, 1997, p. 197.

¹⁶ *Ibidem*, p. 181.

¹⁷ CHOMSKY, Noam. *El nuevo orden mundial (y el viejo)*. Barcelona: Grijalbo Mondadori, 1996, p. 112.

¹⁸ CLAYTON, James D. «Las Estrategias Americana y japonesa en la guerra del Pacífico», en PARET, Peter (coord). *Creadores de la Estrategia Moderna*, Madrid: Ministerio de Defensa, 1992, p. 740.

blica está detrás de las retiradas de las tropas de aquellos países¹⁹. Pero la auténtica eclosión de los medios de comunicación en la guerra se encuentra en Vietnam; hay un antes y un después de esa guerra. En las proféticas palabras del presidente de Vietnam del Sur, Diem, «solo la prensa norteamericana puede ser la causa de que perdamos la guerra»²⁰.

A partir de entonces, los conflictos incorporarán ya abiertamente una estrategia mediática a la estrategia militar²¹ que sirva, en primer término, para la construcción del relato acorde con su visión: lo que se dice, lo que no se dice (por ejemplo, en la segunda guerra del Golfo, el régimen kuwaití no fue presentado al público), lo que se hace y lo que no se hace, con todos sus matices. Los medios de comunicación socializan a través de gestos, de climas afectivos, de tonalidades de voz, y promueven creencias, emociones y adhesiones totales²² en un mundo en el que los Ejércitos democráticos no pueden ganar guerras sin apoyo popular, sin un consenso real. Son imprescindibles.

Simultáneamente se desarrolla un plano ofensivo siguiendo los dictados de la propaganda política mediante fórmulas de creación tanto de héroes propios como de diablos enemigos. Esta plástica reduccionista se ha demostrado históricamente muy eficaz; se consigue concentrando todos los argumentos en personas o recurriendo a los mitos de la guerra, lo que prueba que el papel de los líderes en el surgimiento de los conflictos pueda ser menor del que se les atribuye²³. Ejemplo de ello es el mito de Hitler, tan útil que sirvió para dar una nueva identidad a Alemania al transferirle a aquel líder la responsabilidad completa de la Segunda Guerra Mundial y de sus atrocidades, lo cual, a su vez, permitió la reconstrucción del pasado del pueblo alemán²⁴.

Los medios de comunicación tienen una notable capacidad para determinar la agenda de los asuntos públicos, fijar la forma de abordarlos y establecer los criterios de valoración por la clase dirigente²⁵. Nixon, por ejemplo, contrapone la diferente repercusión de un mismo acto por su distinto tratamiento informativo: el suicidio de un bonzo frente a las cámaras en el contexto de la guerra de Vietnam y el cometido por un tártaro ruso para protestar por 35 años de destierro de su pueblo en la URSS²⁶.

¹⁹ HOFFMAN, Bruce. *Historia del terrorismo*. Espasa Calpe, 1999.

²⁰ NIXON, Richard M. *Op. cit.*, p. 121.

²¹ RAMONET, Ignacio. *Op. cit.*, p. 206.

²² TEDESCO, Juan Carlos. *El nuevo pacto educativo*. Madrid: Editorial Anaya, 1995, p.83.

²³ MICHAVILA NÚÑEZ, Narciso. «Opinión pública y conflictos armados», en *Revista Utopía y Sociedad*, n.º 19, 2002, p. 161.

²⁴ MICHAVILA, Narciso. *Op. cit.*, p. 162.

²⁵ *Ibíd.*, p. 157.

²⁶ NIXON, Richard M. *Op. cit.*, pp. 121 y 122.

Pero esta relación entre opinión pública, decidores y medios es bidireccional, pues no se trata solo de dar noticias, sino también de venderlas; los medios pueden expresar una opinión diferente de la del pueblo (dentro de todo el espectro de noticias), pero no completamente diferente, pues sino no satisfacerían los intereses comerciales. Como sostiene el general John Galvin:

«Los medios responden al pulso del público, a su orientación, por ejemplo Vietnam. No fueron tanto los medios los que cambiaron la opinión pública, como el público el que cambió los medios. Pienso que los medios reflejan muy bien los pensamientos del público, la presión del público, sus cambios... Creo que el mensaje viene del público»²⁷.

Un caso paradigmático es el de los secuestros aéreos²⁸, en los que el diálogo se sitúa a nivel internacional y permite una exposición pedagógica que va más allá del simple atentado, proporcionando un tema del gusto de los terroristas a los medios de comunicación. Por si fuera poco, el agresor traslada toda la responsabilidad al tiempo que conmina a la acción al agredido.

El mundo de la segunda mitad del siglo xx se había vuelto complicado; el incremento de la información disponible era tan intangible, que el periodista tenía que ser alguien que cribase y no solo transmitiese la información, un organizador, no solo un intérprete, alguien que haga accesibles los hechos²⁹. El problema, así, no era tanto la información, que, como se decía, hay mucha, sino la selección de la información. Como apuntaba Bernays allá por 1928:

«En teoría, cada ciudadano toma decisiones sobre cuestiones públicas y asuntos que conciernen a su conducta privada. En la práctica, si todos los hombres tuvieran que estudiar por sus propios medios los intrincados datos económicos, políticos y éticos que intervienen en cualquier asunto, les resultaría del todo imposible llegar a ninguna conclusión en materia alguna. Hemos permitido de buen grado que un Gobierno invisible filtre los datos y resalte los asuntos más destacados de modo que nuestro campo de elección quede reducido a unas proporciones prácticas. Aceptamos de nuestros líderes y de los medios que emplean para llegar al público que pongan de manifiesto y delimiten aquellos asuntos que se relacionan con cuestiones de interés público; aceptamos de nuestros guías en el terreno moral, ya sean sacerdotes, ensayistas reconocidos o simplemente la opinión dominante, un código estandarizado de conducta social al que nos ajustamos casi siempre»³⁰.

Todo ello permite estrategias que dan un amplio juego, al que se añaden la combinación de lo cierto y lo manifiestamente falso y todas las aproxima-

²⁷ MICHAVILA, Narciso. *Op. cit.*, p. 163.

²⁸ LE BORGNE, Claude. *La guerra ha muerto*. Madrid: Ediciones Ejército, p. 253.

²⁹ Citado por GARCÍA FERRERAS, Antonio en VV.AA. *Terrorismo, víctimas y medios de comunicación*, s.l., Fundación Víctimas del Terrorismo, 2003, p. 99.

³⁰ BERNAYS, Edward. *Propaganda*, s.l. Editorial Melousina, 2008, p.15.

ciones que caben, por tangenciales que resulten, en la realidad. Además, y como se ha visto, junto a intereses informativos, en un universo trasnacional existen intereses empresariales e intereses nacionales, lo que hace que existan intereses cruzados que pueden afectar al enfoque a nivel nacional e internacional y entre ambos.

Es por eso que la idea norteamericana de que la guerra debe ser tan transparente como la democracia y los medios de masas deben ilustrarla solo aguantó hasta el conflicto de Vietnam, cuando las ideas más nobles pudieron verse salpicadas ante las cámaras por la sangre derramada para sostenerlas³¹.

El siglo xxi es también el siglo del espectáculo. Los programas televisivos promueven en forma de *realities* conductas estereotipadas y poco edificantes, pero llamativas; si no conmueven en el minuto de un plano, aburren, lo que obliga a un permanente esperpento. Todo puede explicarse en menos de un minuto a una población semiculta. El hombre postmoderno no piensa, se informa; busca emoción en la noticia más que verdad, por eso las noticias falsas, diseñadas para ello, son más virales que las verdaderas: se adaptan mejor a lo que se demanda.

El terrorismo incorpora una estrategia de comunicación, pues se fundamenta en la «propaganda por los hechos», y pretende un impacto psicológico, trayendo el debate sobre la causa que promueve y generando un discurso. Es un fenómeno antiguo, pero cuyo desarrollo actual solo se explica con los medios de comunicación de masas a los que es parejo; es un acto de comunicación. Entre el terrorismo y los medios existe una perversa concurrencia de intereses.

Esta lógica la ha llevado al extremo el terrorismo del siglo xxi. Si hay algo en lo que coinciden las estrategias de grupos con al Qaeda y el Dáesh es en el activismo mediático, en el cuidado del mensaje y de los medios para su transmisión. El propio Ben Laden en una entrevista reconocía que ello suponía más del 90% del esfuerzo en la preparación para la batalla. El Dáesh ha ido aún más lejos si cabe incorporando las redes sociales, mejorando las labores de edición e incorporando las últimas técnicas de realización, al tiempo que incrementando exponencialmente el número de agencias y de publicaciones, creando un potente entramado mediático y hasta secuestrando y utilizando a un periodista como presentador.

El desarrollo de las redes sociales ha llevado al terrorismo, en cuanto hecho social, a un nuevo campo. Así, tres minutos después de los atentados de Niza (2016) había más de 3000 cuentas en las redes sociales, entre las que se encontraban cincuenta perfiles de Twitter que permanecieron activos durante tres horas. En los atentados de la Sala Bataclán (2015) había ocurrido lo mismo, pero, en este caso, los terroristas optaron por utilizar por primera

³¹ RAMONET, Ignacio. *Op. Cit.*, p. 199.

vez perfiles de Telegram —algo más novedoso— para difundir la masacre y amplificar su repercusión. Sus contenidos, en esta ocasión, permanecieron activos durante días, toda vez que no se tenía la experiencia previa³². El ciclo de respuesta del Estado, con todo, se acortó y ganó en eficacia.

Las posiciones que se adopten podrán ser cambiadas en el futuro; lo importante es formular una pregunta, comunicar un mensaje a un público objetivo mediante un acto de terror. Se trata de conmocionar para llegar a la audiencia en una sociedad posheroica que rechaza la muerte: «La elección de los Juegos Olímpicos [...] ha sido como pintar el nombre de Palestina sobre una montaña que se ve desde las cuatro esquinas de la Tierra»³³. La opinión ya podrá cambiarse después.

De partida, los medios, en su búsqueda de la neutralidad, de la equidistancia, asumen sus temas y debates —lo que resulta trascendental—, parte de su lenguaje y explican sus razones, lo que les permite ya *ab initio* obtener un rédito formal y de legitimación. Es el criterio de equidistancia, de objetividad, de ecuanimidad, que siempre subyace en la mente del que informa y motiva que pueda perderse la referencia y acaben equiparadas víctimas y verdugos, falsedad y verdad. El resultado es una difícil ecuación que, de partida, acepta el lenguaje de impugnación y admite varias soluciones.

La actividad terrorista está hecha a la medida de los medios de comunicación y genera situaciones paradójicas. Como decíamos, los medios están en permanente demanda de audiencia favorecida por noticias que aúnan inmediatez, exclusividad y dramatismo:

«Los terroristas explotaron la codicia normal de los medios de comunicación [...] para dar informaciones de impacto internacional, por lo dramático y la dimensión humana de la noticia [...]. En esta atmósfera la competitividad de los medios, siempre brutal, se convierte en algo especialmente feroz»³⁴.

Además, está la cuestión de la capacidad y calidad de esos medios. Entre la censura (lo que no se quiere dejar ver o explicar) y la propaganda (lo que se quiere hacer pensar o sentir) hay un espectro de posibilidades³⁵. Así, en la guerra de las Malvinas, habida cuenta de que la censura por amputación era insuficiente, se impuso el control de la información mediante un proceso de selección (el Pool), el control del acceso a la información (trato exclusivo con oficiales británicos) y los canales de transmisión (Ejército británico)³⁶.

³² ESCRIVÁ, Ángeles. «El altavoz del terror del Estado Islámico», en El Diario *El Mundo* [en línea]. 26 noviembre 2016. Disponible en web: <http://www.elmundo.es/internacional/2016/11/26/58385a4fe2704e2c3a8b45b5.html>.

³³ HOFFMAN, Bruce. *Op. cit.*, p. 107.

³⁴ *Ibidem*, pp. 207 y ss.

³⁵ Sáez ORTEGA, Pedro. *Op. cit.*, p. 123.

³⁶ RAMONET, Ignacio. *Op. cit.*, s.p.

Merece resaltarse que, si la comunidad internacional puede legalizar una intervención armada, es la opinión pública a fin de cuentas la que la dota de legitimidad. La posición de muchos países del continente durante la segunda guerra de Irak o el conflicto de Vietnam son un buen ejemplo de ello a escala global.

Por ello, el resultado de la influencia de los medios en la conducción de los conflictos es la evolución de la doctrina militar de EE.UU. que, durante la década de los noventa y comienzos del nuevo siglo, evolucionó hacia el establecimiento de criterios claros y restrictivos sobre el papel que sus fuerzas militares deben desempeñar en un conflicto (criterios Weinberger) y en la manera de hacerlo (doctrina Powell sobre «la fuerza decisiva desde el primer momento»). Se señalaban unos medios tendentes a garantizar el «efecto cero», la guerra sin bajas propias, al tiempo que se esforzaba en reducir el número de las enemigas. Desde la guerra de Kosovo el principio de «bajas cero» se ha incorporado a los conflictos bélicos³⁷.

La proliferación de medios tecnológicos hace que los periodistas puedan emitir en tiempo real sus crónicas desde el mismo lugar de los hechos, algo que hace poco era siquiera impensable y que incide en los resultados de las acciones a nivel operativo y hasta estratégico. El flujo de la información es tan rápido y dispone de tales tecnologías que la institución militar no puede controlarlo³⁸; si, como se ha visto, en la guerra de las Malvinas el material empleado seguía un camino controlable, ahora ya no es así³⁹.

Es el *efecto CNN*: sus albores se encuentran en la transmisión de imágenes de los sucesos de la plaza de Tian An Men en 1989 y de la caída del Muro de Berlín ese mismo año. Con ello desaparece la figura del mediador y la información llega cruda y en tiempo real; desde el punto de vista técnico, son consecuencia de la portabilidad de los sistemas y del desarrollo de la tecnología satélite, lo que hace que la televisión sea autónoma para trabajar en tiempo real y desde cualquier lugar del mundo⁴⁰, convirtiéndose en «factorías de la historia». Como dijera el subsecretario de defensa de EE.UU.: «Nuestro mejor servicio de inteligencia son los medios»⁴¹. Tanta trascendencia se da a este fenómeno que Jeff Bezos (Amazon) sostiene que estamos en la era de la desintermediación.

Las noticias distorsionan la guerra señalando objetivos que escapan a la lógica militar convencional y obedecen a estrategias de prensa; simultánea-

³⁷ RAMONET, Ignacio. *Guerras del siglo XXI. Op. cit.*, pp. 132-133.

³⁸ Internet es el desarrollo de un concepto militar ideado precisamente para no ser completamente controlado.

³⁹ WOOD, Paul. «Las guerras del siglo XXI» en VV.AA., *Una mirada al mundo del siglo XXI*, s.l.: Ministerio de Defensa, 2008, p. 64.

⁴⁰ RAMONET, Ignacio. *Los Conflictos Armados. Op. cit.*, p. 203.

⁴¹ HOFFMAN, Bruce. *Op. Cit.*, p. 229.

mente limita y condiciona la forma en que se llevan a cabo las operaciones, obligando a establecer márgenes de seguridad y a proteger la información⁴². Merece reseñarse que el número total de bajas en Vietnam no llegó a sumar el de un solo día en guerras anteriores, cuando no había un desarrollo tan independiente de los medios de comunicación.

Según Paul Wood, los medios marcan los tiempos y fijan el calendario político. Hoy el ciclo de la información es de 24 horas, máximo 48, de modo que la noticia puede viajar desde la misma línea de frente a los servicios de emisión y estar disponible en el día, obligando así a una respuesta política que, como mucho, puede dilatarse hasta el día siguiente⁴³.

Además, los medios generarían una ansiedad que marcaría el tiempo de la respuesta acortándolo, obligando a dar contestación a algo que no lo precisa solo por imagen e impidiendo que la implementación de una fase de la respuesta cuaje antes de pasar a la siguiente. De este modo, se antepone la emocionalidad de la opinión pública a la racionalidad o, incluso, a la resolución del problema planteado.

Michael Grannat, estableció en 1999 lo que denominó *la progresión de la respuesta de los medios de comunicación a una crisis*. a) Estallido: ocurre inmediatamente después a la producción de la crisis, se produce una avalancha de los medios sobre la escena de la crisis para intentar encontrar respuestas e intentar obtener imágenes; b) Investigación: intentar construir un relato de los hechos y encontrar toda la información relevante posible acerca del evento; c) Caza del hombre: los medios se lanzan a la búsqueda de algún culpable, error y chivo expiatorio; d) Epílogo: es a largo plazo y se encarga de seguir las acciones que se corresponden con las etapas de conclusión de la crisis, como son la reconstrucción, afectados, juicios... y es cuando se realizan los documentales⁴⁴.

La comunicación es un factor crítico inherente a todo proceso público, cualquiera que sea su naturaleza. Por ello, una mala gestión comunicativa puede provocar la prolongación de una crisis, puesto que las crisis conllevan adicionalmente una crisis de la información; si se falla en el control de esta crisis, se falla en el control de la crisis general. Y esa es la cuestión, porque la información se ha vuelto incontrolable. El problema ha dejado de ser tal para transformarse en un problema de opinión pública.

Y es que con la llegada del nuevo siglo el patrón de comunicación sufrió un radical proceso de cambio. En 2016, ya un 62% de los adultos estadouni-

⁴² JORDÁN, Javier; CALVO, José Luís. *El nuevo rostro de la guerra*. Barañáin: Ediciones Universidad de Navarra, 2005, p 210.

⁴³ WOOD, Paul. «Las guerras del siglo XXI», en VV.AA. *Una mirada al mundo del siglo XXI*, s.l.: Ministerio de Defensa, 2008, p.64.

⁴⁴ VV.AA., 2008, Conferencia «Gestión de Crisis», en Departamento de Estrategia de la Escuela Superior de las Fuerzas Armadas.

denses accedían a noticias a través de las redes sociales, y un 44% a través de Facebook⁴⁵. Las redes sociales son, de este modo, el eje sobre el que se construye el «ecosistema de información» en el siglo xxi, al tiempo que también constituyen una expresión de esa horizontalidad democrática que da voz a todos los actores con independencia de su calidad.

Como consecuencia, los medios han perdido el monopolio de la distribución de la noticia. Este siempre ha estado en manos de quienes las producen, que ahora son agentes individuales⁴⁶, y su canalización ha quedado consignada por diferentes factores, uno de los cuales, y no necesariamente el más relevante, es su veracidad. A resultas de lo cual los conceptos de *episteme* (verdad científica) y *doxa* (opinión) flotan juntos en una nube que no permite una diferenciación explícita de ambos. El argumento académico, las referencias y los criterios de autoridad para la construcción de discursos no tienen relevancia ante una opinión pública con escasa capacidad de discriminación y poco tiempo para documentarse, que busca emoción a la hora de informarse más que veracidad y a la que no le gusta ser contradicha.

La democracia, o más bien la extensión del igualitarismo implícito a la ciudadanía a ámbitos inapropiados, es en parte la causa de ello. No todas las opiniones valen lo mismo en todos los casos y en todos los ambientes. Las redes sociales son espacios en los que los usuarios encuentran una relativa homogeneidad y, por ello, las ideas y creencias se igualan, se amplifican y se refuerzan con independencia de los factores que concurren en las personas y su calidad académica.

Las sociedades del siglo xxi consumen grandes cantidades de información y lo hacen de un modo relacional, dicho sea de paso, como lo han hecho siempre; esto es, sus fuentes se encuentran condicionadas por lo que hace su entorno más próximo al que se dota de veracidad. El receptor se convierte en emisor, generándose una cadena de distribución que determina que la información recibida disponga de un gran nivel de credibilidad. En la era de la información, tanto las tecnologías para la edición como la distribución de la información lo hacen todo más fácil. El escenario informativo se ha hecho más complejo, pero también mucho más potente.

Además, los algoritmos de los buscadores de las redes sociales —los algoritmos son conjuntos de reglas para realizar operaciones— no son neutrales toda vez que trabajan sobre la base de búsquedas personalizadas basadas en las preferencias demostradas anteriormente; como resultado, el algoritmo selecciona información que cree que agradará al individuo y le evita aquello que no lo hace, con independencia de su relevancia científica.

⁴⁵ GOTTFRIED, Jeffrey; SHEARER, Elisa. *News use across social media platforms* [en línea], Pew Research Centre & Knight Foundation, s.f. Disponible en web: <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>.

⁴⁶ ALANDETE, David. *Cómo combatir la posverdad*, s.l.: Diario El País, 22 noviembre 2016.

Es el *microtargeting* una técnica basada en algoritmos estadísticos que analiza, individualiza y agrupa a los usuarios según los deseos, creencias o expectativas manifestadas por estos, y ofrece de modo acorde bienes, objetos o servicios. Esto genera una clasificación homófila que agrupa a las personas que piensan igual. El *microtargeting* domina las comunicaciones; la aceptación de una información falsa asegura la llegada de otras nuevas que incrementarán la distorsión cognitiva⁴⁷. Como apuntaba Churchill, «nosotros definimos nuestros algoritmos; por tanto, ellos nos definen a nosotros».

De este modo, la combinación de la globalización y la democratización digital ha generado una suerte de tribalismo emocional, esto es, de grupos identitarios de libre adscripción que son dinamizados y generan a veces una suerte de derivas sumamente peligrosas. La realidad se configura así como un mosaico, un retorno al mundo del Alto Medioevo que se produce en la era de la globalización. Al mismo tiempo, sistemas operativos más simples acceden a gran cantidad de fuentes externas y, utilizando lógicas descriptivas, las reordenan, logran conclusiones y aprenden de ellas, de modo que cambian los procedimientos. Son el germen de la llamada *Web 3.0*, la web inteligente⁴⁸.

De esta manera realimentan el pensamiento polarizándolo naturalmente hacia los extremos, generando filtro burbujas (la *filter bubble*, como las denomina Eli Pariser) que contribuyen aún más a la fragmentación de la sociedad, a su atomización, a reductos ideológicos y culturales, a los que se llega a llamar «cámaras de eco». El grupo se coordina cognitivamente, comparte y refuerza sus creencias sin discutirlos; fuera del grupo se siente miedo, lo que dificulta aún más poder modificar la opinión en un ambiente de perenne unanimidad⁴⁹.

Esto enlaza con los imaginarios en cuanto que herramientas de construcción, de «creación de realidades». Estamos a la postre ante un proceso social de afirmación de la identidad. Se trata de construir una identidad colectiva en la que los miembros del grupo se identifiquen, se sientan seguros y tengan un sentimiento de permanencia y estabilidad⁵⁰.

Así, y según un arcano instinto coalicional, se crean clústeres de individuos, auténticos enjambres sobre la base de informaciones acomodaticias que ratifican entre sí sus creencias mientras rechazan los datos no concurrentes con sus ideas; los datos reciben de este modo el mismo tratamiento que las

⁴⁷ MANRIQUE, José Luis. «Populismo y posverdad, ¿Solo tendencias?», en *Revista Inmanencia* [en línea], vol. 5, n.º 1. 2016. Disponible en web: <http://ppct.caicyt.gov.ar/index.php/inmanencia/article/view/10831>.

⁴⁸ Ibídem.

⁴⁹ ABRAHAM FERNÁNDEZ, Jesús. *Algoritmos, las nuevas armas de ¿construcción?* Masiva, s.l.: Instituto Español de Estudios Estratégicos, DIEEE junio 2017.

⁵⁰ ARRANZ MARTÍNEZ, Raquel. *La creación de imaginarios*. Documento de investigación del IEEE, 2018.

opiniones, descartándose subjetivamente aquellos que no se comparten o disgustan sobre la base de esa sola razón⁵¹.

Es la idea de Žižek, que distingue entre globalización y universalización, de modo que en el nuevo orden mundial se encuentra un retorno al Medievo: «El atisbo de verdad de esta comparación está en el hecho de que el nuevo orden mundial es, como el Medievo, global pero no universal en la medida en que el nuevo ORDEN planetario prende [*sic*] que cada parte ocupe el lugar que se le asigne»⁵². La globalización es, de este modo, opuesta a la universalización.

La verdad es también un espacio de moralidad y cada uno puede, teóricamente, tener la suya propia sin que tal cosa pueda o deba tener incidencia, siempre y cuando se dé cumplimiento al marco normativo vigente. En cualquier caso, la vocación integradora de toda sociedad exige la existencia de espacios comunes de verdad, lo cual trae como derivada que la fractura de la verdad provoque, a la postre, la fractura de la sociedad.

Esto conceptualmente hace que debamos retrotraernos nada menos que al juicio de Tomas Moro en el Palacio de Westminster, cuando reclamaba su derecho a pensar lo que quisiera, hecho este que acabó por costarle la cabeza. La libertad de pensamiento, el principal valor, el eje desde el que Occidente construye su discurso, no es un producto eterno, sino el fruto de toda una evolución. Su formulación se produjo durante la Ilustración; antes no era sencillamente concebible, procediendo su planteamiento al célebre juicio de Moro. Pero es que sus raíces están en el “cogito ergo sum” de Descartes, en la duda como metodología. Y esa duda arranca de la tradición de desconfianza y suspicacia, griega y romana que construyeron su sistema institucional como un juego de balances y contrapesos: dos Cónsules, las dos ciudades de San Agustín, las dos espadas (la del Emperador y la del Papa), Montesquieu, la división de poderes... La isonomía y la isogoría, la igualdad ante la Ley y la igualdad en el uso de la palabra, en los derechos políticos, devienen connaturalmente también de esos tiempos.

Occidente no es tanto la libertad como la duda. Occidente es la civilización de la duda, una civilización que desconfía de todo e incluso de sí misma; sobre la duda se construye la tolerancia, porque una persona que duda tiende más a tolerar a otros que no piensan como él. La tolerancia incorpora aún un componente asimétrico que tiende a desaparecer con la igualdad, y de ahí llega por desarrollo natural la libertad. La posverdad estimula la duda artificialmente, más allá de lo razonable y movida por un interés sino ilegítimo si oculto, lo que hace que pueda venir a ser un ataque en toda regla.

⁵¹ GONZÁLEZ-RIVERA, Juliana. «La información en la era de la *posverdad*: retos, mea culpas y antidotos» [en línea], en Universidad EAFIT. Disponible en web: <http://www.eafit.edu.co/medios/eleafitense/112/Paginas/informacion-posverdad.aspx>.

⁵² ŽIŽEK, Slavoj. *En defensa de la intolerancia* [en línea]. Disponible en web: http://estafeta-gabrielpulecio.blogspot.com.es/2009/03/slavoj-zizek-en-defensa-de-la_4989.html.

Al golpearnos en la duda utilizando para más ende los códigos axiológicos sobre los que se construyen las sociedades, se nos pone frente a nuestras propias contradicciones internas que todo sistema llevado al límite incorpora, porque los sistemas están contruidos sobre equilibrios que se visualizan y hacen dudar del modelo ético - que también se ve atacado - que sirve a la legitimidad del conjunto. Como afirmaba Stanislav Levchenko, alto funcionario del KGB, “busca tus vulnerabilidades y allí encontrarás el KGB”⁵³.

Uno de los grandes debates que se plantean se sitúa en que es y que no es información, algo cuyo volumen se ha hiperacentuado los últimos años. Información y opinión son y deben ser cosas distintas. Primero hay que informar, después y en su caso, opinar pero nunca mezclar ambos conceptos, pues el resultado es la pérdida de toda referencia y la distorsión y, con ello, la desinformación⁵⁴.

Fruto de su naturaleza mixta (empresa y servicio público), los medios de comunicación difunden, a un mismo tiempo, hechos e ideas con fines informativos, publicitarios, propagandísticos y hasta lúdicos, no pocas veces al mismo tiempo. La información aporta hechos analizados. La publicidad reposiciona un producto en el mercado y lo inserta con vistas a su toma en consideración y a modificar la conducta del individuo, y la propaganda selecciona o censura hechos y argumentos con criterio dogmático para sustentar las opiniones que promueve. Al presentarse todo esto como un conjunto y de un modo indisociado, se produce una confusión de términos que se añade a lo que ya de por sí figura en el conjunto del sistema⁵⁵.

Los medios de comunicación son uno de los pilares de Occidente, el cuarto poder, en la medida en que supone un mecanismo de vigilancia del conjunto relativamente independiente y que genera un nuevo equilibrio dentro del sistema de balances y contrapesos del modelo institucional democrático. Su pluralidad y diversidad sirven a la calidad democrática del conjunto. No obstante, surgen contradicciones al haber quienes se sirven de la normativa existente, instrumentando antinaturalmente sus oquedades y fisuras, para sus propios fines.

Así, por ejemplo, aparecerán grandes grupos y corporaciones ligadas no pocas veces a intereses estatales y con una gran capacidad de influencia que utilizan la ausencia de fronteras eficaces para activar, estimular o reformular las narrativas existentes o para llevar a cabo políticas de desinformación concurrentes con sus intereses específicos, ubicados en debilitar a las so-

⁵³ MILOSEVICH-JUARISTI, Mira. *El poder de la influencia rusa: la desinformación*. Real Instituto Elcano. ARI 7/2017 - 20 enero 2017.

⁵⁴ VERA, José Antonio. “Le llaman *posverdad* lo que no es sino manipulación y propaganda.” Discurso durante la entrega de los XXXIV Premios Internacionales de Periodismo Rey de España.

⁵⁵ MANRIQUE, José Luis. *Op. cit.*, s.p.

ciudades que los acogen. Esto supondrá una posibilidad directa de injerencia en los asuntos internos de terceros y una amenaza a la soberanía. El desarrollo del posibilismo a través de políticas de influencia tendrá un peso cada vez mayor que deberá ser contrarrestado.

Ello obliga a la adopción de fórmulas estables que sirvan a una conciliación entre la libertad de información y seguridad en el marco cultural y democrático frente a los desafíos que las dinámicas tecnológicas aplicadas a las redes sociales van a generar. Y no son cuestiones menores toda vez que su regulación afecta al acervo de Occidente y tensionan el sistema.

Los medios, por su parte, tienen una debilidad ante los patrocinadores y el poder político, toda vez que su actividad como empresas está orientada además de (o, incluso, antes que) por el servicio público por el beneficio. Así, por ejemplo, les interesa a veces más la viralidad o el llegar primero a la información que la verdad o la calidad⁵⁶.

Fruto de ello, y con la competencia de las redes sociales y los diferentes distribuidores de contenido, los medios han visto reducirse las audiencias y han debido digitalizarse también, lo que les coloca al mismo nivel que otros medios de información. Resultado de la aplicación de los criterios de eficiencia, los grandes periodistas y las grandes firmas han dejado de ser rentables puesto que ha de competir con el llamado «periodismo cívico» o «periodismo 3.0», centrado en blogs y páginas web autónomas. Esto, aplicando las leyes del mercado, a la postre redundará en la calidad del periodista y, por ende, del periodismo.

Y es que el periodismo tradicional se ha desdibujado en un mundo sin referencias ni una medición adecuada de la calidad, pasando a depender cada vez más de los contenidos de las redes sociales. Estas, simultáneamente y al mismo nivel que el bien intencionado «periodismo ciudadano», se han visto ocupadas por factorías de la desinformación que, de este modo y presentándose como una fuente alternativa más, han visto facilitada la inyección de su producto en la comunidad informativa.

En el ámbito digital, por su parte, se ha producido una importante concentración de empresas, dando cumplimiento a la admonición de Berners-Lee que, desde un principio, advirtió de la posibilidad de que el vasto espacio virtual podría ser cercado y loteado por un oligopolio de compañías digitales. Y es esto precisamente lo que está pasando⁵⁷. El acrónimo GAFA designa a las compañías Google, Amazon, Facebook y Apple, los emporios dominantes de la era digital: el 80% de las búsquedas se hacen por Google; Amazon con-

⁵⁶ KRAUS, Arnoldo. «Posverdad», en *Diario el Universal* [en línea], [ref. 15 enero 2017]. Disponible en web: <http://www.eluniversal.com.mx/entrada-de-opinion/articulo/arnoldo-kraus/nacion/2017/01/15/posverdad>.

⁵⁷ MERCHAN GABALDON; Faustino. «Verdad frente a posverdad», en *La Tribuna del País Vasco* [ref. de 2 diciembre 2017].

trola el 40% de las compras en línea, y una tercera parte de la humanidad está en Facebook. Estas compañías, además de vender productos, controlan las plataformas por las que otros venden los suyos. La Comisión Europea, por ejemplo, le impuso a Google una multa de 2700 millones de dólares por sesgar su motor de búsqueda a favor de sus propios servicios⁵⁸.

Tecnología y sociedad

No es casual que el fin de la Guerra Fría haya coincidido con la difusión de múltiples hallazgos tecnológicos que se produjeron en su contexto. Uno de ellos es, sin duda, Internet. La Red de redes surgió en ese periodo para garantizar el enlace y como un potenciador del conocimiento a través de la interconexión. Se esperaba que este se realimentase a sí mismo y generase efectos sinérgicos. Internet estaba llamado a ser el gran democratizador del conocimiento, el acelerador de la libertad y la solidaridad y, por tanto, la piedra angular de la globalización, además de un medio para que se llevase a cabo.

Y es que la expresión *International networks of computers*, apocopada Internet, describe a una red informática global, descentralizada, sustentada sobre la conexión entre ordenadores de una forma protocolizada, que en su versión web 1.0 surgió en los sesenta. El primer correo electrónico se envió en los setenta, y a este siguieron otras innumerables innovaciones que hicieron que los internautas abandonaran el papel de consumidores pasivos de información para transformarse en productores de contenidos. Reunidos en comunidades virtuales interactivas generaron las redes sociales, cuna de la web 2.0. A principios del siglo XXI, setenta millones de personas se enlazaban en la red. Su expansión ha sido imparable, multiplicándose su uso entre 2000 y 2017 un 976,4%: a finales de 2016, Facebook registraba 1800 millones, Youtube 1000, Instagram 500 y Twitter 350⁵⁹.

José Antonio Marina recuerda que Erich Schmidt, director de Google, afirmó en 2011 que la humanidad hasta 2003 había producido una cantidad equivalente a cinco exabytes de información, añadiendo a continuación que esa cifra se generaba ahora cada dos días. La revista Science calculó por su parte que, hasta 2007, la cifra era de 295 exabytes, que se había incrementado en 2011 a 600 exabytes⁶⁰.

Así, Internet es la base de la sociedad del conocimiento. Cumple los fines para los que fue concebida, en la medida en que se presentó como un instrumento incontrolable para la creación de una gran aldea global que trascen-

⁵⁸ Ibidem.

⁵⁹ MANRIQUE, José Luis. *Op. cit.*, s.p.

⁶⁰ MARINA, José Antonio. «Porque la sociedad de la información está a punto de fracasar», en *Diario El Confidencial*, 27 junio 2017.

diese distancias y cualquier tipo de barrera entre sus habitantes, por más que existiesen barreras a su desarrollo y se generasen problemas derivados de tal dependencia. En este sentido, la Estrategia Nacional de Seguridad publicada en 2017 nos recuerda que:

«El desarrollo de la tecnología es un instrumento de activación económica, crecimiento y progreso, pero también prueba la capacidad de adaptación de sociedades a los cambios tecnológicos... En gran medida, la tecnología ha premiado la interconectividad en detrimento de la seguridad. Así, actos como el robo, uso y difusión de la información y datos sensibles y acciones hostiles que incluyen actividades de desinformación e interferencias en procesos electorales representan hoy un desafío de grandes dimensiones tanto en lo que respecta a los Gobiernos como a los ciudadanos. Además de la conectividad de un mundo en red, que incluye el Internet de las cosas, la *inteligencia artificial*, la ingeniería genética y la robotización tendrán importantes implicaciones para la seguridad. Por eso, los esfuerzos para diseñar un sistema eficaz de gobernanza sobre las nuevas tecnologías serán clave para la Seguridad Nacional»⁶¹.

Hoy las redes sociales han convertido el ciberespacio en un gran archipiélago de islas del confort, si bien es cierto que esta fragmentación no es nueva y las burbujas han existido ya en la sociedad, de modo que lo único que se ha hecho es trasladarlas a Internet⁶².

Ciertamente, las posibilidades de las que dota la tecnología pueden hacer de cada persona un activista, pero también existen grupos organizados y orientados al logro de tales fines, a veces patrocinados o a la sombra de Estados, contruidos con grandes medios para el logro o las labores de apoyo a ciertos fines. Su trabajo, a escala industrial, se encuentra amplificado por miles de redes de bots (robots que actúan como si fuera personas), equipos o granjas de troles (simuladores de identidades) y sitios webs y redes sociales que amplifican la propaganda, un trabajo que, a su vez, se encuentra apoyado por redes de *hackers*. Un *malware* con un algoritmo puede estar recogiendo datos durante años para fragmentar un grupo y ejercer una influencia masiva de influencia, y todo ello con toda la complejidad que los grandes sistemas de desinformación disponen⁶³.

El fenómeno de retorno a un nuevo hombre se convierte en una paradoja llena de contradicciones, que se acentuará cada vez más con el desarrollo

⁶¹ Gobierno de España. *Estrategia de Seguridad Nacional 2017*. Presidencia del Gobierno, pp.36-37.

⁶² CARNICERO URABAYEN, Carlos. «Posverdad y redes sociales, una amenaza a la democracia», en *Diario Huffingtonpost*. [en línea], 17 septiembre 2017. Disponible en web: https://www.huffingtonpost.es/2017/09/17/posverdad-y-redes-sociales-una-amenaza-para-la-democracia_a_23063245/

⁶³ ABRAHAM FERNÁNDEZ, Jesús. *Op. cit.*, s.p.

tecnológico. Las narrativas —una herramienta sociológica que posibilita la influencia cuando no el control— vienen a ser un guion perfectamente estructurado por distintos agentes y desarrollado por una poderosa burocracia tecnológica, ligada o no a Estados, y que, en cualquier caso, trasciende sus fronteras y permite la injerencia directa. Una narrativa es una selección de ideas y referencias que hacen un uso instrumental del pasado al reconstruirlo conforme al imaginario que pretende alcanzar. Es un instrumento de persuasión política de extremada potencia que la tecnología acrecienta a través de su focalización.

Además, la mejora en los sistemas de comunicación referidos a la información permite tanto el acopio de datos como su tratamiento. De este modo, se posibilita un mayor control de los ciudadanos a los que, recíprocamente, se les ofrece la oportunidad de participar directamente en los asuntos del Estado.

No obstante, y recordando a Byung-Chul Han, «Una acumulación de información no puede generar la verdad»: la clave no está en los datos, sino en la comprensión de la información. Para paliar esto se dispone de herramientas como el *data mining* (o exploración de datos), con el que se intenta descubrir los patrones dotados de significado, esto es, la ley de los grandes números que les acompañan, la interconexión de los grandes conjuntos de datos⁶⁴, como un estudio de una revista norteamericana que acreditaba cómo las personas que sacaban a pasear a sus perros votaban mayoritariamente al partido demócrata.

Las conexiones imposibles revelan la naturaleza de las sociedades y sus elementos, esto es, las personas. La posible utilización de los datos de Facebook de cincuenta millones de personas en el contexto de las elecciones norteamericanas delata la necesidad de la regulación de un espacio que concede un poder tal a personas, empresas o instituciones aun de terceros países.

Las contradicciones son grandes. Hoy las grandes empresas comerciales como Alí Babá no tienen inventario, las grandes compañías de relaciones como Facebook no tienen contenidos, o las grandes compañías de taxis como Uber no tienen vehículos. Y aún se discute a qué sector pertenecen. Parece que todo se ha hecho posible para el hombre a través de la tecnología⁶⁵.

Esto genera importantes contradicciones. Thomas Friedman, en su libro *Gracias por llegar tarde*, detalla la paradoja de que el mundo actual necesita entre diez y quince años para comprender una nueva tecnología y redactar

⁶⁴ ORTEGA, Andrés. «Campañas de desinformación: la debilidad de la desconfianza», en Blog del Real Instituto Elcano [en línea]. 05 diciembre 2017. Disponible en web: <https://blog.realinstitutoelcano.org/campanas-desinformacion-debilidad-desconfianza/>.

⁶⁵ MERCHAN GABALDON, Faustino. «Verdad frente a posverdad», en *La Tribuna del País Vasco*, 2 diciembre 2017.

normativas para proteger a la sociedad, mientras las tecnologías desaparecen en un plazo de entre cinco y siete años. El mundo para este autor es plano y el futuro es posible, pero solo si superamos las múltiples tensiones implícitas en la era de las aceleraciones y se disminuye la velocidad; es preciso, por ello, atreverse a llegar tarde y a usar el tiempo para reimaginar el trabajo.

Marius Carol, utilizando este argumento y asociándolo al pensamiento de Eric Teller, un ejecutivo del laboratorio Google X de investigación, sostiene que el problema de esta situación es que podemos tener la sensación de haber perdido el control porque no somos capaces de adaptarnos al mundo a la velocidad que está cambiando: «Cuando nos hayamos acostumbrado al cambio, ese ya ni siquiera será el predominante y estaremos inmersos en otro nuevo». Es evidente que no se puede frenar el progreso tecnológico ni abandonar la regulación; lo que propone como alternativa es intentar aumentar la capacidad de adaptación de la sociedad. «Esa es la única manera de librarnos de la ansiedad que provoca la tecnología», añade. ¿Y eso cómo se hace? «Cuando la velocidad de cambio es tan rápida, la manera de conservar la capacidad de trabajar es dedicarse a estudiar toda la vida». ¿Y cómo se consigue? «Experimentando constantemente, revaluando normativas, innovando con ciclos más cortos. Por eso todo parece viejo desde que lo adquirimos»⁶⁶. El problema, como apunta José Antonio Marina, es que se está primando la innovación sobre el empleo de las tecnologías, con lo que su dinamismo se está volviendo autónomo. Estamos dentro de él y, sin embargo, no lo comprendemos; el proceso, consecuentemente, nos supera⁶⁷.

Las nuevas tecnologías tienen así un relevante papel en este marco: han dotado de una gran accesibilidad a la población. El relativismo entronca, como se ha visto, con la horizontalidad democrática, una suerte de isogoría que hace válida y respetable cualquier opinión. La realidad se hace variable y los conflictos, además de ser un choque de fuerzas, se transforman en un choque no solo de voluntades (la definición de Clausewitz de guerra), sino de percepciones y de realidades.

Como consecuencia, las nuevas tecnologías van a propiciar el desarrollo de dos tendencias sociales no necesariamente contrapuestas: una orientada hacia mayor democracia directa —las encuestas tienen un peso cada vez mayor en el desarrollo de la actividad política— al tiempo que también hace posible la recíproca; un mayor control del ciudadano por parte de los aparatos del Estado, y, consecuentemente, un mayor dirigismo tanto mediante el control directo como del indirecto, como por ejemplo y según

⁶⁶ CAROL, Marius. «Fracasar rápido», en *Editorial del Diario La Vanguardia*, 15 febrero 2018.

⁶⁷ MARINA, José Antonio «Porque la sociedad de la información está a punto de fracasar», en *Diario El Confidencial*, 27 de junio de 2017.

se ha visto, con la formulación de narrativas asociadas al empleo de *data mining*.

Estos dos movimientos —dirigismo y democracia directa— se suman en el populismo, que en nombre de la radicalidad democrática, es decir, de una democracia que no se somete a normas, se apela continuamente a la voluntad del pueblo como justificación y legitimación de cualquier conducta decidida por unos líderes que disponen de instrumentos sociológicos formulados en forma de constructos, como las narrativas, para el control de las masas humanas a las que dicen representar.

Tenemos, pues, que la tecnología confronta democracia representativa con democracia directa y dirigismo con libertad personal, habiéndose de encontrar una conciliación entre todos estos puntos. El papel de los populismos, un concepto de raíces emocionales, se torna así relevante.

Por otra parte, la tecnología propicia el mutuo y directo conocimiento, lo que trae consigo una igualación de las relaciones, que se desarrollan de un modo más horizontal. El modelo de liderazgo deja de ser carismático, pues el carisma puede mantenerse mientras exista una cierta distancia entre el líder y sus seguidores, distancia que las nuevas tecnologías reducen para primar el ejemplo y, con ello, el liderazgo transformacional.

El siglo xxi es el siglo de la horizontalidad, y el liderazgo transformacional favorece vía el ejemplo este tipo de aproximación; se cumple así la admonición de Jack Welch CEO de la empresa General Electric, en el sentido de la tendencia a la desaparición de los niveles intermedios de decisión en las organizaciones y a la adopción de los esquemas organizativos horizontales y propios de una orquesta. Consecuentemente, las organizaciones se van ahuecando mientras desaparecen los niveles jerárquicos y ganan en horizontalidad, quedando consignadas en el largo plazo como una orquesta a las órdenes directas de su director.

La seguridad es una necesidad sensible de unas sociedades que cada vez incorporan estándares más altos y demandantes, lo que se materializa mediante la introducción de conceptos nuevos que, de esta forma, quedan securitizados. La tecnología (como los elementos ciber) es el elemento transversal que los liga y, por tanto, uno de los factores principales a proteger. La preocupación por un fenómeno como la *posverdad* obedece a esta misma lógica.

En este contexto, la burocracia tecnológica propicia el rearme de las sociedades, lo que se ha traducido en un creciente incremento de la inversión en I+D orientado a la seguridad y la defensa, especialmente en el ámbito de la ciberseguridad (la ciberseguridad es un factor transversal). Pero el elemento decisivo para su logro es la educación de la ciudadanía. La fortaleza de una sociedad dependerá de la fortaleza de sus ciudadanos y esta de su adecuada preparación.

Verdad, emoción y razón

En el postmaterialismo, la materia y la realidad se diluyen hasta desaparecer; dependen en todo de la voluntad que la interpreta. Jean Baudrillard llega a hablar inclusive de un «asesinato de la realidad». El presente y el culto al modo posibilitan el discurso performativo: la sola voluntad expresada, por irreal que pueda resultar, es fundacional y diseña el futuro y las declaraciones intentan ser profecías autocumplidas. Algo existe o es de un cierto modo simplemente por afirmarlo, y si no más adelante se dirá otra cosa y ese será otro momento; la sociedad posmoderna, una sociedad que vive en esos códigos, lo entiende y no lo penaliza. Eso se apoya además en palabras sin límites precisos o que se desplazan a conveniencia.

Por eso su expresión cuida la forma más que el fondo, impregnada esta de un relativismo que no admite una verdad única, sino diferentes verdades, en algunos casos hasta personalizadas. Como apuntaba Nietzsche «no existen hechos, solo interpretaciones», es decir, lo importante no es el hecho en sí tanto como la opinión que se tiene del mismo.

Es la metafísica positivista la que lleva a pensar que las verdades sociales son universales y pueden presentarse como naturales, es decir, que no es tan importante la coincidencia con el hecho objetivo como el consenso del grupo sobre este. Los jugadores, en función de su número y cualificación, pueden cambiar las reglas de la partida y, con ello, el criterio de verdad. En las palabras de Luigi Pirandello que sirven para titular una de sus obras, *Así es (si así os parece)*, el resultado no es que no exista la verdad, sino que existen muchas, más o menos sólidas o discutibles.

En este contexto, la verdad pierde su definición aristotélica, que la sitúa como una correspondencia entre la realidad y el pensamiento, esto es, a un juicio que reflejará la objetividad de lo real. Como consecuencia, pasa así a convertirse en un término polisémico. La verdad epistemológica está contenida en juicios afirmados como realidades y que se corresponden con los hechos; la verdad científica es el máximo exponente de la lógica y es la máxima manifestación de la objetividad; la verdad de las ciencias fácticas es, en contraste, una certidumbre que se prolonga mientras no se demuestre otra cosa⁶⁸.

La verdad se convierte así en una referencia en un mundo que no las tiene, y obliga a quien la encuentra a abandonar la zona de confort para tomarla en consideración. Por eso se hace incómoda, cuestiona nuestras emociones, las reta. El conflicto surge cuando se reclama revisión de los principios. Cambiar demanda un esfuerzo y coraje para admitir el error, y el revisionismo desagrada, por eso la contradicción es silenciada.

Por eso también queda emocionalmente asociada a las «malas noticias», pues perturba y altera el cauce de las emociones propias, por lo que en lugar

⁶⁸ MANRIQUE, José Luis. *Op. cit.*, s.p.

de mirar hacia los hechos se produce un distanciamiento de la verdad. Pero sin la verdad, sin atender a la realidad, no es posible el consenso y se fractura la comunidad. Y es que las personas necesitan referencias.

Fórmulas como el intuicionismo facilitan liberarse de la verdad, con el cual se rellenan los huecos de información según la lógica vigente; o la «preferencia adaptativa», que consiste en reinterpretar los hechos que refutan una tendencia con el propósito de mantenerla. De este modo, el saber se congela y la ciencia se degrada⁶⁹.

Daniel Kahneman, en su obra *Pensar rápido, pensar despacio*, habla de dos modelos de pensamiento. El primero, rápido, intuitivo y emocional, una suerte de lo que los griegos denominaban *frónesis* (inteligencia práctica); es el que se utiliza para la resolución de los asuntos corrientes, pese a que incorpora errores y sesgos considerados aceptables. Y un segundo sistema lento, deliberativo y lógico, que no es instintivo pero que es la base de la ciencia y el pensamiento crítico. El primer sistema es el que prevalece y con él las primeras impresiones de nuestro razonar. Por ellas entra el engaño, la apariencia emocional de realidad, nuestros deseos y premoniciones.

En cualquier caso, no puede olvidarse que no somos espíritus puros: cualquier decisión surge de los sentimientos, de lo irracional, para alcanzar luego forma y coherencia en la razón. Primero sentimos e intuimos y después decidimos y actuamos. Como señala Buyng-Chul Han, «El sentimiento precede al pensamiento»⁷⁰; la música precede a la palabra, porque cualquier decisión racional debe pasar por el tamiz emocional del ser humano, al ser este una totalidad indiferenciable. El romanticismo es eso.

Lo emocional acaba así por primar sobre lo racional en una suerte de actitud antivictoriana, de revancha sobre el racionalismo cartesiano, que ha sido hasta ahora el eje de Occidente. La verdad no queda consignada al hecho, sino a los sentimientos que suscita o a las adhesiones que provoca. La emoción se sitúa por encima de la razón. En la era de la tecnología, paradójicamente, pues ha permitido su logro, la razón deja de ser la piedra angular del conocimiento. El hombre está definitivamente ya de vuelta de todo.

Esto no es sino una reedición del pensamiento de Nietzsche. Este ya apostaba por el instinto —y la irracionalidad que comporta— como el criterio definitivo de verdad. El resultado implica, a su vez, una reformulación de la máxima cartesiana que queda como «siento, luego existo», y hasta permite practicar una geopolítica de los sentimientos en forma de identidades volátiles de todo tipo y escala, accesibles solo por el mero hecho de sentir las. Eso, a su vez, conduce necesariamente una vez más a un refuerzo de la actitud

⁶⁹ FICHTENTREI FUENTE, Daniel. «Posverdad: la ciencia y sus demonios», en *Revista electrónica Intramed*. [en línea]. 2 mayo 2017. Disponible en web: <http://www.intramed.net/contenido.asp?contenidoID=90809>.

⁷⁰ BUYNG-CHUL, Han. *La sociedad del Cansancio*. S.I. Ed. Herder, 2012.

descreída. La realidad —una palabra que Novokov sostenía que debía encontrarse entrecomillada para poder significar algo— se transforma en una cuestión variable y discutible que depende no solo del punto de vista del observador, sino también de sus emociones y constructos mentales. La verdad se licúa entre el relativismo y la subjetividad.

La realidad puede tener ciertas dosis de maleabilidad y de interpretación que no tienen ni los hechos ni los datos en los que cabe descomponerla. No obstante, puede deconstruirse y reconstruirse de una manera significativamente diferente. Estamos ante una manipulación que se encuentra en las raíces mismas de la *posverdad*, y ese es precisamente el problema. El subjetivismo extremo no reconoce las diferencias entre los hechos y los datos, las leyes y las reglas, los modelos y los retratos. Confunde el mapa con el territorio. Una idea, por el mero hecho de que sea aceptada por una comunidad, no es una idea cierta⁷¹.

La comunicación se hace espasmódica y tajante para fortalecer su carga emocional, con lo que acentúa el distanciamiento. Además, y como se ha apuntado, aunque la difusión de conocimientos es mayor, la calidad media de la información es inferior; no tienen referencias de las fuentes y, por tanto, sus afirmaciones no resultan contrastables. La clave se sitúa en su selección. Todo, la verdad y lo que no lo es, se encuentra en la red.

Antes los medios de comunicación hacían un cribado de la información que distribuían, verificando con rigor y criterio su procedencia, oportunidad y jerarquía; la información era más o menos pura, mientras la pluralidad de fuentes similares dotaba de mayor objetividad al conjunto del sistema, corrigiendo eventuales disfunciones. Ahora, en no pocas ocasiones, hacen de árbitro entre informaciones y desinformaciones en lugar de verificar los hechos y dar cobertura a aquellos cuya certidumbre ha quedado constatada.

Edward Bernays, famoso por haber introducido el concepto de relaciones públicas, con éxitos tan notables como la difusión del tabaquismo entre las mujeres en los años treinta del pasado siglo —los cigarrillos eran presentados como «antorchas de la libertad»—, escribía en su clásico *Propaganda*:

«La manipulación consciente e inteligente de los hábitos y opiniones organizados de las masas es un elemento de importancia en la sociedad democrática. Quienes manipulan este mecanismo oculto de la sociedad constituyen el gobierno invisible que detenta el verdadero poder que rige el destino de nuestro país. Quienes nos gobiernan, moldean nuestras mentes, definen nuestros gustos o nos sugieren nuestras ideas son en gran medida personas de las que nunca hemos oído hablar»⁷².

⁷¹ FICHTENTREI FUENTE, Daniel. *Op. cit.*, s.p.

⁷² BERNAYS Edward L., *Propaganda*. S.l.: Editorial Melusina, s.f., p.16.

La posverdad

Los tiempos que se presentan como nuevos incorporan su propio lenguaje y se acompañan de palabras surgidas *ad hoc*. No son conceptos ampulosos; son, realmente, las palabras de moda que buscan impactar en los diferentes rangos culturales: selfi, escrache, *vape*, ciclogénesis, emoticonos —algo que ahorra directamente decir una frase para hacer llegar el sentimiento— o, en el mundo académico, adjetivos como transversal. Una cosa parecida sucede con la guerra híbrida sustituta de la guerra asimétrica, a cuya reconfiguración y actualización contribuye por más que no sea otra cosa que una simple aplicación del concepto genérico de guerra. Como está escrito en el libro del Ecclesiastés, «a más palabras, más vanidad».

No obstante, tales conceptualizaciones son interesantes no tanto por su valor académico sino por su carácter de radiografía sociológica y hasta antropológica. No es que el lenguaje del momento sea insuficiente, sino que se pretende escenificar la mutación de la realidad con el recambio del lenguaje como forma de certificarlo. De hecho, su formulación nos describe algunas de las líneas maestras del presente. La palabra no es así solo un símbolo del cambio, sino una nueva definición de la realidad.

Los antecedentes de la palabra *posverdad* los encontramos en la trilogía de las distopías o ciencia ficción distópica (antítesis de la utopía) aparecidas en la primera mitad del siglo xx; son los trabajos de George Orwell 1984, de Aldous Huxley *Un mundo feliz* y de Ray Bradbury *Fahrenheit 451*. En ellos, y como *leitmotiv*, la verdad pierde toda su relevancia, con lo que los autores pasan a describir la lógica de mundos surgidos de paradigmas diferentes pero todos ellos instalados en la *posverdad*.

En *Un mundo feliz* Huxley aborda un mundo en el que la supresión de la diferencia y el control del pensamiento permitían la felicidad de la humanidad a costa de su banalización; la verdad resultaba banalizada por todo un océano de insignificancias que servían a la represión del conocimiento. La cruz cristiana era sustituida, como símbolo cuasi religioso, por la «T» del «modelo T», símbolo del taylorismo de Henry Ford, fundador de la legendaria marca de vehículos.

En 1984 Orwell presenta de la mano de Winston Smith, un trabajador del Ministerio de la Verdad —una institución encargada de «revisar» los textos publicados para hacer «ajustes» a los acontecimientos—, una sociedad británica dominada por un sistema de «colectivismo burocrático» y controlada por el Gran Hermano. En ella la verdad es ocultada, empleando para ello hasta una neolengua en la que los significados disminuyen y las emociones se amplían. Las palabras se encuentran erosionadas toda vez que lo que no se puede pensar no existe y, con ello, los espacios de pensamiento se reducen, el abanico perceptivo del lenguaje se achica y la comunicación se traslada a los afectos. Recordando el *Tractatus Logico-Philosophicus* de

Wittgenstein, «Los límites de mi lenguaje significan los límites de mi propio mundo».

Se trata no ya de evitar la crítica, sino también de evitar hasta el propio pensamiento. Así, «Guerra es paz, libertad es esclavitud, ignorancia es fuerza». Ha nacido el lenguaje orwelliano, un lenguaje que altera la realidad y que, como añadido, reduciendo el número de palabras, trata de minorar el marco de pensamiento. Ray Bradbury, por su parte, habla de un mundo en que los libros son perseguidos y las televisiones y los medios interactivos lo ocupan todo.

McLuhan, en los años sesenta, en su famoso trabajo *La aldea global*, entre otras cosas desplazaba el foco del contenido al continente, haciendo del medio el mensaje. Esto es (y como apunta Umberto Eco), no le preocupa al autor siquiera pensar si los argumentos eran verdad, lo importante era sencillamente que fueran. Lo que desde nuestro punto de vista podría parecer una contradicción, desde el suyo es simplemente presencia simultánea.

La idea de *posverdad* la formuló Steve Tesich en 1992 para significar que la sociedad, en los tiempos del *affaire* Irán-Contra, había decidido vivir en un tiempo posterior a la verdad y, por tanto, ajeno a ella. El primer uso del término en España se produce en 2003 de la mano de Luis Verdú en su obra *El prisionero de las 21:30*⁷³. En 2004, Ralph Keyes publicó el libro *La era de la posverdad: deshonestidad y decepción en la vida contemporánea*, contribuyendo a su definitiva instalación.

En 2010 apareció el término *política de la posverdad*, con el que se da carta de naturaleza a una cultura política en la que la política efectiva se ha desconectado definitivamente de la retórica que la acompaña. Los hechos no aparecen ya en el discurso público. El término *posverdad* anuncia, de por sí, una era posfactual con la sistematización y legitimación de una práctica. Cuestiones como el referéndum del Brexit o la elección de Donald Trump contribuyeron a que tomara, tras varios años, definitiva carta de naturaleza.

La palabra *posverdad*, un concepto flexible, inmediatamente después de ser definida comienza ya a ser un término banalizado —de hecho, la propia palabra banaliza el desenfoque, que es una forma de quitarle importancia y legitimarlo, lo que viene a ser su principal función—, y por ello se adivina que va a ser sustituido en breve por algún otro nuevo concepto anglosajón dotado de una singularidad específica —tal vez el nuevo término de moda sea el *fake news* reformulado como neologismo— que documentará fehacientemente que aquellos que lo usan están a la última.

⁷³ HUMBERTO RODRÍGUEZ, Luis, «¿Posverdad... o mentira?», en *Periódico Mirada 21*. Vitoria: Universidad Francisco de Vitoria [en línea], 29 diciembre 2017. Disponible en web: <http://mirada21.es/secciones/nacional/posverdad-o-mentira/>.

Al decir de Baudrillard: «El momento crucial se da en la transición desde unos signos que disimulan algo a unos signos que disimulan que no hay nada. Los primeros remiten a una teología de la verdad y del secreto [...] Los segundos inauguran la era de los simulacros»⁷⁴. Los simulacros son un fruto de la hibridación entre la realidad y la ficción, lo que hace que la ilusión no pueda ser completamente independiente. La *posverdad* no deja de ser, a lo sumo, un simulacro, un artefacto, en la medida en que no existe, toda vez que la verdad no puede superarse; detrás de la verdad no hay nada. La *posverdad* es un sofisma que oculta de este modo la naturaleza demagógica de sus atributos⁷⁵.

El mundo se ha hecho multireferencial, multidisciplinar y, a la vez, diverso. La subjetividad es inevitable en todo lo que el hombre hace, máxime cuando la globalización ha unido referencias culturales diferentes con soluciones válidas y eficaces en cada entorno sociológico; la objetividad pasa a presentarse como una quimera, algo relativo, cuando no como una falacia.

Por eso la *posverdad* se banaliza y se presenta como una lectura alternativa más de la realidad, como «hechos» o «realidades alternativas» infraponderadas, deliberadamente o no, en un mundo anegado por mares de datos y de informaciones y dotado de la misma naturaleza contraintuitiva que la ciencia; una relectura que se acomete desde claves nuevas o sobre la base de un diferente ángulo de aproximación, ocultando con ello la malicia que subyace en su deliberada creación.

Eso es lo que la diferencia de la alternatividad que encarna el pensamiento crítico con el que aspira a confundirse. La *posverdad* se ha diseñado y construido para empatizar. Como resultado, los hechos, la realidad, acaban contando menos en la conformación de la opinión pública que las apelaciones a las emociones o las creencias.

Por ello viene a ser un auténtico *ductus obliquus*⁷⁶, una idea emotiva que no refleja la realidad y con la que se trata de influir en la opinión pública. Se busca falsearla, transformar la percepción a partir de la manipulación de las emociones del colectivo: se resaltan unos factores y se ignoran otros mientras se confunden los términos de las afirmacio-

⁷⁴ BAUDRILLARD, Jean. *Cultura y simulacro*. S.L.: Editorial Kairos, 2004, p.18.

⁷⁵ MARTÍNEZ MURCIANO, Luis María, 2017. *El tiempo está después. Tiempo y simulacro como paradigmas del cine posmoderno* [en línea]. Trabajo de fin de Máster en guion, narrativa y creatividad audiovisual. Universidad de Sevilla, Facultad de Comunicación, Sevilla. Disponible en web: <https://idus.us.es/xmlui/bitstream/handle/11441/64927/TFM-LUIS%20MARIA%20MARTINEZ.pdf?sequence=1&isAllowed=y>.

⁷⁶ El *ductus obliquus* o la conducta oblicua puede presentarse como una combinación de un *ductus simulatus*, donde el hablante defiende el caso que apoya pero disfraza sus razones para apoyarlo, y un *ductus contrarius*, donde sutilmente persuade a su audiencia de precisamente lo contrario de lo que está diciendo.

nes⁷⁷. Recordando a Derrida, «La mentira no es algo que se oponga a la verdad, sino que se sitúa en su finalidad».

La *posverdad* sirve fundamentalmente para reafirmar la opinión del grupo en que se inserta, en la medida en que contribuye a asentar y solidificar ideas preestablecidas, prejuicios y clichés y provoca que se descarten los hechos. El resultado es la manipulación, la alienación y el aniquilamiento del pensamiento crítico al tiempo que golpea en las líneas de fractura de las sociedades para provocarlas primero, convulsionarlas después y desorientarlas finalmente. Con la *posverdad* se deconstruye, en su sentido derridiano, la verdad inicialmente y la sociedad como último estadio.

Los hechos objetivos influyen menos en la opinión pública que los llamamientos a la emoción. El infantilismo de la opinión pública del que deriva su mutabilidad es fruto de la combinación de una ausencia de responsabilidad, ya sea individual o colectiva —adolece de los defectos de todos los *global commons*, donde todos son responsables y nadie realmente lo es; esto permite cambiar radicalmente de parecer en muy poco tiempo, sin que nada pueda ser demandado al respecto—, de la falta de conocimiento de los asuntos públicos y de la primacía de la emoción. Como consecuencia, los datos reciben el mismo trato que las emociones, descartándose aquellos que generan desafecto.

La *posverdad*, como apuntaba Baudrillard⁷⁸, «No se trata ya de imitación ni de reiteración, incluso ni de parodia, sino de una suplantación de lo real por los signos de lo real». De ahí la dificultad de averiguar la exactitud de los hechos que tratan, derivada tanto de la falta de equilibrio en la presentación de la información como de la ausencia de credibilidad de las fuentes elegidas⁷⁹. Es por ello contingente, diversa, inestable, indeterminada, un conjunto de culturas desunidas o de interpretaciones que engendra un grado de escepticismo sobre la objetividad de la verdad, la historia y las normas⁸⁰.

Y es que el poder no se mide según el patrón de riqueza y el intercambio de bienes; de hecho no se da, no se intercambia, sino que se ejerce; no existe más que en acto y es «productor» de saber y de verdad⁸¹. Como decía Michael Foucault, «Estamos sometidos a la producción de la verdad desde el

⁷⁷ MANRIQUE, José Luis. *Op. cit.*, s.p.

⁷⁸ BAUDRILLARD, Jean. *Op. cit.*, p.11.

⁷⁹ MILOSEVICH-JUARISTI, Mira. *Op. cit.*, s.p.

⁸⁰ MARTÍNEZ MURCIANO, Luis María, 2017. *El tiempo está después. Tiempo y simulacro como paradigmas del cine posmoderno* [en línea]. Trabajo de fin de Máster en guión, narrativa y creatividad audiovisual. Universidad de Sevilla, Facultad de Comunicación, Sevilla. Disponible en web: <https://idus.us.es/xmlui/bitstream/handle/11441/64927/TFM-LUIS%20MARIA%20MARTINEZ.pdf?sequence=1&isAllowed=y>.

⁸¹ GARCÍA CANEIRO, José; VIDARTE, Francisco Javier. *Guerra y filosofía*. Valencia: Tirant Lo Blanch, s.f., p. 199.

poder y no podemos ejercitar el poder más que a través de la producción de la verdad»⁸².

Es decir, el que tiene el poder tiene la verdad y no es una cuestión menor, pues la recíproca también es cierta. La transformación de un concepto no verdadero en algo que lo es encarna la esencia de aquello que nos ocupa en cuanto ejercicio real del poder. La lucha por el significado de un término es, en el fondo, una lucha por el poder. Esto lo pondría Lewis Carroll en boca de Humpty Dumpty: «las cosas significan lo que yo quiero que signifiquen, ni más ni menos. El problema es —dijo Alicia— si usted puede hacer que las palabras signifiquen tantas cosas diferentes. El problema es —dijo Humpty Dumpty— saber quién es el que manda. Eso es todo»⁸³. En este sentido, Goering decía que él decidía quien era o no judío.

La verdad sitúa el fiel de la balanza el margen del peso de las partes, por lo que estas, especialmente los poderosos, no buscan la decisión de un tribunal que limita sus opciones. Por eso los grandes juicios de la historia han versado sobre su concepto, desde Sócrates a Thomas Moore (libertad de pensamiento) pasando por Jesucristo o la Junta de Valladolid (1550-51, el imperio se detuvo para estudiar la licitud de la Conquista).

El célebre diálogo entre Pilatos y Jesucristo desarrollado en el *Lithostrōtos* (λιθόστρωτος, ubicado hoy, parece ser, en un convento en plena Vía Dolorosa) fue un diálogo sostenido nada menos que por un funcionario público sobre la verdad y el poder⁸⁴, y tanto Sócrates como Jesucristo fueron ejecutados por «impiedad» en un tiempo de confusión y deriva.

Entonces, como ahora, la *posverdad* abandona cualquier escrúpulo con respecto a los hechos para poder así suscitar una reacción emocional. Se buscan emociones poderosas como el temor, la rabia, la hostilidad, lo que se obtiene de común simplificando y presentando una realidad en blanco y

⁸² FOUCAULT, Michael. «Curso del 14 de enero de 1976», en VV.AA. *Microfísica del poder*, Madrid: La Piqueta, 1979 p. 140.

⁸³ LEWIS, Carrol. *Alicia a través del espejo* [en línea]. Capítulo 6. Disponible en web: www.elaleph.com/libros.

⁸⁴ «Pilato volvió a entrar al Pretorio, y llamó a Jesús y le dijo: ¿Eres tú el Rey de los judíos? Jesús respondió: ¿Esto lo dices por tu cuenta, o porque otros te lo han dicho de mí? Pilato respondió: ¿Acaso soy yo judío? Tu nación y los principales sacerdotes te entregaron a mí. ¿Qué has hecho? Jesús respondió: Mi reino no es de este mundo. Si mi reino fuera de este mundo, entonces mis servidores pelearían para que yo no fuera entregado a los judíos; mas ahora mi reino no es de aquí. Pilato entonces le dijo: ¿Así que tú eres rey? Jesús respondió: Tú dices que soy rey. Para esto yo he nacido y para esto he venido al mundo, para dar testimonio de la verdad. Todo el que es de la verdad escucha mi voz. Pilato le preguntó: ¿Qué es la verdad? Entró de nuevo al Pretorio y dijo a Jesús: ¿De dónde eres tú? Pero Jesús no le dio respuesta. Pilato entonces le dijo: ¿A mí no me hablas? ¿No sabes que tengo autoridad para soltarte, y que tengo autoridad para crucificarte? Jesús respondió: Ninguna autoridad tendrías sobre mí si no se te hubiera dado de arriba; por eso el que me entregó a ti tiene mayor pecado».

negro para movilizar a la opinión pública. Y repetir, porque la política es, en esencia, repetición, pedagogía.

¿Por qué, si no todos sí muchos, hemos recibido mensajes que alertan sobre ataques terroristas en centros comerciales o elevaciones al nivel máximo del estado de alerta, por ejemplo? Se busca atentar contra el sentido de la seguridad de la sociedad. La *posverdad* es un colaje, al decir de Umberto Eco en su célebre prólogo a la obra de Orwell, un trampantojo que tiende a sucesivas posiciones eclécticas y hacia un cierto pragmatismo en la medida en que existe un reconocimiento de la realidad. No busca imponerse; los equilibrios que plantea son su victoria, pues esta se consolida en términos de influencia. Forma parte de una estrategia, es un medio que sirve a otros fines: con ella se alimentan las narrativas que manipulan sentimientos y alteran la realidad apelando a clichés y prejuicios mientras se socaba la facultad de discernir.

Los propios medios de comunicación, en pro de una falsa objetividad, quedan condicionados en sus juicios y obligados a otorgar el mismo espacio tanto a la verdad como a aquello que no lo es. Por eso en política obtiene mayor cobertura mediática quien se sirve de la *posverdad*, pues sus postulados y debates, a favor y en contra, le dan un papel de centralidad en el panorama mediático ofreciéndole réditos.

La *posverdad*, según Roger Bartra, se construye en cinco etapas: en la primera un sitio o persona difunde una información impactante; la noticia se difunde indiscriminadamente en redes sociales; por su impacto, los medios la retoman y la difunden por no quedar fuera del *trending* informativo; la noticia es desmentida, pero tal cosa no tiene el mismo impacto que la noticia; la aclaración no se vuelve viral y la noticia queda en la mente de algunos, lo cual hace que sea una verdad a medias⁸⁵.

Con las insinuaciones se actúa sobre la dimensión emocional construyéndose sobre ella e implícitamente desplazando al receptor hacia una realidad paralela. La gente no quiere pensar tanto como confirmar lo que ya piensa. Es la psicopolítica: una construcción política realizada sistemáticamente sobre la base de su componente irracional, esto es, desde el sobredimensionamiento del factor emocional, a partir de una expresión exacerbada de la dimensión emocional-identitaria que se utiliza como medio para hacer llegar un mensaje. La política fractura así a la sociedad, la muele para hacer posible poder someterla. Como decía Orwell, «*el poder está en la facultad de hacer pedazos los espíritus y volverlos a construir dándoles nuevas formas*»⁸⁶.

En este sentido, Dominique Moïsi, en su obra *Geopolítica de las emociones*, desarrolla el análisis de las entidades colectivas a través de la psicología, porque el mundo de la globalización solo puede entenderse a través de las

⁸⁵ ORTEGA, Octavio. *Op. cit.*, s.p.

⁸⁶ ORWELL, George. 1984. Barcelona: Editorial Destino, 1999, p. 261.

emociones de sus ciudadanos, sus aspiraciones y frustraciones más íntimas; lo irracional se haya presente en todo y no es posible obviarlo. El caos de la globalización trae de vuelta el concepto de identidad. De este modo, las fronteras emocionales pesan más que las fronteras de cualquier otra índole. La fragmentación, a su vez, hace más fácil la dominación mediática.

Moïsi concentra su trabajo en tres emociones sobre la base de su relación con la confianza: miedo (ausencia de confianza), esperanza (la expresión de la confianza) y humillación (la confianza herida), y con ellas articula el discurso. Estas emociones van a ser la raíz para la vehiculación de los mensajes, toda vez la accesibilidad al subconsciente que permiten.

Y la cosa puede llegar a los extremos de una PSYOPS (operación psicológica), de influencia y hasta de pura desinformación digital. La *posverdad* ha permitido el desarrollo de una estrategia: realizar vastas operaciones de influencia amparadas en los algoritmos y las redes.

Las *fake news* o noticias falsas

Desinformar es distribuir deliberadamente información falsa impidiendo o dificultando que la información correcta fluya hacia sus destinatarios. La desinformación (*deziformatsiya* en ruso) está diseñada para engañar y desorientar al oponente, perturbar su percepción de la realidad, influir en sus decisiones y socavar su eficiencia política, económica y militar. Se trata de una medida activa y por tanto agresiva que se sirve de la duda y la conciencia moral, ejes que sirven a la estructuración de las sociedades occidentales para atacar a estas. Subinformar es una parte de la desinformación que pasa por eliminar o apocar unas noticias y magnificar otras, amputarlas en su contenido o disminuir deliberadamente la importancia que tienen. Estamos ante formas de desmontar la verdad⁸⁷.

La desinformación afecta a los cimientos de la democracia al alterar su base, pues esta se sustenta sobre las decisiones pretendidamente libres e incondicionadas de los ciudadanos que, de este modo, se ven afectadas en los criterios para su adopción. Su relación con la *posverdad* es evidente. El mensaje que subyace en el fondo de todo es «no creas a nadie», o aun «no creas en nada»; se trata definitivamente de desestabilizar y desorientar.

Un concepto un tanto diferenciado de *posverdad*, y en el núcleo duro de la desinformación, son las llamadas *fake news* o noticias falsas. Se decía que la medicina era el arte de conducir a la muerte al enfermo «adornando el camino», con palabras griegas. Ese camino parece ser que se emprende ahora en inglés, el nuevo koiné. Este artificioso concepto, como también la propia idea de *posverdad*, es uno más de esos «espíritus que enturbian el agua para que parezca más profunda» que anunciaba Nietzsche.

⁸⁷ MILOSEVICH-JUARISTI, Mira. *Op. cit.*, s.p.

La novedad que encarna este término, que podríamos traducir en castellano claro como bulos (tal vez este término suene algo más vulgar y su mística sea inferior a las *fake news*), es que se abandona cualquier escrúpulo y lo que se pretende con él, directa y premeditadamente, es tanto engañar como influir en la conciencia emocional o manipular como se intenta desde la *posverdad* (que también). Hay así una separación más o menos tenue entre ambos conceptos, por más que el segundo englobe al primero; se encuentra referida al nivel de relación con la base real de la noticia, aunque la intencionalidad sea la misma.

Pero la creación de un término (volvemos de nuevo a lo que sucedía con la *posverdad*) viene a suponer una cierta legitimación de una práctica mediante su banalización. En un informe para la Comisión Europea, un grupo de expertos de alto nivel solicitaba que se abandonase toda vez que lo consideraba inadecuado, en la medida en que no explica la complejidad de la situación y genera confusión en los debates sobre la materia a todos los niveles⁸⁸.

Las razones de las llamadas *fake news* son variadas y van desde la manipulación o la extensión de cortinas de humo (generar ruido mediático para encubrir informaciones de mayor enjundia) al desprestigio de una institución hasta el puro beneficio económico. Y es que los clics se traducen en beneficio —por ejemplo, el que se obtiene ligado a la publicidad—, habiéndose detectado hasta una industria para su fabricación en lugares insospechados como el pueblo de Veles, en Macedonia.

Las *fake news* suponen una actividad que incorpora algún tipo de beneficio toda vez que su desarrollo es oneroso. No se hace un esfuerzo sin pretender beneficio. Para combatir las es imperativo, en primer término, comprender sus razones e identificar a la fuente que las ha estimulado. Como ya apuntaba Derrida, «Lo relevante en la mentira no es nunca su contenido, sino la finalidad del mentiroso».

Noticias falsas, bulos, han habido siempre en la historia de la humanidad. En eso no hay nada nuevo. La auténtica noticia es, en realidad, la facilidad y profundidad con que ahora penetran en la sociedad de la mano de las tecnologías de la información, las TIC, y el carácter masivo de ello. Las noticias falsas vienen a ser también una suerte de *jamming*, de perturbación intencionada, que eleva el nivel de ruido ambiente y dificulta que la información llegue a su destinatario real, y puede ser focalizada. La auténtica verdad queda escondida ante un cúmulo ingente de falsedades a las que es asimilada.

La desconfianza hacia esta, a su veracidad e intencionalidad, se traduce en desconfianza hacia el conjunto de la sociedad y afecta a su cohesión. Afecta también a las instituciones, a su credibilidad, pues vienen a ser uno de los

⁸⁸ WARDLE, Claire; KELIS NIELSEN, Rasmus; MANTZARLIS, Alexois; JIMÉNEZ CRUZ, Clara. «Seis puntos clave del informe sobre desinformación del Grupo de expertos de la Comisión Europea», en *Periódico El Diario* [en línea]. 12 marzo 2018.

blancos preferentes de sus ataques ya que son, o deben ser, la base que soporta el tejido social. Sirve pues, directamente y sin ambigüedades, a la deconstrucción de las sociedades.

Las personas con bajos niveles de preparación, los iletrados funcionales, son más vulnerables a este tipo de noticias, aunque no exclusivamente. Aun incluso cuando la información ya ha sido refutada, diversos estudios sociológicos aprecian un sesgo en el sentido pretendido por esta, hasta el punto de que no se puede deshacer la información incorrecta y esta adquiere una viralidad con la que la verdad no cuenta por resultar menos atractiva desde el punto de vista informativo; los desmentidos son esa parte que se denomina «epílogo» en el ciclo informativo en la que se sustancia la verdad y cuya relevancia mediática es escasa por su menor valor emocional y por aparecer por fuera de la ventana de interés mediático.

Pero todo esto es antiguo, si bien se ve renovado por todo el aparataje técnico que se ha desarrollado con vistas a su puesta en marcha. El ejemplo de la célebre aria *La calunnia*⁸⁹ del Barbero de Sevilla de Rosinni es una buena muestra.

⁸⁹ La calunnia è un venticello,
un'auretta assai gentile
che insensibile, sottile,
leggermente, dolcemente
incomincia,
incomincia a sussurrar
Piano piano, terra terra,
sottovoce, sibilando,
va scorrendo, va scorrendo
va ronzando, va ronzando;
nell'orecchie della gente
s'introduce,
s'introduce destramente,
e le teste ed i cervelli,
e le teste ed i cervelli fa stordire,
fa stordire e fa gonfiar.
Dalla bocca fuori uscendo
lo schiamazzo va crescendo
prende forza a poco a poco,
vola già di loco in loco;
sembra il tuono, la tempesta
che nel sen della foresta
va fischiando,
brontolando, e ti fa d'orror gelar.
Alla fin trabocca e scoppia,
si propaga, si raddoppia
e produce un'esplosione
come un colpo di cannone,
come un colpo di cannone.
Un tremuoto, un temporale,

La calumnia es un vientecillo,
una aurita así, gentil,
que imperceptible, sutil,
ligeramente, dulcemente,
comienza,
comienza a susurrar.
Bajo, bajo, a ras de tierra,
en voz baja, sibilante,
va corriendo, va corriendo,
va zumbando, va zumbando;
en las orejas de la gente
se introduce,
se introduce hábilmente
y las cabezas y los cerebros,
y las cabezas y los cerebros
hace aturdir y hace hinchar.
Una vez fuera de la boca
el alboroto va creciendo,
toma fuerza poco a poco
vuela ya de un lugar a otro;
parece un trueno, una tempestad
que en medio del bosque
va silbando,
atronando, y te hace de horror helar.
Al final se desborda y estalla,
se propaga, se redobla
y produce una explosión,
¡como un disparo de cañón!
¡como un disparo de cañón!
Un terremoto, un temporal,

La ausencia de una labor de cribado eficaz en las redes sociales hace que el usuario quede consignado como único juez de la veracidad de las noticias que se le hacen llegar, por más que no tenga ni la condición de experto ni acceso a fuentes ni herramientas útiles con vistas a su valoración.

Por el contrario, no pocas de estas noticias son auténticos productos de ingeniería social, construidas sobre retazos de realidad y elementos emocionales dirigidos a segmentos de la sociedad predispuestos a aceptarlos o a conmocionar y hacer dudar a aquellos que no lo están. Todo ello a través de piezas informativas amarillistas construidas deliberadamente para impactar y generar polémica, con las que se intenta afectar a la percepción del lector. Lo importante es centrar o descentrar el debate. Un estudio de la revista *Science*⁹⁰ de 2018 acreditaba que es el elemento humano, y no los bots, el principal responsable de la viralidad de las noticias falsas, y no puede resultarnos extraño, pues para eso han sido construidas.

Se busca para ello golpear en las líneas de fractura de la sociedad, en los intersticios sísmicos, provocando su polarización primero y su fragmentación después. Se trata, a la postre, nuevamente de romper la comunidad al inspirar desconfianza entre sus miembros. Como está escrito en la Biblia, «Un reino donde hay luchas internas va a la ruina; y una ciudad o una familia dividida no puede subsistir» (Mateo 12, 25).

Pretende servirse de periodos de tensionamiento, de polarización *per se*, como pueden ser los procesos electorales con vistas a conseguir lo anteriormente apuntado. En política no se trata tanto de apoyar a tal o cual candidato considerado más favorable, que también, sino, ante todo, cuestionar el marco, hacer dudar a la comunidad, resaltar las contradicciones e insuficiencias del sistema que la soporta, poner a este en tela de juicio, someterlo a presión y hacer dudar de las propias referencias. El marco de las elecciones, por la polarización y por poner de manifiesto la quiebra social, es sumamente propicio para ello.

El ataque contra Hillary Clinton en el contexto del proceso electoral norteamericano de 2016, por ejemplo, podía tener como objetivo no tanto promover

Un tumulto generale
che fa l'aria rimbombar!
E il meschino calunniato,
avvilito, calpestato,
sotto il pubblico flagello
per gran sorte ha crepar.
E il meschino calunniato,
avvilito, calpestato,
sotto il pubblico flagello
per gran sorte ha crepar.

un tumulto general
que hace agitar el aire.
Y el infeliz calumniado,
envilecido, aplastado,
bajo el azote público
podrá considerarse afortunado si muere.
Y el infeliz calumniado,
envilecido, aplastado,
bajo el azote público
podrá considerarse afortunado si muere.

⁹⁰ Vosoughi, Soroush; Roy, Deb; Aral, Sinan. «The Spread of true and false news on line», en *Science*. 9 marzo 2018. Vol. 359, Issue 6380, pp. 1146-1151. DOI: 10.1126/science.aap9559.

a su rival como fracturar la comunidad y atacar al marco, empañar la credibilidad de la democracia norteamericana y dañar a las instituciones que se sustentan sobre esta, debilitando, en cualquier caso, al futuro presidente norteamericano, que se convierte además en sospechoso.

Esto golpea directamente en la línea de fractura, en la juntura entre la sociedad y las instituciones que esta genera en un momento de acentuada debilidad. Es más, una de las consecuencias de la pérdida de calidad democrática iniciada con la crisis de las instituciones inherente a la posmodernidad es precisamente la relajación del sentido crítico por parte del ciudadano, que ya no jerarquiza, distingue o valora en términos racionales la veracidad del discurso público. Por eso son tan vulnerables.

De este modo, lo que sucede con las *fake news*, y con ello con todo el concepto de *posverdad* de las que, recordémoslo una vez más, estas vienen a ser parte, es que son un síntoma de un problema de mayor calado. Este, en algunos países, puede ser producto de la crisis de su modelo de ciudadanía materializado en forma de bajos estándares educativos, analfabetismo funcional y fragmentación social.

De hecho, en la nueva política, el relato convencional anclado antaño en una ideología que lo ligaba y explicaba todo ahora ha desaparecido. Los datos y las historias verificables, por más que interpretables, han sido sustituidas por unas narrativas fragmentadas sobre la base de una trama difusa y que se sirve de una lógica en blanco y negro para polarizar el espacio político y reafirmarse en temas que no son los pivotes efectivos de la política real y que pueden no tener nada que ver con ella⁹¹.

El nuevo relato está construido sobre el discurso corto e impactante (la lógica de caracteres de Twitter), la *posverdad*, y se traslada mediante un lenguaje emocional. Este sirve para interpelar a un ciudadano que, de partida, desconfía de las instituciones clásicas que considera periclitadas⁹². El discurso público se halla salpicado de lugares comunes, a los que parece que se ha de rendir necesariamente culto, y de elementos simbólicos, presentándose por ello deslavazado e incoherente, por más que, como es sabido, envuelva un plan de acción semiclandestino. De hecho, el prefijo *semi-* está en casi todo lo relacionado con el mundo posmoderno.

La pospolítica

La política de la *posverdad*, la *pospolítica*, según la bautizó Christian Salmon en 2007, conforme a esta lógica trata de crear o modelar la opinión pública

⁹¹ SARASQUETA, Gonzalo. «Pospolítica ¿autopsia o metamorfosis del relato? El caso de Donald Trump», en *Revista Especializada en periodismo y comunicación: Questión*. Universidad de Río de la Plata, vol. 1, n.º 57, 2018: Verano (enero-marzo).

⁹² *Ibidem*.

actuando más sobre las emociones y las creencias personales que sobre los hechos objetivos. Para ello utiliza preferentemente los sentimientos que Moïsi identificará en su relación con la confianza: miedo, esperanza y humillación. Los manipula para el logro de objetivos no explícitos, y con ellos golpea algunas de las líneas de fractura de la sociedad.

La *posverdad* se convierte en la savia de esta concepción de la política. Esta se sirve de las redes sociales, de una población con acceso a la información pero con tiempo limitado para su análisis, y aun sin la formación y capacidad de discriminación precisa para el mismo. La clave para su puesta en práctica es la ausencia de crítica por presentarse envuelta en el magma de la *posverdad* y por la propia ausencia de pensamiento crítico, amparada a corto, además, por la debilidad del periodismo.

El término *agitprop* (agitación y propaganda) era una estrategia política eficazmente utilizada durante la Revolución rusa. Surgió como un movimiento creado por artistas de la época para influir en la opinión pública en una doble vertiente: de un modo pasivo, sobre las conciencias con la propaganda, y de un modo activo, mediante la agitación⁹³.

Si pensadores como Chomsky o Derrida eran tradicionalmente definidos como «alternativos», ahora lo alternativo, precisamente, se ubica en el poder. Y eso resulta extraño o, cuanto menos, novedoso. El poder ahora, desde esta concepción de la política, hace *agitprop* y también es «alternativo». Sorprendente oxímoron.

Toda vez que la política se asienta sobre percepciones, el término *pospolítica* viene a describir la generalización y público reconocimiento (no se olvide ni se desprecie esta idea) de una práctica. Se trata de conectar con los sentimientos y emociones del público, con su condición vital, y de ahí, por camino inverso, llegar a su razón.

Estamos más que ante una novedad —esto, de hecho, en mayor o menor medida, siempre ha sido así— ante una sistematización, un modelo que se desarrolla con un reconocimiento público que la legitima, pues supone la aceptación de una práctica. Y en eso, precisamente, radica la autoridad, en el ejercicio legítimo del poder; la cuestión es que, por más que aceptada, supone una importante degradación de la democracia representativa desde el momento que, como resultado de la diglosia, se hurtan a la ciudadanía no ya los fines políticos alcanzados, sino la propia agenda política.

No obstante, eso no es muy diferente de la propuesta de Maquiavelo, una política que se asienta sobre el engaño. Como este escribía a Francesco Guccini en 1521, «Yo nunca digo todo lo que creo ni creo nunca lo que digo, y si se me

⁹³ LENOIR-GRAND PONS, Ricardo. «Cuando la información busca desestabilizar al enemigo», en *Revista On line La Grieta* [en línea]. 17 abril 2017. Disponible en web: <http://lagrietaonline.com/cuando-la-desinformacion-busca-desestabilizar-al-enemigo/>.

escapa alguna verdad de vez en cuando, la escondo entre tantas mentiras, que es difícil encontrarla», y apuntaba en su gran clásico: «Los hombres son tan simples y unidos a la necesidad que siempre el que quiere engañar encontrará a quien le permita ser engañado».

La percepción en política lo es todo. No en vano, Richelieu decía que «El disimulo es la ciencia de los reyes». Hasta el propio Max Weber sostenía que la veracidad no era de aplicación en la política. La política no ha sido nunca entendida como puro engaño, sino que el engaño era algo de lo que se podía servir la política para el logro de sus fines. Es más, entre la verdad y la política se establece una relación dialéctica toda vez que la política no puede ser completamente sierva de la verdad en la medida en que, como expresión de la realidad, aspira a cambiarla. La verdad viene a convertirse, por ello, en una herramienta más al servicio de la política. La diferencia con el momento actual es que las redes también cuentan con esa capacidad y la sociedad civil ha desbordado a través de ellas al Estado.

La manipulación se acomete desde las mismas raíces a través de la imposición del marco, de la fijación del lenguaje. El lenguaje hace posible el raciocinio, y sobre la verdad se construye la civilización y la democracia. La neolengua de la que se sirve la *posverdad*, el lenguaje orwelliano, puede escenificarse en los ciento cuarenta caracteres de Twitter, un lenguaje comprimido cuyo poder de concentración, acentuado aún más por el empleo de imágenes visuales, favorece el extremismo⁹⁴. Con ciento cuarenta caracteres se puede dar opinión, pero no hacer análisis, y en esos caracteres debe haber hueco para lo políticamente correcto, que ocupa un espacio no menor. La política, que es discurso, queda así sesgada por el poco espacio, que obliga a adjetivar llamativamente para captar al público, y ahuecada.

Además es un lenguaje dirigido, focalizado, hacia receptores concretos a través de poderosas herramientas que, como el *data mining*, permiten el estudio de tendencias y la determinación de blancos objetivos⁹⁵. Como apunta Baudrillard, «Vivimos en un mundo en el que la más elevada función del signo es hacer desaparecer la realidad y enmascarar al mismo tiempo esa desaparición»⁹⁶.

Twitter, a su vez, hace válido el liderazgo tipo director de orquesta que describíamos como característico del siglo XXI. Este, recordemos, permite al líder entrar en contacto directo con sus seguidores sin intermediaciones, transmitiéndoles la esencia de su discurso.

⁹⁴ LENOIR-GRAND PONS, Ricardo. *Op. cit.*, s.p.

⁹⁵ FERNANDO JUAN, José. «7 apuntes sobre la *posverdad* en las redes sociales», en *Revista Entre paréntesis*. 19 diciembre 2016. Disponible en web: <http://entreparesis.org/posverdad-en-redes-sociales/>.

⁹⁶ BAUDRILLARD, Jean. *El crimen perfecto*. S.L.: Editorial Anagrama, 1997, p. 17.

Se trata de fijar una relación directa y emocional con el ciudadano sobre la base de una política expresiva. De este modo, la teatralización y personalización del líder político le transforman en una suerte de presentador o conductor, situándole en un universo distinto de los hechos que detalla, sea parte de ellos o no. De este modo, se transforma en la figura del teatro grecorromano del *Deus ex machina*: trasciende los parámetros que vienen a definir la realidad; es más, se transforma en un adalid de la voluntad popular en su lucha contra el sistema de balances y contrapesos característico del modelo democrático en la medida en que este, repudiado como obsoleto e ineficaz, limita su capacidad para la renovación.

El estilo disruptivo que algunos de los nuevos comunicadores políticos despliegan genera una narrativa inédita que encaja parcialmente con el andamiaje clásico del relato, en la medida en que enlaza ideas inconexas sin tener en cuenta su veracidad o verosimilitud. A la carga emocional intrínseca a los mismos, y sobre la base de un guion binario —una lectura de la situación en clave de buenos y malos, justo o injusto— se aplica una tensión narrativa, la agonía del teatro, con la que se desafía el modelo político vigente por caduco y corrupto. El líder pospolítico queda consignado en este escenario como un elemento catárquico en la voz del pueblo.

El *storytelling* (la narrativa) es una comunicación estructurada, toda una unidad de acción con la que se apela a los sentidos y emociones mientras se aporta una verdad que orienta el conjunto. La carga emocional de los relatos capta mejor la atención que la simple información, haciendo que pueda aprenderse el sentido que la elección de acontecimientos, reales o ficticios, pretende imprimir. El miedo o la ironía reemplazan a los datos y la coherencia del conjunto facilita la penetración en una sociedad de conceptos débiles que se funden ante ella como el hielo en un día templado⁹⁷. Como apunta Roger Bartra, además hay mucha información que fluye como entretenimiento, lo que la deriva hacia áreas en las que no predomina la reflexión y facilita de este modo, una vez más, su penetración⁹⁸.

La hiperfragmentación, los saltos narrativos y la presencia de grandes comunicadores como el presidente norteamericano Donald Trump quedan conexados y adquieren un sentido como parte de ella, de modo que empalman con una sociedad ligera y caracterizada sociológicamente por un alto proceso de desideologización y una profunda crisis de las instituciones que la soportan junto con un escepticismo transversal a todos los estratos sociales⁹⁹.

Los valores, sentimientos y emociones funcionan como envoltorios de los mensajes y aseguran un impacto facilitado por el *shock* que provoca el len-

⁹⁷ SARASQUETA, Gonzalo. *Op. cit.*, s.p.

⁹⁸ ORTEGA, Octavio. *Op. cit.*, s.p.

⁹⁹ SARASQUETA, Gonzalo. *Op. cit.*, s.p.

guaje emocional. Se pasa de un tema a otro, dentro de un espectro reducido de ellos, mediante una suerte de trazos, un esbozo característico de la técnica pictórica expresionista que deja a la imaginación del espectador rellenar los huecos. Esto es, se efectúa un microrrelato para que la composición final, ya en clave macro, la haga el votante, posicionándose sobre uno de los extremos del tema abordado, como se pretendía¹⁰⁰.

Son discursos muy focalizados y dirigidos hacia ciertos sectores considerados estratégicos, al tiempo que se rechaza abiertamente encontrar caladeros en otros por los costos del proceso y para marcar aún más el propio discurso. El coste es, nuevamente, una mayor fragmentación de la sociedad contrapuesta a la voluntad inherentemente inclusiva de la democracia.

Utilizan, además, lo que se conoce como *dog whistle policy* para llamar a terceros, es decir, una suerte de metáforas con las que se alude y critica a otros grupos sin explicitar tal cosa. Así se habla de la droga o de los problemas en el centro de las ciudades para evitar formulaciones racistas pese a que se encuentran implícitas al racionamiento o se señalan referencias a la diferencia como formas para evitar el impopular supremacismo inherente al discurso nacionalista extremo.

Los votantes se ven transformados en mera audiencia al habérseles hurtado el debate y con ello la soberanía. Y es que, en esta concepción de la política, el debate racional es sustituido por un discurso emocional en el que se elimina toda huella que descubra un ideario que yace oculto y que puede encontrarse realmente formulado por especialistas. Es decir, existe discurso pero este ni encaja con ninguna ideología concreta (sus fronteras se disuelven y no se aceptan sus explicaciones) ni, sobre todo, se presenta¹⁰¹.

Las emociones son la base del relato mientras la política se escenifica como espectáculo. Lo real, lo objetivo y lo racional son innecesarios para interperlar políticamente. La credibilidad no es relevante, sino un impedimento para la visibilidad. El *shock*, la inventiva y la espectacularización, por el contrario, sí lo son. El líder queda así constituido en un nuevo «conducator» en el marco de un sistema de balances y contrapesos que rechaza tales figuras y flota sobre un magma irreal al que permanece ajeno.

Para pensadores como Žižek, la pospolítica supone dejar atrás las viejas luchas ideológicas para encubrir lo que ha pasado a ser la administración y gestión de expertos, esto es, la despolitización de la política. De este modo, el multiculturalismo normativo implica desplazar la atención de cuestiones estructurales —que, como la economía especialmente, quedan tecnificadas y convertidas en el estado objetivo de las cosas— hacia cuestiones identitario-culturales, lo que necesariamente lleva a una sociedad despolitizada en tanto que solo interesada por el reconocimiento de las identidades

¹⁰⁰ Ibídem.

¹⁰¹ SARASQUETA, Gonzalo. *Op. cit.*, s.p.

marginales, fluidas y mutables (género, ecología, etnia, minorías culturales, sexualidad...) y por la tolerancia con la diferencia. Sin menospreciar estas cuestiones en las que reconoce que se han producido avances, su propuesta, como buen neomarxista, es repolitizar la economía.

La guerra híbrida y la *posverdad*

No resulta posible avanzar sin entender la esencia de uno de los conceptos que se está tratando: la guerra. Pero definir lo que es una guerra es hartamente complejo, porque se está, para empezar, ante una palabra vaga cuyo significado puede incluir desde violencia hasta aspectos morales e intimistas. Es, desde esta perspectiva, un concepto político y sociológico.

Pero también y simultáneamente, se está ante una institución de derecho internacional público; es más, para algunos juristas como Panebianco, la más importante. Y es que la palabra *guerra* es una palabra con un sentido jurídico muy claro y explícito en tanto que define la situación de dos Estados. Es por ello un término demasiado preciso para un mundo en el que la polisemia y la imprecisión otorgan más opciones a la política. Esta dualidad de significados, que aúnan además precisión e imprecisión, genera no pocos problemas.

Para empezar, la guerra no es un concepto estático; sus límites, además, son nuevamente imprecisos, ya que no los marca necesariamente el derramamiento de sangre. La guerra es, eso sí, violencia organizada; es decir, exige para su concreción una organización de la violencia hasta el punto de que solo puede existir guerra si existe una organización que sea capaz de administrar la violencia. Supone violencia en la medida en que encarna un choque de poderes. Pero esa violencia, para no pocos autores, no precisa materializarse en derramamiento de sangre como bien prueba la derrota de la URSS que trajo el fin de la guerra Fría. La guerra no es una actividad necesariamente sangrienta, pero sí una actividad necesariamente política.

Y es que es cierto que la guerra puede plantearse, en términos militares, como una sucesión de batallas: quien las gane todas, gana la guerra. Pero la experiencia de Francia en Argelia o de Estados Unidos en Vietnam prueba que esto no es siempre así; que la victoria, la resolución militar del problema no tiene que encontrarse en relación directa con la paz, su resolución política, por más que el bando ganador trate de partir de tal situación para fijar sus términos.

La guerra es ante todo un enfrentamiento de poderes, un choque en todas sus dimensiones. Y no es un acto ni ético, ni justo, ni económico, ni médico (puede hasta presentarse como una epidemia de politraumatismos), ni siquiera militar. Es un acto político, de gestión de poder, el más relevante, de modo que cualquier análisis que se realice sin tener en cuenta este hecho, esto es, referido solo a uno de los planos, es incompleto, falso y profundamente erróneo. La guerra es una función, un instrumento de la política, y

quien vea en ella otra cosa yerra gravísimamente. Como dijera Mao, la guerra es política con derramamiento de sangre; la política es —vista a los ojos del líder chino— guerra sin derramamiento de sangre.

No es la continuación de la política por otros medios, como dice la traducción tradicional de Clausewitz, sino más acertadamente la prosecución de la política por otros medios, que es lo que realmente dice el germano. La guerra es así una opción política más, esto es, no diferenciada de otras.

Es la política la que en última instancia fija los límites, las restricciones, las condiciones. Los límites no los imponen los medios, es decir, las operaciones militares, los imponen los fines, es decir, los objetivos políticos, aunque ciertamente los objetivos están condicionados por las opciones que hacen posibles los medios. Los límites del campo de batalla los debe fijar la política. Si la política no fija los límites de la guerra, la guerra además de total, se tornará absurda¹⁰². La guerra, pues, posee su propia gramática, pero la política es su cerebro (de hecho, genera una conducta específicamente política)¹⁰³.

La guerra es ante todo un choque de poderes más que un choque de violencias y encarna una actitud, un enfoque hostil hacia otro colectivo que puede materializarse mediante medios violentos que se suman a otros que pueden ser incluso más relevantes. Es más, el maquiavelismo de la estrategia confunde fuerza con poder, y ese es un grave error fruto de una interpretación simplista e irreflexiva de lo que es el poder.

Por eso las doctrinas militares modernas han tenido que recurrir a conceptos como la *guerra asimétrica o híbrida* para poder explicar una actitud de confrontación que no se materializa fundamentalmente en derramamiento de sangre, esto es, en el plano intrínsecamente militar; la pugna se desplaza verticalmente hacia planos no militares —opinión pública, economía, plano mediático, suministros...—, donde la parte más débil puede moverse más cómodamente e incluso con superioridad (al menos temporalmente) infiriendo daño al más fuerte. De hecho, si en un conflicto la parte más débil acepta las reglas que le impone la parte más fuerte, su lucha acabará inevitablemente en derrota. Lo que debe hacer el débil es expandir el marco del conflicto hasta encontrar aquel que lo haga más poderoso que su rival y tratar de llevarlo a él.

En los conflictos se pretende anular la voluntad de combatir de la contraparte (la guerra es una actividad del espíritu como diría Clausewitz) y asegurar la propia; es la dislocación del enemigo tan del gusto de Liddell Hart con la que se intenta deshacer su equilibrio, psicológica y físicamente, para su

¹⁰² GONZÁLEZ MARTÍN, Andrés, et al. «Evolución del pensamiento estratégico», en X Curso de Estado Mayor de las Fuerzas Armadas, 2008. Departamento de Estrategia y Relaciones Internacionales de la Escuela Superior de las Fuerzas Armadas.

¹⁰³ SCHMITT, Carl. *El concepto de lo político*. Madrid: Alianza Editorial, 1991, p. 64.

derrota sin necesidad de un sangriento enfrentamiento directo. En este sentido, Verstrynge constata:

«El notable el giro de 1917: hasta entonces solo se había hablado de la importancia de la guerra psicológica como arma desmoralizadora del soldado enemigo; el frente interior se mantenía por sí solo y se suponía con éxito. Sin embargo, posteriormente a 1916, el casi hundimiento de los contendientes demostró que se necesitaba también “proteger” psicológicamente a la población propia»¹⁰⁴.

Es más, algunos autores atribuyen el fin de la Primera Guerra Mundial al colapso psicológico de los líderes militares —Hindenburg y Ludendorff, principalmente—, que sobrevaloraron la gravedad de la situación militar creando una situación de alarma entre el pueblo y la clase política, lo que tuvo como consecuencia tanto su derrumbe interno como el de los propios aliados¹⁰⁵.

León Trotsky lo expresaba gráficamente con la poco delicada figura del «puñetazo al paralítico»¹⁰⁶; Hitler decía que «todas nuestras verdaderas guerras se entablaron antes de que comenzaran las operaciones militares»¹⁰⁷, apuntando a que «nuestra estrategia consiste en destruir al enemigo desde dentro», mientras Lenin insistía en «retrasar las operaciones hasta que la desintegración moral del enemigo haga a la vez posible y fácil asestar el golpe definitivo»¹⁰⁸. Pero todo ello ya fue subrayado por Sun Tsu, que recomendaba promover el desorden del contrario. Son precisamente estos efectos psicológicos los pretendidos por el terrorismo a través de la asociación de violencia y presión mediática; para ello se sirve de pulsos discontinuos de terror que se prolongan en el tiempo¹⁰⁹.

En cualquier caso, la comunidad internacional ha hecho menos probable el enfrentamiento militar, consignando otras vías diferentes para materializar el choque de poderes. Ese encaminamiento se hace nuevamente a través de palabras. El objetivo de la guerra es la paz, una contradicción dialéctica que solo se supera con la aceptación de que ambos términos pertenecen a la política, razón por la que no entran en conflicto, como a primera vista parece, y cuentan hasta con espacios comunes y de complementariedad.

Además, la guerra es una forma de relación. Entre quienes no hay relación no hay guerra. En esencia, es un diálogo que incorpora un suplemento de violencia y pertenece a la lógica del encuentro. Por consiguiente, para su co-

¹⁰⁴ VERSTRYNGE, Jorge. *Una sociedad para la guerra*. Madrid: Centro de Investigaciones Sociológicas, 1979, p. 368.

¹⁰⁵ LIDDELL HART, B.H. *Estrategia: la aproximación indirecta*. Madrid: Ministerio de Defensa, 1989, pp. 200 y ss.

¹⁰⁶ FRÍAS O'VALLE, José. *Nuestra guerra y nuestra paz*. Móstoles: Colección Adalid, 1985, s.p.

¹⁰⁷ LIDDELL HART, B.H. *Op. cit.*, pp. 208 y 209.

¹⁰⁸ *Ibidem*, p. 153.

¹⁰⁹ Münkler, Herfried. *Viejas y nuevas guerras*. Madrid: Siglo XXI de España Editores, 2002, p. 143.

recto desarrollo precisa desplegar todos los elementos de cualquier forma de diálogo: empatía, alteridad, conocimiento del otro... Como dijera Glucksmann, «se comunica mediante actos más que mediante palabras, o mediante actos que se añaden a las palabras y la acción se convierte en una forma de comunicación»¹¹⁰.

La guerra, en tanto que hecho social, se extiende allí donde llega la sociedad. Si esta alcanza a Internet, a las redes sociales, hasta allí llega esta. De no tomar en consideración este sector, la contraparte puede provocar el desbordamiento por flanco. Utilizando nuevamente las palabras del pensador francés antes citado respecto de la guerra, esta «[...] es un choque de discursos, que no gana el mejor [...] sino el que abarca el campo de batalla [...] no solo establece las condiciones de toda comunicación: es, en sí misma, comunicación»¹¹¹.

La guerra híbrida implica la acción concertada y simultánea de componentes regulares e irregulares, una naturaleza compuesta en la que se asocian indiferenciadamente lo convencional y lo no convencional, al tiempo que existe coordinación entre ellos. La complementariedad y coordinación entre ambos términos genera efectos sinérgicos¹¹².

La Estrategia de Seguridad Nacional 2017 muestra como:

«A los tradicionales conflictos armados se unen formas adicionales de agresión e influencia, amenazas asociadas a la proliferación de armas de destrucción masiva y otras variantes de actos hostiles. Sofisticados sistemas de armas de alta precisión se combinan con la letalidad funcional de ciberataques y acciones de influencia y desinformación. La ambigüedad y la dificultad de atribución son factores constantes de los denominados conflictos híbridos, aquellos que incorporan operaciones de información, subversión, presión económica y financiera junto a acciones militares. Estas acciones, perpetradas tanto por actores estatales como no-estatales [*sic*], tienen por objeto la movilización de la opinión y la desestabilización política»¹¹³.

En este sentido, la utilización de estrategias de comunicación en forma de narrativas, propaganda o *fake news* encaja muy bien con esta lógica de guerra. La información ha estado militarizada desde antes de que Lenin lo hiciera. El derrotar al enemigo desde dentro fomentando el disenso, la desunión

¹¹⁰ GLUCKSMANN, André. *El discurso de la guerra*. Barcelona: Anagrama, 1969, p. 108

¹¹¹ *Ibíd.*, p. 83.

¹¹² GARCÍA GUINDO, Miguel; MARTÍNEZ-VALERA GONZÁLEZ, Gabriel. «La guerra híbrida: Nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales», Documento de trabajo del Instituto Español de Estudios Estratégicos, n.º 02/2015.

¹¹³ Gobierno de España. *Op. cit.*, pp. 59-60.

o hacerle adoptar decisiones inadecuadas es, como ya hemos visto, tan antiguo como la guerra.

Probablemente, sean los rusos los que tengan en este campo una mayor experiencia y práctica, aunque solo sea por el pasado. La principal estrategia de la doctrina de la llamada guerra de Nueva Generación es una «estrategia de influencia, no de fuerza bruta», porque su objetivo trascendental es «romper la coherencia interna del sistema [político, económico, militar] del enemigo, y no aniquilarle». Según la visión conceptual del Ministerio de Defensa ruso de 2011, los objetivos de la guerra informativa son «socavar el sistema político, económico y social, adoctrinar la población para desestabilizar la sociedad y el Estado y forzar a los Estados a tomar decisiones favorables a los intereses de sus oponentes». Esta visión fue perfeccionada en 2013 por el general Valeri Gerasimov, jefe del Estado Mayor de las Fuerzas Armadas de Rusia, que escribió que lo que más distingue la guerra convencional de la guerra híbrida es la simultaneidad en esta de las batallas en tierra, mar, aire y espacio informativo, y el uso de métodos indirectos y no lineales para alcanzar objetivos militares. De este modo, certifica que las reglas de la guerra han cambiado para adaptarse a los nuevos tiempos y, en muchos casos, el papel de los medios no militares superaba a la fuerza de las armas¹¹⁴.

La *posverdad* puede venir a instalarse en este modelo estratégico de guerra; se encuentra dirigida a debilitar una sociedad con vistas a una acción posterior o a socavar su acción exterior y consistencia. Una de las medidas acordadas tras la declaración conjunta OTAN-UE realizada tras la cumbre de Varsovia de la Organización Atlántica celebrada en 2016 fue la lucha contra las amenazas híbridas, en particular mediante la elaboración de procedimientos coordinados. El East Stratcom es un proyecto que obedece a este espíritu por la Unión Europea en 2015 dedicado a desarrollar campañas de comunicación y contenidos, centrado en explicar la política europea para el Este para evitar intentos de desinformación. Y aun la propia Comisión Europea, como ya se ha aludido, ha creado un grupo de expertos de alto nivel que han dictaminado sobre las *fake news*.

La Estrategia Española de Seguridad (EES) la contempla como una amenaza:

«La influencia de movimientos exclusivistas crece por el uso masivo de las redes sociales. Asimismo, la manipulación de la información por parte de agentes externos ejerce de factor de influencia en la era de la *posverdad*, con efectos negativos en la cohesión social y la estabilidad política»¹¹⁵.

Las amenazas híbridas son amenazas inconcretas que, no pocas veces, no se formulan como tales, y, en no pocas ocasiones, es difícil la atribución en su concreción. Además, en los Estados, a veces aparecen instituciones y or-

¹¹⁴ MILOSEVICH-JUARISTI, Mira. *Op. cit.*, s.p.

¹¹⁵ Gobierno de España. *Op. cit.*, pp. 36-37.

ganismos oficiales junto a otros que no lo son y que se presentan como entes privados por más que actúen coordinados o en connivencia con las propuestas políticas de aquellos; como resultado, resulta difícil atribuir responsabilidades, acreditar su naturaleza estatal, y más aún en el nebuloso mundo de las redes e Internet. Un ejemplo pudieron ser, al principio y en su momento, los llamados *pequeños hombres verdes* que pululaban por los territorios ucranianos en controversia en 2014.

Superar la *posverdad*

La *posverdad* plantea, según se ha visto, un grave riesgo para la Seguridad Nacional al tensionar tanto a la sociedad como al aparato que la soporta. El reino del algoritmo, de los automatismos y de la falta de periodismo de calidad le deja el camino expedito¹¹⁶. Esta acrecienta y exhibe maliciosamente las contradicciones y vulnerabilidades de las sociedades, utilizando las oportunidades que se le presentan y generando una crisis en la confianza; con ello se pretende debilitar las instituciones y provocar la atomización del espacio social como forma deliberada de debilitar a las sociedades objetivo. Pero las vulnerabilidades son reales y están ahí. Uno de los primeros pasos para luchar contra la *posverdad*, por tanto, pasa por corregirlas.

No basta con que las cosas se asemejen o simulen ser para que sean reales. La contraintuitividad, el «asombro epistémico», es la marca de objetividad de la ciencia¹¹⁷. Al final los hechos acaban siempre por imponerse, al igual que lo hace la ley de la gravedad por encima de cualquier otra. Cualquier escapada, fuga, huida de la realidad, acabará por ser reconducida. Los hechos se impondrán porque solo se puede vivir al margen de ellos por un cierto tiempo. Lo importante es aguantar la tensión hasta que tal cosa suceda. Como nos recuerda el presidente norteamericano Lincoln, «Puedes engañar a todo el mundo algún tiempo. Puedes engañar a algunos todo el tiempo, pero no puedes engañar a todos todo el tiempo».

La *posverdad* abandonada a sí misma acabará por normalizar su presencia a los niveles en los que siempre ha estado. Tampoco se puede gobernar desde la anomía y el desconocimiento de los gobernados; la *pospolítica* tiene límites. La cuestión no es, por tanto, si tal situación perdurará (que no lo hará), sino si, en ese tiempo, quien así obra será capaz de cambiar la realidad a través de ese tortuoso instrumento.

La dependencia tecnológica, que explica el éxito de las sociedades occidentales, tiene ese contrapunto; como piedra angular, es ahora un factor de debilidad tanto frente a los ciberataques como frente a campañas de desinformación. Internet es un espacio de unión y con ello también una frontera

¹¹⁶ ALANDETE, David. «Como combatir la *posverdad*». Diario El País, 22 noviembre 2016.

¹¹⁷ FICHTENTREI FUENTE, Daniel. *Op. cit.*, s.p.

común, transversal, que afecta a muchos ámbitos específicos y a la sociedad internacional. Su seguridad se torna crítica. El ciudadano, a través de las redes sociales, ha quedado sobreexpuesto a la influencia de actores con intereses particulares y que instrumentan en beneficio propio las reglas establecidas y la conciencia moral de la sociedad. La ciberseguridad es un área también en la que trabajar tanto desde el punto de vista técnico como desde el social.

Los problemas del siglo xxi son multidisciplinarios y poliédricos. Pero las soluciones a los problemas de las sociedades no vienen de fuera, sino de dentro, y pasan a primer término por que, en lo posible, estas generen sus propios anticuerpos para afrontar los virus que las invaden. Se trata de obtener una respuesta natural y propia antes que utilizar compuestos químicos cuyos efectos secundarios, por lo demás y como poco, se desconocen.

Por eso la lucha contra este fenómeno debe ir más allá de la disputa y ser, por el contrario, expresión de la continuidad de los valores del Estado, una necesaria derivada de los mismos sin interrupciones. Se debe luchar sin hacerlo realmente, como se acomete la delincuencia, esto es, sin romper la armonía y centralidad del Estado y buscando preservar su legitimidad, eje de la disputa. Es preciso abordarla desde una dimensión positiva y, por tanto, articuladora para poder primarla y dotarla de continuidad. No es tanto un esfuerzo de «lucha» como de «superación».

Y es que la democracia incorpora *per se* una voluntad inclusiva y de equilibrios que reduce a su mínima expresión las prohibiciones. Esta surge, recordémoslo de nuevo, de la duda y también de la suspicacia hacia el funcionamiento de sus propias instituciones. Cualquier ajuste de sus equilibrios puede tener consecuencias insospechadas. La democracia es el triunfo de la sociedad civil, que viene a ser su centro de gravedad. Por ello, en el paradigma libertad-seguridad debe primar el primero de los componentes.

En este sentido, la definición weberiana del Estado como detentador del monopolio de la violencia legítima no puede restar luz al hecho de que el uso de la autoridad en una democracia real es o debe ser residual, porque el precio de tal cosa se mide en términos de legitimidad. El poder es un tótem, es potencia, no necesariamente acción, y se desgasta con su utilización, máxime cuando este, por muy excepcional que sea el caso, se hace en sentido contrario a los valores que sirven para sustentarla, esto es, contra su acervo. Con todo, «la democracia ha perdurado porque sus instituciones están diseñadas para manejar formas moralmente arriesgadas del poder coactivo»¹¹⁸.

Los valores de una sociedad no son aquellos de los que se hace prédica, sino aquellos de los que se hace práctica. Por eso no todos los métodos adversarios pueden ser asimilados en nombre de la legitimidad, de la propia conservación o de la coherencia, en razón de la concepción de la libertad propia

¹¹⁸ IGNATIEFF, Michael. El mal menor. Madrid: Taurus, 2005, p. 27.

de ella. Este puede ser un buen ejemplo de cómo el camino más corto puede acabar por convertirse en el más largo y costoso.

La democracia es algo más que un Estado de derecho, unas elecciones o un sistema de balances y contrapesos (que también); es, ante todo, una ética, una cultura que implementa el espacio que va desde la norma hasta su puesta en práctica; es una forma de hacer las cosas, así como un estado de deliberación permanente entre gobernantes y gobernados que garantiza una respuesta concertada y poderosa *per se*. La democracia implica decir la verdad y explicarse. La comunicación no es solo una necesidad, sino una obligación innata, la primera.

Una postura rompe con la continuidad antes aludida y además es un concepto estático, una forma que es difícil de aplicar a un fenómeno diverso y dinámico y que, por su rigidez, no termina de encajar con él en todos los casos. Además, la desinformación es un problema multifacético y, por tanto, no tiene una única solución que, además, debe incorporar a actores de todo tipo.

Ciertamente, la aparente debilidad de la democracia enmascara una fuerza arrolladora: la voluntad concertada de millones de personas. El Estado de derecho tiende a ir por detrás de los sucesos, rara vez por delante. Esa lentitud es el precio que ineludiblemente ha de pagarse al tener que gestionar un poder tan inmenso. La respuesta del Estado de derecho es siempre tasada y lenta y parece ineficaz, pues la utilización del poder en este marco es, por principio, residual y reactiva. Pero este es incontestable; el Estado y Occidente pueden permitirse perder para ganar, no les merece la pena el precio de una victoria rápida.

El principal valor a proteger frente a los ataques queda cifrado en la integridad de la sociedad. Superar la *posverdad* puede requerir de prevención e incluso, puntualmente, de medidas coercitivas. La cuestión se sitúa en los límites en que se debe desarrollar la respuesta. El margen será mayor o menor en función de la naturaleza de la amenaza, precisándose, como poco, de normas efectivas y de la tutela judicial como una garantía legitimadora. La utilidad de instrumentos como la censura o la regulación de contenidos en unas sociedades tan abiertas como las occidentales es más que limitada; es poner puertas al campo y dejarse en ello, adicionalmente, la legitimidad. La crítica, la duda, es progreso, obliga a la renovación; su fin implica, por el contrario, el estancamiento.

Es más, tomando en consideración que la misma amenaza se cierne sobre otras sociedades democráticas en las que nos reconocemos e inspiramos como modelo, esta lucha por razones de sinergia debe abordarse conjuntamente a través de las organizaciones y pactos de los que somos parte y que muestran la existencia de una comunidad que comparte valores e intereses (UE, OTAN y Convenio de Cooperación Hispano-Norteamericano, además de en la Organización de Naciones Unidas en cuanto a organismo de concertación política a nivel global).

Y no solo eso. Dadas las contradicciones a las que la *posverdad* arroja a la democracia, las democracias occidentales deben tratar de afrontar sus retos desde cuerpos normativos similares, de modo que unos validen a otros y se presente un frente uniforme que dote de una legitimidad aún mayor a la respuesta institucional y la refuerce. Los aspectos que más gravamen supongan para nuestro actual régimen de libertades deben contar con un acervo común que les dote de una legitimidad especial y estar sometidos a una tutela judicial exterior al propio Estado y conjunta.

El Derecho va por detrás de los hechos que regula y, por tanto, es perfeccionable. Pero legislar en caliente es arriesgado. No obstante, el ciclo de respuesta ante un asunto de tanta enjundia debe de acortarse, y una forma para ello es transferir la experiencia de un país a otro. La cooperación y el intercambio de información es crítica.

La clase política, los líderes de las sociedades, han perdido influencia y hasta aceptación en el conjunto de las sociedades occidentales. Con los medios de comunicación clásicos viene a pasar lo mismo. Son dos pilares de la sociedad que se encuentran debilitados y que, por tanto, urge fortalecer.

Fortalecer las instituciones que sirven como soporte de la sociedad pasa por deshacer el escepticismo; para ello, no hay nada mejor que la transparencia, porque el mal ya está hecho. Como Byung-Chul Han sostiene, «La transparencia solo se requiere de forma urgente en una sociedad en la que la confianza ya no existe como valor»¹¹⁹.

La democracia y la libertad se basan en la evidencia y la verdad, por eso la educación junto al periodismo y la justicia son la base de unas defensas sólidas. Estamos hablando de proyectos a largo plazo orientados al reforzamiento de la ciudadanía. La ciudadanía real se asienta, en primer término, sobre la educación; una sociedad de buenos ciudadanos es siempre una sociedad de ciudadanos educados. Esparta, nos recuerda Tucídides, no tenía murallas porque tenía a sus ciudadanos.

Es cierto que el nivel cultural de las organizaciones ha crecido, pero también la exigencia que recae sobre los ciudadanos. En este contexto, los mensajes cortos prosperan sobre los razonamientos profundos. Falta preparación y reflexión, lo que además requiere de tiempo. Por tanto, otro de los ejes para luchar contra la *posverdad* se sitúa en el humanismo, en la educación de la sociedad. De hecho, todo proyecto político de calado pasa por lo mismo.

La educación refuerza la transversalidad, el núcleo duro, y evita la fragmentación, la segregación de la sociedad, su debilitamiento. Educar en la verdad, robustecer los valores, ayuda a recuperar la confianza. A su vez

¹¹⁹ ORTEGA, Andrés. «Campañas de desinformación: la debilidad de la desconfianza», en *Blog del Real Instituto Elcano* [en línea]. 5 diciembre 2017. Disponible en web: <https://blog.realinstitutoelcano.org/campanas-desinformacion-debilidad-desconfianza/>.

la ética, una ética común, debe servir para reforzar al conjunto de la sociedad e incrementar su cohesión y fe en sí misma.

En este sentido se han hecho grandes logros, especialmente en nuestro país, referidos a la extensión de la educación universitaria, pero aún subsiste una bolsa importante de iletrados funcionales con acceso a información de todo tipo pero sin posibilidad de discernir sobre su calidad, pues esta, entre otras cosas, no es fácil de contrastar. Hace falta también dotar de una formación mediática crítica a la ciudadanía, sacar al lector de la burbuja ideológica y dotarle de herramientas de verificación digital sistemática. También se precisa propiciar una alfabetización tecnológica.

La prensa es el cuarto poder y su existencia contribuye al equilibrio del conjunto del sistema democrático. Los medios son los principales interesados en luchar contra las noticias falsas. El periodismo como marca y fuente de información veraz y de calidad debe ser potenciado. Cuando una noticia falsa se cuela en un ciclo informativo no solo alcanza altas cotas de veracidad, sino que contamina el conjunto del sistema. La fortaleza de una cadena queda consignada a su eslabón más débil. Para reforzarla, el periodista profesional ha de disponer de una formación y un bagaje que le distinga sensiblemente del llamado *periodismo cívico*, para poder acometer un cribado eficaz y convertirse en referencia social.

La ciencia nació para derribar a los mitos. Por eso ellos deben ser los primeros a la hora de denunciar y desmontar la demagogia y el sesgo. Para eso, y teniendo en cuenta el ámbito de las redes sociales, los cibermedios deben hacer una gestión activa de sus comunidades, algo, por lo demás, siempre deseable; la proactividad se muestra crítica en un escenario de *fake news* como el que se plantea.

El periodismo, en tanto que parte del pensamiento crítico, no se puede ni se debe regular (los costos de tal cosa en términos de legitimidad son muy superiores a cualquier eventual beneficio), pero sí se debe promover una suerte de código deontológico que favorezca un profesionalismo autoregulatorio y atento frente a eventuales actitudes poco éticas de los miembros de la profesión.

Fortalecer el periodismo pasa por fortalecer financieramente a las empresas que lo llevan a cabo, y por fortalecer la marca, una marca ligada a la verdad. En un informe elaborado para la Comisión Europea, un grupo de expertos de alto nivel, se recomienda apoyar financieramente a grupos informativos independientes libres de potenciales interferencias de autoridades públicas y de compañías tecnológicas que pudieran verse tentadas a utilizar dichos proyectos como escaparates en sus relaciones públicas¹²⁰.

¹²⁰ WARDLE, Claire et al. *Op. cit.*, s.p.

Las redes sociales también han de verse concernidas en este escenario y buscar la certeza en las informaciones que intencionadamente se difunden a través suyo. Diversos estudios han comprobado cómo las *fake news* cuentan con más viralidad que la información real; esto es lógico, pues se han construido con tal propósito. Algunos, comenzando por Facebook han comenzado a moverse en este sentido, pero todavía queda camino, mucho camino que recorrer. Como David Alandete¹²¹ escribía, «Un algoritmo nunca podrá hacer periodismo pero puede aprender a identificar a los que lo hacen, para bien de todos».

Pero la actuación de estas grandes empresas debe ir más lejos y compartir la información con vistas a propiciar el abordaje sinérgico. Además, y en la misma línea que el planteamiento que resulta válido para el periodismo, es conveniente la adhesión voluntaria de las empresas a códigos de buenas prácticas por más que los márgenes normativos sean, en este caso, más amplios.

La Responsabilidad Social Corporativa (RSC) de las empresas también es clave en este esquema. Mención aparte son las empresas de distribución de información residenciadas en terceros países o con conexiones con ellos, máxime cuando su calidad democrática es baja. Merecen un estudio más ponderado y aun a nivel europeo que favorezca respuestas desde este nivel.

Las *fake news* pueden ocultar operaciones psicológicas de gran calado. Y resulta muy difícil de identificar la fuente de estos ataques, e incluso acreditar la maldad de su proceder. No hay tiempo para contrastar un ingente número de noticias. El *fast checking*, la comprobación rápida, es imprescindible para luchar contra la desinformación. La velocidad de respuesta frente a las *fake news* se plantea como un hito para evitar que estas avancen ni aun como leyendas urbanas. Los desmentidos deben también viralizarse, lo que requiere de contenidos ricos y adaptados al entorno al que van dirigidos. Además, como sostenía Derrida, «Hay que olvidar la lógica maniquea de verdad y mentira y centrarlos en la intencionalidad de quienes mienten». Esto es, trascendiendo del hecho, buscar la fuente y el porqué.

El pensamiento crítico debe promoverse. La crítica es imprescindible para el progreso de las sociedades, para su mejora. Una sociedad precisa de referentes intelectuales, de faros en lo alto de la montaña, personajes u organismos encumbrados a los que poder seguir; pero también de críticos que, permanentemente y desde la buena fe, cuestionen el modelo vigente y a aquellos mientras proponen universos distintos y nuevos sueños. Las sociedades se crecen en sus contradicciones. Ese pensamiento crítico pertenece al acervo de Occidente, debe ser preservado a cualquier costo e impedir que se incorpore o lo incorporen al mundo de la *posverdad*.

¹²¹ ALANDETE, David. *Op. cit.*, s.p.

En cualquier caso, estamos ante un hecho novedoso y que se adivina evolutivo que precisa de ser estudiado desde un punto de vista multidisciplinar e involucrando a todos los actores implicados. El siglo xxi es el siglo del pensamiento complejo; poco hay de sencillo, directo o intuitivo en él.

Conclusiones

El siglo xxi ha propiciado un nuevo retorno al antropocentrismo que hace del relativismo, el escepticismo y lo alternativo, el culto al presente y el formalismo sus características principales; es lo que Sartori llama *el estado de vaciedad del vacío*. La posmodernidad es, por encima de todo, una actitud centrada sobre el presente y la forma; su formulación viene a coincidir con la idea de D. Bell sobre el crepúsculo de las ideologías, la reducción del espacio para la auténtica diferencia política, lo que resulta capital. No obstante, hasta en eso falta definición.

Las sociedades se encuentran muy fragmentadas, hecho que la globalización ha potenciado aún más; se han hecho conscientes de su diversidad mientras que el abanico de referencias que tradicionalmente ha utilizado ha sido muy tensionado. Esta fragmentación dificulta el desarrollo de acciones colectivas y promueve el conformismo.

La opinión pública, pese a su infantilismo —esto es, su mutabilidad y carencia de responsabilidad—, viene a representar el ser de las sociedades y mantiene una relación bilateral con estas. La cuestión es que el patrón de la información ha cambiado y la opinión pública se forma al margen de los medios de comunicación establecidos y de la ausencia de criterios de calidad, razón por la que resulta muy influenciable. Es lo que el filósofo José Antonio Marina denomina *síndrome de inmunodeficiencia social*.

La tecnología en una sociedad de la información que acumula datos es un factor crítico. Se consume mucha información y, sin embargo, falta análisis, comprensión. El hombre moderno no piensa, se informa. La tecnología es un elemento transversal al progreso y con ello una vulnerabilidad; debe ser objeto de especial protección, especialmente la noosfera. Internet traslada a la red las fracturas de la sociedad al tiempo que las acentúa.

En este contexto, y paradójicamente —pues la razón es la piedra angular que ha servido a la construcción de Occidente—, la emoción prima sobre la razón y la verdad se relativiza y, con ello, la realidad a la que esta obedece, lo que a su vez deriva en una nueva fractura de la sociedad. La *pospolítica* es una práctica que implica actuar sobre las emociones para llegar a la razón, ahuecando un discurso que de este modo se hace resonante mientras se hurta la agenda política a una ciudadanía a la que se tiene entretenida con cuestiones secundarias. Y, además, escapa a la rendición de cuentas inherente al modelo democrático. El papel de las narrativas y la capacidad de penetración de los imaginarios, acentuada de la mano de las nuevas tecnologías y focali-

zada por las herramientas tecnológicas de comprensión social como el *data mining*, se muestra capital en tal esquema disruptivo.

En este contexto, del que se deriva una debilidad de las instituciones y hasta de la crítica, surgen conceptos como la *posverdad* o las *fake news*, que suponen la banalización de lo que comúnmente se ha venido a llamar desinformación y, por tanto, contribuyen a su aceptación. Por eso tales nombres deben ser rechazados. Además, no expresan plenamente la realidad que estamos tratando. Son dos sofismas o modelos para el sofisma que harían palidecer al mismísimo Gorgias. El tiempo que vivimos, tal y como pronosticaba Enrique Santos Discépolo en el tango con el que abríamos este capítulo, reproduce también aquella época.

Como decía Confucio: «Si los nombre [*sic*] son incorrectos, el discurso no es coherente. Si [*sic*] el lenguaje es incoherente, los asuntos no pueden resolverse... Por eso el hombre de bien solo usa los nombres cuando implican un discurso coherente, y solo discurre sí [*sic*] lleva sus palabras a la práctica. Por eso el hombre de bien es prudente con lo que dice»¹²².

La amenaza híbrida, que se sirve de la instrumentación de este conjunto de factores, se nos plantea como un reto capital. Su naturaleza no convencional y multiforme persigue debilitar a las sociedades afectando a su cohesión y exhibiendo sus contradicciones. Son amenazas difusas cuya procedencia y naturaleza resultan difíciles de identificar formalmente, por más que se intuyan. La desinformación, que es de lo que estamos hablando bajo nuevos e inapropiados nombres, recordémoslo de nuevo, se utiliza para la ruptura de la comunidad.

La *posverdad* se sirve de las reglas, la conciencia moral y los valores de Occidente en su beneficio; estresa a la sociedad ensanchando y haciendo más visibles sus costuras, sus líneas de debilidad. Sufren un estrés especial algunos puntos nodales, las líneas de juntura en las que interaccionan Estado y sociedad y que son las instituciones.

Este fenómeno es complejo y evolutivo, no admite una única solución sino toda una pluralidad de ellas y, además, incorpora a múltiples actores. Sus soluciones deben ser acordes con la propia cultura y estar orientadas al largo plazo. La educación se presenta como clave para incrementar la resiliencia de estas y evitar la penetración de noticias falsas. Es un anticuerpo natural.

Y es que la lucha contra la difusión de contenidos falsos puede arrastrar a las sociedades a la censura, y con ello, como corolario, a que se suprima el pensamiento crítico y se mengüen a la postre libertades y derechos; esto es todo lo que ha hecho que Occidente sea lo que hoy es. Por tanto, el control de la información no es la piedra angular sobre la que construir la solución; los

¹²² YAÑEZ, Manuel. *Confucio*. Madrid: EDIMAT Libros, 1998, p. 96.

costos exceden a los beneficios. La clave está, nuevamente hay que recordarlo, en el interior de la sociedad, y pasa por resolver sus problemas efectivos. Estamos en un ámbito cuya centralidad requiere de una ponderación extrema y no admite ni soluciones rápidas ni mágicas. Se deben promover las actitudes deontológicas y colaborativas antes que las restrictivas. El Derecho siempre va por detrás de los hechos que pretende regular.

La respuesta, en cualquier caso, debe venir de los Estados, pero también desde el ámbito de la sociedad civil, de entidades independientes, para alcanzar el mayor grado posible de adaptación e implicar, de un modo cooperativo, al conjunto de las democracias occidentales, lo que permite afrontar tal reto desde la mayor de las legitimidades posible.

Para eso necesitamos un periodismo fuerte y de referencias críticas que impidan que perdamos el norte y las esencias. El periodismo, actualmente, adolece de problemas en la formación de su personal mientras su neutralidad e independencia se han visto cuestionadas como resultado de la feroz competencia desde las redes sociales y de su propia dependencia de la política y las empresas. A la política también le ha pasado factura la pérdida de referentes. Ambos son pilares insustituibles de nuestras sociedades cuyo reforzamiento es imperativo.

Las sociedades se construyen desde la palabra. Por otra parte, el acervo de la civilización occidental son la libertad y la duda. Estos son valores que deben ser protegidos simultáneamente y a cualquier costo. No hay nada más impuro que las impurezas que salen de dentro. Como recuerda el sociólogo Tzvetan Todorov, «La democracia tiene mucho más que temer de las perversiones o desvíos del proyecto democrático que vienen del interior».

Bibliografía

Publicaciones

ARON, Raymond. *Un siglo de guerra total*. París: Editorial Hispano Europea, 1958.

BALLESTEROS, Ángel. *Diplomacia y Relaciones Internacionales*. Madrid: Ministerio de Asuntos Exteriores, 1995.

BAUDRILLARD, Jean. *La ilusión del fin. La huelga de los acontecimientos*. Barcelona: Editorial Anagrama, 2015.

Cultura y simulacro, 2015, Barcelona: Kairós

El crimen perfecto, 1997, Editorial Anagrama.

BAUMAN, Zygmunt. *En busca de la política*. Buenos Aires: Fondo de Cultura Económica, 2001.

BERNAYS, Edward. *Propaganda*. Editorial Melousina, 2008.

- BYUNG-CHUL, Han. *La sociedad del Cansancio*. Ed. Herder, 2012.
- Psicopolítica*, 2014, Editorial Herder.
- CHOMSKY, Noam. *El nuevo orden mundial (y el viejo)*. Barcelona: Grijalbo Mondadori, 1996.
- COMPAYNS MONCLÚS, Julián. *España en 1898: entre la diplomacia y la guerra*. Madrid: Biblioteca Diplomática Española, 1991.
- Eco, Umberto. *Apocalípticos e Integrados*. Barcelona: Lumen, 1984.
- FOUCAULT, Michael. «Curso del 14 de enero de 1976», en VV.AA. *Microfísica del poder*, Madrid: La Piqueta, 1979.
- FRÍAS O'VALLE, José. *Nuestra guerra y nuestra paz*. Móstoles: Colección Adalid, 1985.
- GARCÍA CANEIRO, José; VIDARTE, Francisco Javier. *Guerra y filosofía*. Valencia: Tirant Lo Blanch, s.f.
- GENETTE, Gerard. *Figuras III*. Barcelona: Lumen, 1989.
- GLUCKSMANN, André. *El discurso de la guerra*. Barcelona: Anagrama, 1969.
- HOFFMAN, Bruce. *Historia del terrorismo*. Calpe: Espasa, 1999.
- IGNATIEFF, Michael. *El honor del guerrero*. Madrid: Taurus, 1999. *El mal menor*. Madrid: Taurus, 2005.
- JORDÁN, Javier; CALVO, José Luís. *El nuevo rostro de la guerra*. Barañáin: Ediciones Universidad de Navarra, 2005.
- LE BORGNE, Claude. *La guerra ha muerto*. Madrid: Ediciones Ejército, s.f.
- LEWIS, Carrol. «Alicia a través del espejo», [en línea]. Capítulo 6. Disponible en web: www.elaleph.com/libros
- LIDDELL HART, B.H. *Estrategia: la aproximación indirecta*. Madrid: Ministerio de Defensa, 1989.
- MÜNKLER, Herfried. *Viejas y nuevas guerras*. Madrid: Siglo XXI de España Editores, 2002.
- NIXON, Richard M. *La verdadera guerra*. Barcelona: Planeta, 1980.
- ORWELL, George, 1984, Barcelona: Destino, 1999.
- PARET, Peter (coord). *Creadores de la Estrategia Moderna*. Madrid: Ministerio de Defensa, 1992.
- RAMONET, Ignacio. «Los Conflictos Armados», en VV.AA. *Seminario de Investigación Para la paz*. Diputación General De Aragón, 1997.
- ROJAS, Enrique. *El hombre light*. S.L.: Ediciones Temas de Hoy, s.f.
- SÁEZ ORTEGA, Pedro. *Guerra y paz en el comienzo del siglo XXI*. Madrid: Fundación del hogar del empleado, 2002.
- SCHMITT, Carl. *El concepto de lo político*. Madrid: Alianza Editorial, 1991.
- VERSTRYNGE, Jorge. *Una sociedad para la guerra*. Madrid: Centro de Investigaciones Sociológicas, 1979.

- TEDESCO, Juan Carlos. *El nuevo pacto educativo*. Madrid: Anaya, 1995.
- TERNON, Yves. *El Estado criminal*. Barcelona: Península, 1995.
- VV.AA. *Una mirada al mundo del siglo XXI*. Madrid: Ministerio de Defensa, 2008.
- VV.AA. *Terrorismo, víctimas y medios de comunicación*. S.l.: Fundación Víctimas del Terrorismo, 2003.
- VV.AA. *A multi-dimensional approach to disinformation. Report of the Independent High level group on fake new and on the disinformation*. Luxemburg publication Office of the European Union, 2018.
- YAÑEZ, Manuel. *Confucio*. Madrid: EDIMAT Libros, 1998.
- ZAMBRANA, Justo. *El ciudadano conforme. Mística para la globalización*. Madrid: Taurus, 2006.
- ŽIŽEK, Slavok. *¡Bienvenidos al desierto de lo real!* [en línea]. Suplemento Radar, Diario. 23 septiembre 2001. Disponible en web: <http://www.pagina12.com.ar/2001/suple/radar/01-09/01-09-23/pagina3.htm>
- En defensa de la intolerancia* [en línea]. S.l., s.f. Disponible en web: http://estafeta-gabrielpulecio.blogspot.com.es/2009/03/slavoj-zizek-en-defensa-de-la_4989.html.

Recursos electrónicos y artículos

- ABRAHAM FERNÁNDEZ, Jesús. «Algoritmos, las nuevas armas de ¿construcción? Masiva», en *Instituto Español de Estudios Estratégicos*. DIEEE 06-2017.
- AGUIRRE, Miguel Ángel. «Desinformación, democracia y seguridad», en *Periódico El País*. 9 febrero 2018.
- ALANDETE, David. «Cómo combatir la posverdad», en *Diario El País*. 22 noviembre 2016.
- ARRANZ MARTÍNEZ, Raquel. «La creación de imaginarios», en *Documento de investigación del IEEE*. 2018.
- BERCKEMEYER, Fernando. «La mentira de la posverdad», en *Revista-uno.com* Número 27.
- BIANCO, Gabriella. «Desde el post-modernismo [sic] a la post-verdad [sic]» [en línea], en *CECIES, Pensamiento latinoamericano y alternativo*. [ref. del 20 marzo 2018]. Disponible en web: <http://www.cecies.org/articulo.asp?id=582>
- CAROL, Marius. «Fracasar rápido», en *Editorial del Diario La Vanguardia*. 15 febrero 2018.
- CARNICERO URABAYEN, Carlos. «Posverdad y redes sociales, una amenaza a la democracia» [en línea], en *Diario Huffingtonpost*. 17 septiembre 2017. Disponible en web: https://www.huffingtonpost.es/2017/09/17/posverdad-y-redes-sociales-una-amenaza-para-la-democracia_a_23063245/.

- ESCRIVÁ, Ángeles. «El altavoz del terror del Estado Islámico» [en línea], en *Diario El Mundo*. 26 noviembre 2016. Disponible en web: <http://www.elmundo.es/internacional/2016/11/26/58385a4fe2704e2c3a8b45b5.html>
- FERNANDO JUAN, José. «7 apuntes sobre la *posverdad* en las redes sociales» [en línea], en *Revista Entre paréntesis*. 19 diciembre 2016. Disponible en web: <http://entreparesis.org/posverdad-en-redes-sociales/>.
- GARCÍA GUINDO, Miguel; MARTÍNEZ-VALERA GONZÁLEZ, Gabriel. «La guerra híbrida: Nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales», en *Instituto Español de Estudios Estratégicos*. Documento de Trabajo del Instituto Español de Estudios Estratégicos n.º 02/2015.
- Gobierno de España. *Estrategia de Seguridad Nacional 2017*. Presidencia del Gobierno.
- GONZÁLEZ MARTÍN, Andrés et al. «Evolución del pensamiento estratégico», en *X Curso de Estado Mayor de las Fuerzas Armadas*, 2008. Departamento de Estrategia y Relaciones Internacionales de la Escuela Superior de las Fuerzas Armadas.
- GONZÁLEZ-RIVERA, Juliana. «La información en la era de la *posverdad*: retos, mea culpas y antídotos» [en línea], en *Universidad EAFIT*. Disponible en web: <http://www.eafit.edu.co/medios/eleafitense/112/Paginas/informacion-posverdad.aspx>
- GOTTFRIED, Jeffrey; SHEARER, Elisa. «News use across social media platforms» [en línea], en *Pew Research Centre & Knight Foundation*. Disponible en web: <http://www.journalism.org/2016/05/26/news-use-across-social-media-platforms-2016/>.
- GRAMSCI, Antonio. «Quaderni del Carcere» Volumen I Quaderni 1-5, en EIN-AUDI, Giulio. 1977.
- HUMBERTO RODRÍGUEZ, Luis. «¿*Posverdad*... o mentira?», en *Periódico Mirada 21*. Universidad Francisco de Vitoria. 29 diciembre 2017.
- KRAUS, Arnoldo. «*Posverdad*» [en línea], en *Diario el Universal*. 15 enero 2017. Disponible en web: <http://www.eluniversal.com.mx/entrada-de-opinion/articulo/arnoldo-kraus/nacion/2017/01/15/posverdad>.
- LENOIR-GRAND PONS, Ricardo. «Cuando la información busca desestabilizar el enemigo» [en línea], en *Revista On line La Grieta*. 17 abril 2017. Disponible en web: <http://lagrietaonline.com/cuando-la-desinformacion-busca-desestabilizar-al-enemigo/>.
- MANRIQUE, José Luis. «Populismo y *posverdad*, ¿Solo tendencias?» [en línea], en *Revista Inmanencia*. Vol. 5, n.º 1. 2016. Disponible en web: <http://ppct.caicyt.gov.ar/index.php/inmanencia/article/view/10831>.
- MARINA, José Antonio. «Porque la sociedad de la información está a punto de fracasar», en *Diario El Confidencial*. 27 junio 2017.

- MARTÍNEZ MURCIANO, Luis María (2017). *El tiempo está después. Tiempo y simulacro como paradigmas del cine posmoderno* [en línea]. Trabajo de fin de Máster en guion, narrativa y creatividad audiovisual. Universidad de Sevilla, Facultad de Comunicación, Sevilla. Disponible en web: <https://idus.us.es/xmlui/bitstream/handle/11441/64927/TFM-LUIS%20MARIA%20MARTINEZ.pdf?sequence=1&isAllowed=y>.
- MERCHAN GABALDON, Faustino. «Verdad frente a *posverdad*», en *La Tribuna del País Vasco*. 02 diciembre 2017.
- MICHAVILA NÚÑEZ, Narciso. «Opinión pública y conflictos armados», en *Revista Utopía y Sociedad* n.º 19/2002.
- MILOSEVICH-JUARISTI, Mira. «El poder de la influencia rusa: la desinformación», en *Real Instituto Elcano*. ARI 7/2017 – 20 enero 2017.
- ORTEGA, Andrés. «Campañas de desinformación: la debilidad de la desconfianza» [en línea], en *Blog del Real Instituto Elcano*. 5 diciembre 2017. Disponible en web: <https://blog.realinstitutoelcano.org/campanas-desinformacion-debilidad-desconfianza/>.
- ORTEGA, Octavio. «Favorece ignorancia *posverdad* en México» [en línea], en *Revista Reforma*. 26 marzo 2017. Universidad Nacional de México. Disponible en web: http://www.iis.unam.mx/pdfs/iismedios/marzo2017/02_reforma
- PIEDRAHITA, Francisco. *Sobre la posverdad*. Discurso de despedida del rector del ICESI.
- REDONDO, Myriam. *La doctrina del post. Posverdad, noticias falsas... Nuevo lenguaje para la desinformación clásica*. S.l., s.f., s.p.
- REPORTEROS SIN FRONTERAS. «RSF a Mark Zuckerberg: La sabiduría de las multitudes es ilusoria» [en línea], en *RFS*. Disponible en web: <https://rsf.org/es/noticias/rsf-mark-zuckerberg-la-sabiduria-de-las-multitudes-es-ilusoria>.
- SARASQUETA, Gonzalo. «*Pospolítica* ¿autopsia o metamorfosis del relato? El caso de Donald Trump», en *Revista Especializada en periodismo y comunicación. Questión*. Universidad de Río de la Plata, vol. 1, n.º 57, 2018: Verano (enero-marzo).
- UNIÓN EUROPEA. Grupo de Expertos de Alto Nivel. Informe para la Comisión Europea; «Un enfoque multidisciplinar de la desinformación».
- VERA, José Antonio. «Le llaman *posverdad* lo que no es sino manipulación y propaganda», en *Discurso durante la entrega de los XXXIV Premios Internacionales de Periodismo Rey de España*.
- VOSOUGHI, Soroush; ROY, Deb; ARAL, Sinan. «The Spread of true and false news on line», en *Science*. 9 marzo 2018. Vol. 359, Issue 6380, pp. 1146-1151 DOI: 10.1126/science.aap9559.
- VV.AA. Conferencia. «Gestión de Crisis», en *Departamento de Estrategia de la Escuela Superior de las Fuerzas Armadas* 2008.

WARDLE, Claire; KELIS NIELSEN, Rasmus; MANTZARLIS, Alexois; JIMÉNEZ CRUZ, Clara. «Seis puntos clave del informe sobre desinformación del Grupo de expertos de la Comisión Europea», [en línea], en *Periódico Eldiario.es*. 12 marzo 2018.

Capítulo segundo

Políticas de seguridad y defensa en la era de la posverdad

Alfonso Merlos

Resumen

La era de la *posverdad* viene marcada por la difusión estratégica a través de campañas metódicas y de alcance global, de informaciones de dudosa veracidad y de historias falsas que, en determinados procesos políticos y electorales, pueden representar una amenaza para la seguridad de los Estados y de la propia comunidad internacional. Las guerras de información basadas en el uso masivo y estudiado de las nuevas tecnologías de la comunicación exigen de nuevas estrategias de defensa que identifiquen con precisión la fisonomía de estos nuevos riesgos y sean capaces de atacarlos, neutralizarlos y amortiguarlos en sus efectos. Los planes y mecanismos a desarrollar e implementar tendrán forzosamente un carácter, en el corto plazo, dinámico y transformacional.

Palabras clave

Política, seguridad, defensa, *posverdad*, comunicación, inteligencia, redes sociales.

Abstract

The era of “post-truth?” is characterized by strategic diffusion, through methodic and global reach campaigns, untruthful information, and false stories that specific politic and electoral processes can represent a threat for the security of the states and for the international community. The information battles based on the massive use and studies of the new communication technologies require new defense strategies that identify precisely the physiognomy of these new risks and its ability to attack them, neutralize them, and reduce its effects. The plans and mechanisms to be developed and implemented will have to forcefully have a character, in the short run, dynamic and transformational.

Keywords

Politics, security, defense, “post-truth”, communication/s, Intelligence, networks, social.

Introducción: un futuro de incertidumbre y fragilidad

En la actual sociedad de la información, en la que cada impacto es global y susceptible de ser evaluado a través de una métrica cartesiana, los medios de comunicación tradicionales siguen conservando más alcance que aquellos portales o plataformas de difusión de contenidos que pueden llegar a coquetear con el concepto y la calificación de *fake news* en sus expresiones y sus mensajes.

Es la conclusión que sistemáticamente ha venido alcanzando el Instituto Reuters en países de nuestro entorno como Francia o Italia. No solo la credibilidad es mayor en los primeros casos, sino que son estos los que registran un mayor tiempo de permanencia para las audiencias. Y aun así, hay una segunda cara de la moneda: estos distribuidores de materiales (con frecuencia averiados) obtienen un número mucho mayor de interacciones que los *mass media* que históricamente han conformado el *mainstream*, produciéndose esta mezcla de efecto cascada y en red a través de: a) comentarios a las noticias; b) *posts* compartidos, y c) reacciones de los usuarios de otra índole¹.

¿Es tan masivo y, sobre todo, influyente el alcance de las *fake news* como suele darse por sentado a través de prejuicios u observaciones acientíficas que han calado en la opinión pública con carácter general? Es un hecho que las redes sociales terminan por recoger y hacer cristalizar un flujo de datos constante, inabarcable, imposible de verificar en su totalidad. Pero hay una segunda cuestión medular: ¿puede la *inteligencia artificial* llevar a cabo el trabajo, a través de la creación de algoritmos, de identificar las intoxicaciones que traen causa del denominado *periodismo ciudadano*?

La pregunta no es menor en la medida en que no solo las *fake news* tienden a echarse a rodar ladera abajo instituyéndose en una bola de nieve que engorda incesantemente con riesgos directos y daños colaterales múltiples y serios. Además, producen especialmente debate, polémica, polaridad, posiciones extremas. ¿Cómo alcanzar a señalar si el origen de un mensaje está en un robot? ¿Cómo descubrir si el original está programado? ¿Cómo identificar cuentas similares con acciones semejantes? ¿Cómo dejar al descubierto, uno por uno, aquellos seguidores que han podido ser comprados en la red social? ¿Sería viable disponer de una máquina que chequease un millón de noticias por hora lanzando un aviso inmediato sobre las que carecen de apego al principio de veracidad y, por tanto, parar el golpe antes de su conversión en *trending topic*?

Que la Unión Europea esté sopesando la opción de que estas plataformas sean obligadas a contratar editores humanos que comprueben la autenticidad de las informaciones no es un planteamiento en absoluto inmotivado o

¹ KLEIS, Rasmus; GRAVES, Lucas. «News you don't believe: Audience perspective on *Fake news*», en *Reuters Institute*. Octubre 2017.

caprichoso. Que estudie multas a aquellas webs que reproduzcan contenidos sin contrastar, tampoco. Todos los derechos y libertades fundamentales, en su ejercicio pleno, presentan sus límites, y estos tienen su fundamento ético y jurídico.

La sociedad de la información se ha transformado paulatinamente en una jungla en la que personas sin cualificación, sin formación o sin instrucción pueden erigirse en *influencers* durante horas o días con efectos devastadores, colocándose en la privilegiada posición de actores con capacidad para producir materiales caseros y colgarlos en la Red para obtener un impacto político que puede superar al de los medios convencionales, aprovechándose de un escenario de «desintermediación», en el que los ciudadanos son a la vez productores y consumidores, objetos y sujetos, proveedores y usuarios: un mundo sin los clásicos *gatekeepers* o cancerberos de las esencias del interés general.

Hoy es historia la comunicación en la que la emisión procedía de una o pocas fuentes y se vehiculaba hacia muchos receptores con escasa interactividad. Se han multiplicado los focos productivos: el envío de mensajes a una multitud en la que la stampa final es la de una selva en la que todos los «animales comunicativos» emiten y reciben simultáneamente; la *conectividad* genera automáticamente *sociabilidad* y opera en un marco, esencialmente, de *horizontalidad*.

¿Se trata en su espíritu y su plasmación de una revolución tecnológica que trasciende la pura técnica? ¿Puede haber en esta forma de ciberactivismo una raíz asociada a la profunda crisis de legitimidad de las instituciones políticas y representativas en numerosos Estados del mundo desarrollado?

Es evidente que el ciberespacio ha potenciado la capacidad táctica de ciertos actores preexistentes en los entornos operativos tradicionales, y que ha establecido un ecosistema favorable que ha conllevado la génesis y aparición de nuevos agentes y grupos de presión con capacidades relevantes. Y es evidente que el carácter viral y global de las redes sociales no solo ha actuado como altavoz de la información y la propaganda: está representando una amenaza a considerar para la seguridad y la defensa de organizaciones privadas y Estados. ¿Están desplegando, especialmente estos últimos, las políticas preventivas y reactivas adecuadas y útiles en tiempo y forma?

Repensando el concepto de interés nacional

El debate sobre la afectación de las *fake news* a las políticas de seguridad de los Estados y, por consiguiente, a su propia defensa, tiene pleno sentido, y va ligado a lo que sigue significando el interés nacional en pleno siglo XXI y en una sociedad internacional tan formidablemente globalizada en tantos aspectos, especialmente el de la comunicación y los transportes.

El interés nacional es una noción fundamentada básicamente en el símbolo jurídico del Estado nación, y es esencial para comprender el mundo en que vivimos. Desde que Tucídides por primera vez refirió que una identidad de interés es el más seguro de los vínculos entre Estados e individuos, se ha entendido el alcance, con el paso de los siglos, de lo que significa y en lo que se traduce la «razón de Estado»: la transformación de los intereses personales y particulares en una razón común entre individuos apoyada en una estructura política que será el Estado².

El cardenal Richelieu elaboró una concepción moderna del concepto de gobernar, no desde la perspectiva de los intereses particulares del gobernante, sino de los generales de la nación. Y esa idea sigue vigente. También la de Maquiavelo, al considerar que la supervivencia del Estado debe ser la principal preocupación y misión de los dirigentes, convirtiéndose en un fin en sí misma.

El paso de los siglos, y la sociedad actual tan influida por el relativismo y la relajación de ciertas normas éticas, ha visto cómo se ha ido derritiendo el sentido de «razón de Estado» equivaliendo a un «bien moral», el que deriva de la unidad de organización política; pero el papel del Estado como actor catalizador del Gobierno en la sociedad global sigue siendo hoy vital.

Atrás ha quedado, en los desvanes de la obsolescencia, la idea de Kenneth Waltz, según la cual el interés nacional se traduce en la lucha por la supervivencia de los Estados, en un entorno donde no hay autoridad supranacional que regule de forma efectiva sus relaciones. Sin embargo, sigue siendo la necesidad y el deseo de seguridad (traducida esta también en términos económicos) la que conduce a los Estados a intentar sumar y acumular cada día poder, incluyendo el que deriva de la posesión de la mejor información.

La influencia de los principios de la economía de mercado en los postulados liberales asociados al mínimo Estado es innegable, y ha dado lugar a una sociedad donde la defensa a ultranza de las fronteras clásicas ha perdido buena parte de su sentido. Así, los Estados que han intentado gestionar sus recursos y manejar sus potencialidades en clave de interés nacional no han dejado de apartarse de los poderosos motores de crecimiento de la economía mundial con el subsiguiente perjuicio. Hoy mismo es un riesgo, al menos a evaluar desde el plano teórico y en una fase embrionaria de los Estados Unidos de Donald Trump.

No hay interés nacional sin seguridad nacional. Y en la relación entre el primero y la segunda opera indefectiblemente la información: su cantidad, su calidad, su relevancia, su especificidad, su naturaleza... Un Gobierno que no disponga de la información adecuada, o que no evalúe adecuadamente aquella a la que pueda acceder, y que adopte decisiones contra su seguridad

² AAVV. *Evolución del concepto de Interés Nacional*, Monografías del CESEDEN, 2010.

nacional fracasará en la defensa de sus intereses: tanto los estratégicos e inmutables como los de coyuntura o pasajeros.

Una sociedad en la que el problema puede venir derivado no de la falta de información sino del exceso de la misma provoca que el Estado se enfrente a nuevos desafíos desde el punto de vista del análisis de riesgos y amenazas. Aquellos y estas obligan al desarrollo de nuevas estrategias y tácticas, de nuevos métodos para la extracción de información potable para la generación de inteligencia, con el fin último de disponer de la preparación necesaria y suficiente para enfrentar escenarios imprevistos.

En un mundo sacudido y convulsionado por el concepto de *posverdad*, los Estados se enfrentan a ciertas ecuaciones para la salvaguarda y la promoción de esos intereses nacionales que permanecen casi inalterables. En primera instancia, la definición de aquellos intereses compartidos (y no compartidos) con otros actores; en segundo término, la definición de los riesgos a los que se está sometido y el grado de cobertura necesario para su protección, y en tercer lugar, la concreción y materialización de los medios materiales y morales disponibles para incluir en la Estrategia de Seguridad Nacional. Esto ha significado y significa contemplar la tecnología y las posibilidades de financiarla y acoplarla a los mecanismos para la consecución de los objetivos establecidos, empezando por la defensa de la integridad, de la independencia y de la soberanía nacional.

Por encima de este enfoque, que tiene un componente de tradición y permanencia en el tiempo, carece de sentido omitir que los Estados, en la defensa de su propio interés nacional, se enfrentan hoy a fenómenos globales que propician riesgos y amenazas que están trastocando su propia fisonomía y que agravan o multiplican sus efectos. Entre ellos, las disfunciones de la propia globalización que, con frecuencia, se traducen en: a) desequilibrios demográficos; b) pobreza y desigualdad; c) cambio climático; d) peligros tecnológicos, y e) ideologías radicales y no democráticas.

Se trata, en su conjunto, de tendencias de largo alcance y estructurales con una inmensa fuerza para provocar desórdenes e inestabilidad en el sistema internacional. Y ello en un escenario en el que los Estados no constituyen (como antaño o como anteriormente los imperios) las únicas fuentes de poder: de un lado, porque una parte de su soberanía es cedida voluntariamente a cambio de beneficios acordados de la más diversa especie; de otro, porque la propia globalización ha facilitado que empresas multinacionales, e incluso organizaciones no gubernamentales, hayan podido erigirse en auténticos poderes transnacionales que compiten con los Estados para condicionar la política, la economía y algunos aspectos de la propia seguridad internacional.

El teatro de la *posverdad* afecta además de forma muy notable a los denominados *Estados fallidos* o *Estados frágiles*, aquellos que tienen una especial y grave dificultad o incapacidad para preservar y ejercer el monopolio legítimo de la fuerza, asegurar el respeto a la ley, aportar seguridad física a su pobla-

ción o suministrarle unos servicios públicos mínimos; aquellos que padecen conflictos armados prolongados, colapso institucional, abusos y enfrentamientos sectarios o a organizaciones de carácter tribal.

Y la afección no viene determinada siempre o únicamente (pensemos, por ejemplo, en Irak) por el hecho de que unidades insurgentes tengan acceso a las últimas herramientas tecnológicas y las exploten para la propalación de propaganda o falsedades. Viene, en parte, porque las *fake news* fabricadas desde las sociedades más económicamente desarrolladas (Estados Unidos, Europa y otras), que aluden a fenómenos ocurridos en los citados *Estados frágiles*, pueden condicionar las políticas que llevan a la práctica los Gobiernos de las primeras respecto del territorio de los segundos.

Aún más. Que Estados que operan bajo el paraguas, por ejemplo, de la OTAN sean incapaces de controlar los bulos (incluso en forma de campaña) que se difunden desde sus fronteras, puede terminar provocando que esos *Estados fallidos* objeto de la desinformación vean agravada su situación, produzcan un añadido de desestabilización sobre sus vecinos y contagien de incertidumbre a regiones enteras.

Hacia una transición en los modelos de seguridad

Toda guerra de información se sustancia en la distribución de datos o relatos intencionadamente manipulados al servicio de ciertos fines, o en ocasiones se basa en la aportación de información insuficiente o directamente en su omisión. No se trata, por tanto, de divulgar simples mentiras, sino de mensajes tanto verdaderos como falsos para producir el efecto del engaño en los receptores. El objetivo no es otro que el de desacreditar y debilitar a los oponentes, distorsionar así su percepción de la realidad, y, en ese sentido, se trata de una operación que se incardina de lleno en el ámbito de la defensa.

Cualquier modelo de seguridad por el que se apueste, y cualquier política que de él derive, busca identificar y gestionar los posibles riesgos para impedir que dañen los intereses fundamentales de cualquier comunidad, representada políticamente por un Estado o por un conjunto de ellos, como es el caso de la Unión Europea o la OTAN.

Es un planteamiento invariable, más allá de que el marco estratégico en el que se deba articular la estrategia de seguridad y defensa se vea afectado por nuevos fenómenos (¿coyunturales, estructurales?) como los que traen causa de todo lo que significa el universo de la *posverdad* en el campo de la información y las nuevas tecnologías.

Hoy han quedado completamente superados los modelos que parten de la base y argumentan que las relaciones internacionales solo se entablan entre Estados, y que por consiguiente las amenazas y los riesgos tienen carácter exclusiva o preponderantemente militar. Esta concepción, resultado de uno

de los paradigmas del realismo político que identificaba el principal foco de los estudios de seguridad con el fenómeno de la guerra, ha quedado desbordada —décadas atrás— por la proliferación y la diversificación de los actores con capacidad para acumular y ejercer el poder en la sociedad internacional. Aún más, ni siquiera hoy puede colegirse que la política exterior solo exista entre Estados nación soberanos, en la medida en que estos no son los únicos que disponen de capacidad para ejercer la coacción sobre terceros actores y, así, moldear el orden internacional.

Sobre el papel, la globalización de las comunicaciones induce al aterrizaje en un marco estratégico muy influido por el idealismo y por la configuración de una amplia comunidad (en realidad todos los habitantes del planeta) conectada, con relaciones esencialmente cooperativas y con las barreras entre los pueblos (no solo las fronteras físicas) derribadas o ausentes.

Sin embargo, y a pesar de que existan por añadidura reglas comunes e instituciones que limiten los conflictos, a pesar de que existan en la sociedad global ciertos valores comunes reconocidos y aceptados, el empuje de las *fake news* ha introducido en el ecosistema informativo internacional una idea de descontrol, de anarquía, de cierto caos. ¿Es posible contenerlo o revertirlo?

El hecho es que este fenómeno particular y el contexto más amplio definido como *posverdad* se lee mejor si cabe a la luz de la doctrina elaborada al finalizar la guerra Fría por los autores agrupados en la escuela de Copenhague. En términos históricos recientes, apenas hace tres décadas, ya cobra fuerza el dibujo de un nuevo concepto de seguridad en el que los riesgos y las amenazas incluían, sin ningún género de dudas, fenómenos de carácter no tradicional.

Así, la tendencia que cobra cuerpo y vigor es la de un grupo de *amenazas no militares* a la seguridad, tremendamente heterogéneas, que pasan al primer plano y que se concretan en hechos incontestables como el subdesarrollo, la corrupción, el derroche de los recursos o las violaciones de los derechos humanos, entre otros. Y esta amalgama provoca que al Estado nación, en su gestión, se unan otros actores del sistema (no estatales) u organizaciones regionales.

Desde este prisma, y en el interior de este encuadre, la apuesta por un marco de *seguridad colectiva* ha basculado a otro de *seguridad compartida*³. Así, si la sociedad internacional contemplaba de forma más rotunda e inmediata un compromiso de acción, incluso armada, contra el infractor que ponía en peligro la paz y la seguridad, hoy procura desechar la idea prioritaria del uso de la fuerza haciendo hincapié en herramientas ligadas a la confianza y la cooperación.

³ CALDUCH, Rafael, *Dinámica de la Sociedad Internacional*, Madrid: Ceura, 1993.

La era de la *posverdad* se configura como un espacio de tiempo en el que la gestión de los desafíos se produce de forma más interdependiente y con un mayor énfasis en las actuaciones responsables y eficaces, y en el que, desde espacios territoriales como la Unión Europea, se diseñan estrategias globales para mantener un estatus de libertad y prosperidad, combatiendo fenómenos como el terrorismo, abordando cuestiones capitales como las que resultan de la ciberseguridad y contemplando en primer término aspectos vitales que conciernen, por citar un caso, a la seguridad en los suministros energéticos.

También esta era pone en el primerísimo orden el concepto de *resiliencia*⁴, entendida como la capacidad de los Estados y las sociedades para reformarse, soportando situaciones adversas extremas (incluidos los desastres) y gozando de fuerte impulso para superar las crisis internas y externas. Y, por añadidura, coloca nuevas responsabilidades sobre las organizaciones de las que esos Estados son parte.

En el caso de la Unión Europea, la redefinición de su estrategia de seguridad recoge una visión estructurada en varios parámetros sobre los que acometer una inversión incesante y colectiva.

De un lado, se subraya la necesidad de exhibir *credibilidad*, siendo necesario en este sentido un desarrollo pleno de todas las herramientas de la política exterior, desde la investigación hasta la lucha contra el cambio climático, pasando por las infraestructuras, la movilidad, el comercio, la diplomacia y el desarrollo. De otro, se enfatiza la oportunidad de disponer de *rapidez en la respuesta*, de acuerdo a la velocidad a la que se producen los cambios, y esto flexibilizando y ajustando las decisiones a las prioridades y los objetivos de forma exigente y permanente. Por último, se pone el acento en la *imagen de integración*, tan útil en todos los ámbitos para trasladar una percepción de coherencia y, por consiguiente, de solvencia.

En el caso de España, el fin de la seguridad nacional se configura como un estado a alcanzar a través de la acción y de una serie de principios de actuación en los que cobra progresivamente más sentido:

- a) La *anticipación*, que implica disponer de los medios necesarios para alertar y prevenir de todos aquellos elementos que puedan poner en peligro la seguridad nacional.
- b) La *interdependencia responsable*, que supone contribuir a la creación y el fortalecimiento de marcos e instrumentos multilaterales (con socios europeos e internacionales) que garanticen la seguridad.
- c) El *enfoque integral*, que se plasma a través de la implicación, coordinación y armonización de todos los organismos, actores y recursos del

⁴ DE CARLOS, Javier. «Tendencias Globales, Seguridad y Resiliencia», en *IEEE*, Documento de Investigación. Junio 2017.

Estado para hacerlos converger en la consecución de los objetivos fijados en el sistema de seguridad.

- d) La *resiliencia*, que se manifiesta en la capacidad de resistencia y recuperación mediante instrumentos flexibles, susceptibles de adaptarse a las más diversas circunstancias y de sobreponerse a las situaciones de crisis, minimizando y absorbiendo sus consecuencias negativas.

Nuevos horizontes de la cultura de defensa

Difícilmente puede llevarse a cabo un análisis pormenorizado y profundo de las derivadas que la era de la *posverdad* conlleva en términos de seguridad nacional si no se delimita de dónde viene y hacia dónde va la *cultura de defensa*. Y esta no puede sino entenderse como un conjunto de conocimientos, normas, valores, metas, actitudes y prácticas compartidas socialmente y orientadas a proteger y garantizar los intereses nacionales. En definitiva: un proyecto compartido.

El punto de salida del que debe partir el análisis sobre la evolución de la cultura de defensa en los nuevos parámetros que marcan la sociedad global de la información y el conocimiento es: ¿cuáles son los motivos que justifican la necesidad de seguir fomentando esa idea apenas naciente en su concepción moderna?

De un lado, parece positivo que se haga preciso generar conciencia sobre la utilidad de percatarse de la importancia de las cuestiones relativas a la seguridad nacional en todas sus dimensiones. De otro, parece positivo que se haga útil asumir una serie de deberes y obligaciones respecto a la seguridad nacional.

Esta segunda causa, interpretada con cierto sesgo ideológico, puede ser desvirtuada al hacerse equivaler al imperativo de construir algún tipo de espíritu grupal de signo patriótico. Pero no es ese su fundamento ni su meta. La referencia es clara, y está dirigida a los beneficios colectivos que son consecuencia del hecho de que todos los sectores sociales y el conjunto de la ciudadanía conozcan las principales amenazas y riesgos a los que se exponen, así como las formas de actuación que el Estado trata de llevar a cabo para atajarlos, con el mayor grado de transparencia de las organizaciones dedicadas a facilitar seguridad.

Un proyecto de cultura de defensa exitoso no puede sino fomentar el sentido cívico y de corresponsabilidad, favorecer la percepción general de protección, ampliar la confianza y el prestigio social de las Fuerzas Armadas para otorgar más legitimidad a la tarea que desempeñan y concienciar incluso sobre el uso responsable de todos los recursos que ofrece Internet.

En este sentido, la información, la comunicación y la *participación de todos* en la *seguridad de todos* no puede sino derivar en un grado más elevado de co-

hesión donde del compromiso solidario se desprenden mejores resultados en la acción.

La seguridad (siendo en términos absolutos inalcanzable), especialmente en democracia, es la garantía de la construcción y consecución de otros fines. Es el mejor paraguas para la salvaguarda de los derechos fundamentales y las libertades públicas. Por tanto, la cultura de defensa puede y debe promover no el planteamiento de que el ciudadano ha de sacrificar hasta perder derechos y libertades para estar seguro, sino, muy por el contrario, el foco de que el ciudadano habrá de disponer de seguridad para poder ejercitar en toda su plenitud sus derechos y libertades, empezando por aquellos que nacen en su ámbito más íntimo, privado y personal.

Son las sociedades abiertas los entornos con más ventajas para que quienes las conforman, civilmente, entiendan la relación inversamente proporcional entre seguridad y riesgo: a mayor grado de consecución de la primera, menos presencia del segundo, y viceversa. Y son las sociedades abiertas los marcos idóneos para que se pueda desarrollar una auténtica conciencia sobre el hecho de que: a) hay amenazas que provienen de agentes hostiles; b) hay bienes que se deben proteger, determinando en primera instancia aquellos esenciales, y c) hay una cobertura, mecanismos que deben articularse para alcanzar la seguridad.

La permanente transformación de la naturaleza de las amenazas ha provocado una readaptación constante de las prioridades de la política exterior y de defensa en todo el planeta. Hoy la seguridad humana se busca defendiendo más personas que territorios, y eso implica, en muchos casos, defender como bienes el propio Estado del bienestar con los derechos y libertades que lleva aparejados y que resultan de un proceso acumulativo de conquistas históricas y colectivas, ya irrenunciables.

Por lo que respecta a las guerras de información, es incontrovertible que la naturaleza misma del conflicto bélico no ha cambiado desde el inicio de los tiempos, pero los medios y modos de afrontarlo no han dejado de virar. Hoy, la democratización de los avances tecnológicos y determinadas facilidades de acceso, sumado este factor a la proliferación de adversarios con conocimientos para convertir en armas esas herramientas, está propiciando cambios cualitativos y viscerales en los tradicionales paradigmas de confrontación. Ese cambio viene determinado, sobremanera, por el empleo de medios de comunicación digital y de redes sociales como arietes para producir hostilidad (en ocasiones, en insufribles cantidades industriales).

La Inteligencia: ayer, hoy y mañana

La sociedad del conocimiento en la que el concepto de *posverdad* ha irrumpido fuertemente, deslizándose por numerosas vertientes, se configura como un sistema complejo en el que la inteligencia, como ha ocurrido histórica-

mente pero hoy de forma más acentuada, está llamada a jugar un papel de primera magnitud.

La inteligencia, tanto la humana como la propia de los servicios secretos de los Estados y las corporaciones privadas, combina la dotación de significado a la realidad con la anticipación ante esa realidad. Así, Estado y empresa disponen de inteligencia cuando usan aquella que obtienen y almacenan para construir un significado propio de su realidad, la de su organización y su entorno.

Ese conocimiento es usado para adoptar decisiones sobre el futuro: gestionando el riesgo, anticipando amenazas (también oportunidades) y, en el mejor de los casos, actuando sobre el momento para conformar posibles futuribles donde la organización fomente ventajas competitivas.

Las amenazas y oportunidades que más sorprenden, con un alto impacto en un país, suelen tener origen en sectores no conocidos o no explotados. Establecer un sistema de inteligencia exige dedicar medios para conseguir unos retornos que se percibe llegarán no inmediatamente, sino a medio y largo plazo. Por consiguiente, la seguridad está relacionada de forma directa con la inteligencia y la vigilancia.

Pero incluso en el mundo de las *fake news*, de la intoxicación difundida masivamente a través de campañas en redes sociales y otros medios tecnológicos, la utilización de la inteligencia no ha supuesto un cambio. Se ha transformado la cultura informacional como recurso intangible, la supervisión de los cambios en el entorno, la circulación del conocimiento en redes.

También el espionaje está variando sensiblemente las coordenadas en que se desarrolla, sin mutar su esencial naturaleza. Sigue siendo una actividad perpetrada conscientemente para penetrar en un espacio informacional protegido o descuidado, a fin de conseguir un incremento de conocimiento por medios encubiertos, insospechados o desconocidos por su legítimo propietario. Sigue siendo esa actividad con la que se busca información protegida bajo diferentes niveles de clasificación y de accesibilidad muy limitada, cuyo contenido es sensible y de alto valor para el conocimiento de capacidades e intenciones de un enemigo, e incluso de un aliado.

Hoy, en plena ola de democratización y expansión casi ilimitada en el uso de nuevas tecnologías, se está incrementando el riesgo de accesos no permitidos y robos de esta información que ponen contra las cuerdas a su legítimo dueño y le generan vulnerabilidad. No solo el robo de información secreta militar, sino industrial, económico-financiera o de índole política.

En efecto, el signo de los tiempos ha conllevado al auge del espionaje digital, una modalidad de ciberataque directamente instigado contra la confidencialidad de los datos en la que el uso de «armas de información» se lleva a cabo para alcanzar un acceso no autorizado a redes, sistemas y repositorios electrónicos considerados de interés estratégico para, por ejemplo, un Estado.

Es este marco el que impone a las organizaciones volcar sus esfuerzos con especial énfasis en distintos ámbitos y con distintos objetivos: el primero, el de alcanzar la independencia tecnológica a través de la búsqueda de la autonomía en el desarrollo e implantación de soluciones y dispositivos para alcanzar niveles óptimos de seguridad de datos; el segundo, el de elevar al máximo nivel la protección de información sensible, desarrollando políticas de defensa eficaces al cortocircuitar eventuales agresiones, y el tercero, el de reforzar la propia función y las capacidades de los equipos de respuesta a emergencias informáticas para garantizar una óptima gestión de la calidad en seguridad de la información⁵.

Proteger hoy el conocimiento significa hacerlo no solo sobre el contenido sino sobre los propios canales por los que discurre desde su generación hasta su explotación final, y de los propios departamentos en los que se almacena o recopila; significa que las empresas que lo producen con aplicaciones a la innovación industrial deben mantenerlo con frecuencia en secreto para salvaguardar su posición en un contexto internacional competitivo, pudiendo generar así valor añadido.

En una sociedad de la información en la que es creciente el número de actores que queda públicamente expuesto, perder información repercute, además de económicamente, en la pérdida de reputación de la organización atacada en el ciberespacio. Y este riesgo es permanente y alto en la medida en que cada día grupos más pequeños trabajan en modo mercenario en todo el mundo en la cancha del ciberespionaje.

Y aun así, la era de la *posverdad* y de la *deep web* sigue siendo la era de la sobreabundancia de fuentes abiertas. En este sentido, sería imprudente —a cualquier efecto de captación, análisis y explotación de información— ignorar la que fluye a través de las redes sociales, ya sea por desconocimiento o por infravaloración. Al contrario: puede resultar decisiva para completar y redondear el ciclo de inteligencia.

Por esta razón, dos de las principales amenazas del uso de datos provenientes de las redes sociales como fuente de investigación son la información falsa y la *infoxicación*. Por Internet fluyen todo tipo de contenidos sin filtrar, salvo en países determinados en donde se aplica censura, y eso implica que el celo debe extremarse en la valoración del mensaje y la fuente. Del mismo modo, por las redes fluye el ruido inútil que dificulta la obtención de información realmente relevante, y el uso deliberado y sistemático de las nuevas tecnologías (de este magma) en modo campaña puede movilizar rápidamente a millones de personas, con los problemas de seguridad que ello puede generar.

⁵ DÍAZ MATEY, Gustavo. *Los servicios de inteligencia ante el siglo xxi*, Ediciones Chavín, 2011, pp. 167-190.

Un hándicap para Estados y organizaciones económicas con fuertes aparatos de inteligencia es la imposibilidad de controlar la herramienta. Las redes se encuentran en manos de grandes corporaciones que definen sus propios objetivos y necesidades⁶ y que operan sin considerar el inmenso daño social que pueden producir conglomerados o individuos antisistema que, simplemente, difunden su ideología, realizan captación de nuevos miembros, explican su agenda o ejercen influencia⁷.

Dados estos parámetros, ¿no resulta hoy imprescindible como nunca que la propia sociedad civil adquiera una cierta *cultura de inteligencia* y que lo haga a través de una mecánica de sensibilización pública que mejore el conocimiento por parte de los ciudadanos de los fines y las funciones de sus servicios de información como institución que forma parte del Estado democrático y que actúa al amparo de la legislación y es controlado por esta?

El arma de doble filo de las TIC

Internet y el resto de Tecnologías de la Información y la Comunicación han determinado, y lo siguen haciendo, importantísimos cambios sociales, y han llevado al primer plano la ciberseguridad como conjunto de herramientas, políticas, conceptos y salvaguardas, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas y seguros que pueden utilizarse para proteger los activos de la organización y a los usuarios en el ciberentorno.

Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los servicios o aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios y la totalidad de la información transmitida y/o almacenada en ese ciberentorno, y la seguridad vuelve a ser aquí crucial, el concepto clave, para entender la inevitabilidad de trabajar en la protección de eventuales agresiones.

Los ataques 3.0 pueden perjudicar y perjudican hoy a sistemas complejos, golpeando a individuos, a la propia sociedad civil, a empresas y a los Estados. Los *malware* (códigos maliciosos capaces de actuar de forma inadvertida) pueden operar hoy sobre cualquier ordenador, y los programas espía tienen capacidad para recabar información sobre cualquier entidad, comprendiendo datos personales del espionado, sus acciones en el ciberespacio, los contenidos de su disco duro o las características de sus conexiones.

Hay más: programas de suplantación de identidad (*pishing*) distribuidos a través de correo electrónico, idénticos a la correspondencia enviada por or-

⁶ PINTADO RODRÍGUEZ, César, «Las redes sociales y la defensa. Un análisis DAFO», en IEEE, Documento de Opinión. 119/2013.

⁷ Aún así, plataformas como Facebook, en casos extremos han actuado clausurando a, por ejemplo, grupos yihadistas o bandas de neonazis entregados a la apología del racismo.

ganizaciones bancarias o marcas legales y que incluyen enlaces que redireccionan a páginas falsas desde las que se absorben datos confidenciales. O, en el caso de los *adwares*, accesos a publicidad camuflados en programas que recopilan y envían datos confidenciales del usuario sin su conocimiento.

En una era supeditada sobremanera al uso de las nuevas tecnologías, la ciberguerra (las operaciones orientadas a penetrar sin autorización los ordenadores y sistemas o redes de información de algún Estado con el propósito de perjudicarlo) marca el signo de los tiempos.

Alterar, perturbar o impedir el funcionamiento de los equipos informáticos afectados o de los objetos que están controlados por dichos equipos, dañar los datos en ellos contenidos o introducir información falsa conforman una galería de acciones incluidas en la caja de herramientas de toda suerte de malhechores. No solo se trata de actuaciones cibernéticas de apoyo a operaciones bélicas convencionales en el marco de misiones militares, sino de aquellas que se implementan exclusivamente en el ciberespacio, de forma autónoma e independiente.

Precisamente, en la medida en que los ciberataques se erigen en una de las amenazas más peligrosas y con mayores posibilidades de desarrollo a corto plazo, cualquier estrategia de seguridad nacional debe tener hoy como objetivo prioritario garantizar la integridad, confidencialidad y disponibilidad de los sistemas que soportan la prestación de servicios ampliamente utilizados, comenzando por la gestión de las infraestructuras críticas del Estado⁸.

Estas últimas se encuentran, vía grupos subversivos que operan en el ciberespacio, en la parte más alta de su lista de objetivos por las averías económicas que puede producir su destrucción o interrupción y por su virtualidad de garantizar la fiabilidad de las redes de abastecimiento del gas, de sistemas de transporte, de distribución de petróleo o del propio tendido eléctrico.

La metamorfosis en los procesos de comunicación

La comunicación es una de las herramientas en las que se apoya la legitimidad de acción de cualquier persona con deberes y responsabilidad de actuación en el campo de lo público. Una buena comunicación contribuye a la transparencia, a generar confianza y a rendir cuentas ante la ciudadanía. Pero en el ámbito de la seguridad, por la convicción de que compartir información debilita y hace vulnerable, suele prodigarse la incomunicación y el secreto; por consiguiente, la opacidad.

En efecto, el ámbito de la defensa presenta una serie de singularidades (muchas de ellas obvias) que invitan e imponen restricciones en ocasiones in-

⁸ EFE, «España superará los 700 ciberataques en infraestructuras estratégicas en 2017», 6 de junio de 2017.

eludibles a la difusión de datos y mensajes. De hecho, el exceso informativo en este campo: a) produce el efecto perverso de brindar conocimiento a los actores generadores de amenazas y, por tanto, les allana su camino para causar daños, y b) puede contribuir al pánico social, en la medida en que la sensación ciudadana de seguridad e inseguridad es subjetiva: la primera crece lentamente, la segunda se dispara exponencialmente.

Hoy, como en el inicio de los tiempos, la información es expresión de poder. El mandato representativo en democracia tiene fuerza cuando el ciudadano se siente protegido en sus intereses, depositando su alícuota parte de poder en unos representantes que van a velar por él. La ocultación de información puede provocar una ficticia sensación de seguridad, porque los riesgos y las amenazas siguen ahí.

En la era de la *posverdad*, la globalización económica y cultural corre paralela a la globalización de las amenazas, que no solo son transnacionales sino extraestatales, como el ciberterrorismo y el crimen organizado con medios tecnológicos. Algunos de los actores que practican estas formas de violencia (sea con fines políticos o crematísticos) buscan con frecuencia un impacto mediático, y eso significa que la comunicación no solo es relevante para las instituciones oficiales de poder, también es crucial para quienes pretenden revertir los patrones de seguridad estatal.

Aún más. En la era de las *fake news*, los grandes medios de comunicación de masas siguen sirviendo de canal fundamental para alcanzar vastas audiencias, pero han proliferado los conductos que hacen posible evitar su mediación para copar la atención de los ciudadanos. Eso se traduce en que se ha ensanchado el terreno de juego para expandir rumores, para confundir la conciencia colectiva mediante la duda, para crear estados de incertidumbre política y social, para malograr debates de interés general... o para desestabilizar y provocar cambios de tendencia en los procesos electorales.

En ese espacio en el que confluyen la política y la seguridad se está detectando la capacidad de actores que pueden jugar en favor de la fortaleza de un partido o un régimen, que pueden aumentar artificialmente la popularidad de un candidato o un líder, que pueden hacer invisible a un contrincante destruyendo su reputación o que pueden ahogar las críticas a autoridades, sistemas políticos o estructuras del Estado⁹.

Especialmente en el ámbito de la seguridad y la defensa, por su dimensión estratégica, los mensajes emitidos por las instituciones han de ser consistentes y coherentes. Cualquier tipo de incongruencia (por apariencia pequeña que tenga en tamaño) termina por erosionar la imagen de la institución, y esos mensajes deben contemplar las «líneas rojas» que dejan al margen del discurso público por pura necesidad, lo que se debe ocultar. Una técnica

⁹ PINTADO RODRÍGUEZ, César. «Las redes sociales...», art. cit.

—la de la ocultación— nada fácil de aplicar, con criterios perfectamente definibles y explicables por sus potentes implicaciones éticas y profesionales.

En efecto, la gestión de la información en el área de la defensa adquiere una dimensión trascendente. A partir de su contenido, su forma y el medio por el que se transmite se configuran las percepciones en la calle. Y el gran problema al que se enfrentan las estructuras de seguridad interior es qué comunicar y cómo hacerlo cumpliendo con los criterios de transparencia que incesantemente empujan desde todas las direcciones imaginables.

Un escenario de audiencias volátiles y empoderadas

La multiplicación de actores con capacidad de comunicar e influir en la era de la *posverdad* ha dejado obsoletos ciertos modelos con los que se pretendía explicar la dinámica, la razón de ser y los efectos del ecosistema informativo, tanto a nivel nacional como internacional.

De acuerdo a los modelos de élite dominantes, como el de «propaganda o fabricación del consenso» de Herman y Chomsky¹⁰, los medios son simples instrumentos del sistema capitalista y de quienes lo controlan y trabajan por su supervivencia. En el modelo «indexado» de Bennett¹¹, el discurso político de quienes dominan la vida económica de la sociedad se reproduce y amplifica, produciéndose solamente debates muy debilitados en casos de disenso entre las élites.

La democratización y expansión de las nuevas tecnologías ha propiciado, sin embargo, que se hayan abandonado esas formulaciones fundamentadas en audiencias pasivas y *mass media* actuando unidireccionalmente. Así, la opinión pública alcanza hoy la misma importancia que el resto de sujetos comunicativos, al ser sus percepciones y valoraciones capaces de modificar la diplomacia, los conflictos y las políticas de seguridad y defensa. Los medios tradicionales se sitúan, en consecuencia, en una ubicación intermedia: sin ser instrumentos propagandísticos del Gobierno o el Estado ni tampoco adversarios abiertos.

Aun así, en el caso de Europa y de España, encontramos la irrupción reciente, en las dos últimas décadas, de televisiones como Hispan TV o Russia Today, que han roto ciertos esquemas de la percepción de las audiencias y las han sometido a encuadres nuevos y sesgados sobre temas complejos, como el

¹⁰ PEDRO, Joan, «Evaluación crítica del modelo de propaganda de Herman y Chomsky», en *Revista Latina de Comunicación Social*, n.º 64, 2009.

¹¹ MORENO, José Manuel, «La importancia de los encuadres en la política exterior y los nuevos desafíos comunicativos», en *Análisis GESI*, 33/2017.

conflicto palestino-israelí o los conflictos de Afganistán, Siria o Ucrania, llegando a facilitar informaciones de dudoso origen y veracidad¹².

El fenómeno no es baladí, especialmente considerando que los efectos sobre las audiencias en cuestiones de política exterior son pronunciados: la opinión pública, en términos generales, carece de convicciones ideológicas y posicionamientos fuertes, y dispone de un reducido nivel de conocimiento de temas, como regla, de pronunciada profundidad.

Precisamente por eso, el poder de Internet y, por tanto, de las redes sociales, pudo provocar (en clave de instrumento de movilización) las revueltas de 2011 de la llamada Primavera Árabe, que terminaron por derrocar los Gobiernos de Túnez, Egipto y Libia. En efecto, de forma impactante e imprevisible, el uso de las herramientas cibernéticas desató una tormenta de efectos estratégicos y duraderos, condicionando el inicio, el desarrollo y el enlace de esas revueltas y esos conflictos. La propia democratización de la Red ha tenido una influencia directa sobre la reestructuración de la cobertura de los conflictos armados, al fracturarse el monopolio ejercido por los medios tradicionales. El caso emblemático de la CNN y de su cobertura de la guerra de Irak, con la presencia estelar de Peter Arnett, ha quedado relegado al baúl de los recuerdos¹³.

La aparición de blogs y portales de noticias alternativos ha terminado por configurar un entorno diferente, competitivo, en el que quedan mitigados (cuando no anulados) los procesos de *gatekeeping*, generándose un contexto mucho más volátil e inseguro. La propia propagación de bulos o noticias de difícil confirmación ha terminado por afectar colateralmente (y de manera en cierto modo paradójica) a los viejos medios, deteriorando su imagen profesional ante lectores y espectadores.

Injerencias imprevistas en procesos electorales

Los *hackers* se han convertido en actores invisibles que pueden influir e influyen en los procesos electorales de medio mundo. Es un hecho este que replantea preguntas sobre el uso de las nuevas tecnologías en las sociedades democráticas. Y esta circunstancia debe unirse al hecho de que las redes sociales están debilitando algunas de las condiciones que históricamente han posibilitado la existencia de Estados nacionales democráticos: ¿cómo es posible que millones de votantes reciban por sistema noticias falsas promovidas en la generalidad de los comicios que celebran las primeras democracias del planeta?

¹² RUIZ DE LA SERNA, Ricardo. «La influencia de Irán en España», en *Libertad Digital*. 21 enero 2016.

¹³ VALENZUELA, Javier. «CNN se despide de su reportero estrella, Peter Arnett, tras un reportaje falso», en *El País*, 20 abril 1999.

La era de la *posverdad* conduce a una reflexión de vastas dimensiones. El sentimiento de cohesión que los ciudadanos de las naciones modernas han sentido tradicionalmente entre sí (el grado en el que podían considerarse parte de una comunidad nacional) estaba en gran medida facilitado por la función que cumplían los medios de comunicación de masas. Ahí queda el célebre aforismo de Arthur Miller: «*A good newspaper is a nation talking to itself*».

Los sistemas de gobierno democráticos han dependido en un grado u otro de ese sentimiento compartido de comunidad que incluso ha posibilitado *políticas de Estado* que nacen de la idea de que los ciudadanos hacen converger sus intereses y convicciones ineludiblemente en un puñado de cuestiones decisivas.

En el pasado, las sociedades han dependido de *intermediarios de los intereses generales*, por lo general periodistas, para enmarcar y articular ese sentimiento de realidad compartida. Hoy, las personas reciben fundamentalmente el tipo de información que ellas mismas han seleccionado y configurado previamente o (más temerario) que terceras partes han decidido que les interesa conocer.

Este coctel desinformativo explosivo para la democracia se ha cruzado con el fenómeno del hackeo electoral. Los protagonistas de estos delitos han vulnerado los sistemas de comunicación de figuras políticas, de partidos y de parlamentos. Han vulnerado la integridad y han manchado la limpieza de procesos para favorecer a unos candidatos o programas sobre otros. Y así se entiende el *doxing*, procedimiento selectivo y estratégico implementado con el ánimo de inclinar la balanza electoral de uno de los lados.

Pero hay mecanismos de contaminación más sigilosos y perversos. En la era de la *posverdad* las opiniones políticas son más proclives a polarizarse. ¿Por qué? Por razones que emanan de tiempos pretéritos, de la vicisitud en la que un votante se ve obligado a decantarse por una u otra propuesta. Pero hoy esas tendencias son exacerbadas, a más abundamiento, por los algoritmos de las redes sociales que conducen al usuario, inexorablemente y con presencia de motores predictivos y de *inteligencia artificial*, hacia informaciones que coinciden con sus preestablecidas preferencias. ¿Acaso no debilita cada *news feed* la deliberación democrática para radicalizar las convicciones propias e intransferibles?

Y, aun así, el Estado democrático y social de derecho se enfrenta a fórmulas más agresivas de injerencia en campaña. Es la que se vincula a la usurpación de identidades, al *hacking* de registros electorales y a la propia intervención de los resultados, haciendo inseguros los escrutinios. Es la razón por la que se ha estimulado inevitablemente el levantamiento de barreras tecnológicas (algunas apoyadas en la criptografía, incluso el *blockchain*) para blindar los comicios.

Indiscutiblemente, solo el diseño arquitectónico de una nueva gobernanza cibernética internacional permitirá evitar una crisis de confianza generalizada y global de los ciudadanos frente a las instituciones democráticas¹⁴.

Realidades y mitos de las operaciones rusas

En términos generales, los Gobiernos de distintos Estados (incluido España) han sido extremadamente cautos al evitar atribuir a Moscú la autoría de las noticias falsas que han inundado cíclicamente las redes sociales en momentos sensibles, como procesos electorales o crisis internas de diversa naturaleza. Y eso, a pesar de que una y otra vez se ha constatado que porcentajes altísimos (en ocasiones superando el 50%) de los perfiles que han difundido *fake news* procedían de servidores alojados en territorio ruso.

Para la opinión pública y el *mainstream* de las naciones europeas y Estados Unidos, ha quedado suficientemente acreditado no obstante que Rusia ha intervenido activamente en medios y redes por medio de mecanismos de propagación de noticias falsas en todos los procesos políticos de relevancia occidentales en los últimos años, incluyendo el proceso independentista catalán y el referéndum a favor del Brexit en Reino Unido.

El hecho es que no resiste a la discusión que, como en el caso de otras naciones, para la Federación Rusa la desinformación es un método militar asimétrico e indirecto en los modernos espectros de guerra híbrida, y es, por consiguiente, un instrumento principal en su estrategia de influencia geopolítica.

Como otras naciones, la rusa ha manejado como medidas activas en la guerra de información la propaganda, la provocación o la manipulación de los medios de comunicación extranjeros. Desde Lenin, la militarización de la información ha sido habitual en una estrategia que ha pivotado sobre la influencia, no en la fuerza bruta, siendo su objetivo trascendental romper la coherencia interna del sistema político, económico y militar del enemigo, no aniquilarle.

Esa guerra informativa tenía y tiene como medios «adoctrinar» a la población para desestabilizar la sociedad y forzar a los Estados a tomar decisiones favorables a los intereses de sus oponentes. Desde las propias Fuerzas Armadas Rusas se ha señalado que lo que más distingue la guerra convencional de la híbrida es la simultaneidad en esta de las batallas en tierra, mar, aire y espacio informativo, y el uso de métodos indirectos y no lineales para alcanzar objetivos militares¹⁵.

¹⁴ SANTISO, Carlos; DAHAN, Mariana. «Cómo protegemos nuestras democracias en la era digital», en *El País*. 23 agosto 2017.

¹⁵ MILOSEVICH, Mira. «La “combinación”, instrumento de la guerra de información de Rusia en Cataluña», en *Análisis del Real Instituto Elcano*. 7 noviembre 2017.

En la última década, tanto en los planos oficial como oficioso, Rusia ha trabajado de manera constante y activa para imponer «un punto de vista alternativo» en la óptica de los ciudadanos (principalmente, pero no solo) de Europa y Estados Unidos. ¿Por qué?

A la Federación Rusa le ha beneficiado difundir globalmente el mensaje de que su poder está bajo permanente lupa y amenaza de un Occidente hegemónico y decadente que aspira a excluirla del orden internacional. En el caso de la Unión Europea, al tratarse de una entidad política al borde del colapso y la desintegración, incapaz de solucionar sus múltiples crisis; en el caso de la OTAN, al funcionar como una organización desgastada y sin horizonte ya, con riesgo de provocar la Tercera Guerra Mundial por su afán infundado de expandirse hacia las fronteras del Este.

Así, ha convenido la difusión de contenidos (no solo noticias) que han perseguido poner en evidencia la disfuncionalidad del sistema político, económico y social de la democracia liberal, creando confusión y sembrando dudas, favoreciendo las diferencias o la desunión de los miembros de instituciones adversarias, transmitiendo que ni la integración continental es el camino más seguro hacia la prosperidad ni el movimiento de construcción europeo es irreversible¹⁶; esa percepción ha alimentado a los partidos populistas y continentales extremistas ubicados tanto en la derecha como en la izquierda.

La guerra de información/desinformación alentada desde Moscú no solo ha ido encaminada a generar un marco en el que se propalan noticias de dudosa veracidad, sino a poner el foco sobre la figura de *agentes independientes*, activistas antiglobalización o militantes de diversas causas fuertemente ideologizados y radicalizados para elevar la voz en favor de causas que, de algún modo, sirven a los objetivos de poder de Rusia: uno de ellos, crear divisiones para minar progresivamente la fortaleza de Europa y sus propios instrumentos y mecanismos de respuesta ante diversas coyunturas.

El hecho es que una galería de medios prorrusos no solo han hecho campañas encubiertas a favor del Brexit, Marine Le Pen y la ultraderecha alemana; igualmente, han mantenido una línea editorial sin contemplaciones al matiz y alineada con el punto de vista de Moscú sobre la guerra en Siria, las provocaciones de Corea del Norte o la presidencia de Donald Trump.

En definitiva, en la era de la *posverdad* los medios prorrusos han identificado los flancos más vulnerables de Europa y sus crisis (moneda única, Estado del bienestar, inmigración/refugiados) para desacreditar todo un modelo de principios y valores, de desarrollo. ¿Están activados los mecanismos de defensa para responder a estas novísimas agresiones sin viso de ser flor casual de un día?

¹⁶ Ibídem, s.p.

Conclusiones: cómo detener a atacantes invisibles

En la era de la *posverdad*, en la que se persigue movilizar y hacer prevalecer las emociones por encima de la realidad y el rigor de los hechos, toda estrategia de seguridad nacional deberá partir del diagnóstico de que las campañas de desinformación forman parte de planes más amplios y ambiciosos de desestabilizar a un oponente, por lo general un actor estatal.

La viralización automática y global de mensajes engañosos a través de perfiles programados o robots está disparando exponencialmente una amenaza ya de primera magnitud. En el origen está el hecho de que los medios de comunicación tradicionales han perdido el monopolio y el control de los flujos de información transnacionales y, a pasos agigantados, se dejan por el camino la notoriedad, la influencia y la publicidad. Hasta tal punto de que un candidato como Donald Trump llegó a ser presidente de la primera potencia mundial no solo viviendo de espaldas a las corrientes de opinión que generaban (contrarias a sus intereses), sino declarándoles «enemigos del pueblo» y calificándoles despectivamente, como hiciera su consejero Steve Bannon, de «principal partido de la oposición».

La preponderancia de la comunicación sobre la propia información se ha convertido en un factor fundamental de riesgo y susceptible de ser explotado para producir inestabilidad. Esencialmente, en la medida en que la acción comunicativa no plantea una búsqueda de la verdad (obligación que sí contempla la actividad informativa).

Carecerá de sentido, por insuficiente, cualquier política de seguridad que no identifique las redes sociales como lugares para poner en contacto a personas con ánimo hostil y dañino que pueden socavar, en un momento determinado, intereses nacionales a través de campañas de manipulación masiva. Más si cabe en un ecosistema posmoderno en el que, más allá de la esencia de los actos, se imponen los distintos tipos de narración sobre los mismos y, por tanto, la diversidad de percepciones producidas.

Cualquier estrategia futura de defensa tendrá que partir del desafío vital de identificar operaciones de engaño. Con la multiplicación de emisores se ha disparado la dificultad para averiguar la exactitud de lo contado y de comprobar la credibilidad de las fuentes. Es la moneda de cambio cotidiana en un mundo en el que los hechos objetivos se remiten a la trastienda, presentándose en el frontispicio de lo comunicable y lo noticiable el universo de las creencias personales y, aún más revolucionario, las simples emociones.

El daño producido por las *fake news* que originen reacciones en cadena de puro desconcierto entre los ciudadanos (a veces millones) será incalculable no solo si no se articulan políticas de seguridad y defensa efecti-

vas y acordes a la idiosincrasia de la amenaza, sino, por añadidura, si no se planifican acciones de alfabetización digital que doten a la sociedad civil de mecanismos de defensa frente a la intoxicación y la mentira. El pensamiento crítico vuelve a ser el patrimonio y el arma más codiciada, y más escasa.

Capítulo tercero

Redes sociales y posverdad en el devenir de los Estados

Eva Moya

Resumen

Occidente ha descubierto todo el potencial de las redes sociales para manipular la opinión pública de sus ciudadanos, al margen de los grandes medios de comunicación. Los casos del Brexit, el presidente Trump y el escándalo de Facebook y Cambridge Analytica demuestran que las redes están siendo utilizadas como un arma política y geoestratégica, llegando a alterar los destinos de los Estados. Este capítulo tiene por objeto analizar la evolución de las amenazas de las redes sociales en diferentes ámbitos, con la intención de prever usos futuros que afecten a la seguridad de los ciudadanos y la defensa de los estados.

Palabras clave

Redes sociales en seguridad y defensa, propaganda y manipulación en redes sociales, las redes sociales y la opinión pública, las redes sociales como arma.

Abstract

Occident has discovered the full potential of social networks to manipulate the public opinion of its citizens, outside the mass media. The cases of Brexit, President Trump and the Facebook and Cambridge Analytica scandal show that the networks are being used as a political and geostrategic weapon, even altering the destinies of States. The purpose of this chapter is to analyse the evolution of social network threats in different spheres, with the intention of considering future uses that affect the security of citizens and the defense of states.

Keywords

Social networks in security and defense, propaganda and manipulation in social networks, social networks and public opinion, social networks as a weapon.

Pero... ¿cómo hemos llegado hasta aquí?

La sinergia es la clave. No se puede entender el éxito y la potencia de las redes sociales sin comprender el contexto en el que han nacido, se han desarrollado e incluso han evolucionado.

Proponer aquí un resumen de este punto de partida sería una osadía por parte de la autora; sin embargo, sí he querido introducir una serie de elementos clave, desarrollados en el mapa conceptual propuesto, que ayudarán al lector a tomar perspectiva de una de las preguntas más frecuentes: ¿cómo es posible que las redes sociales tengan semejante impacto en las sociedades que las manejan?

Para comprenderlo haremos un breve pero importante viaje al pasado para descubrir cómo la mezcla entre el desarrollo de nuevas tecnologías revolucionarias, a la par que un contexto social único basado en ideales democráticos potenciados por un proceso de globalización, han sido los elementos clave de unas nuevas y reconvertidas generaciones que utilizan las redes sociales como un punto de apoyo social, así como una fuente de información sobre la realidad muy relevante. Este viaje se resume en el siguiente esquema conceptual:

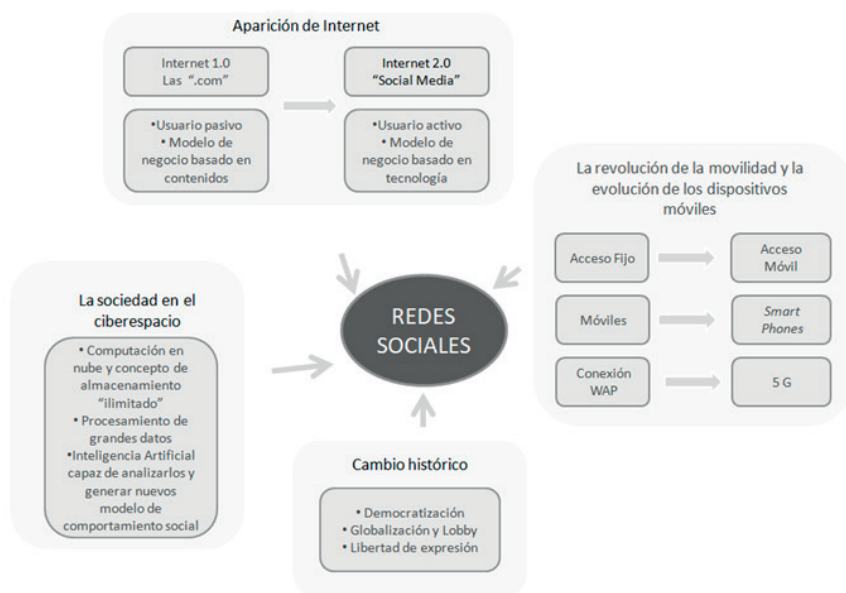


Imagen 1: Mapa conceptual de elaboración propia para comprender el éxito de las redes sociales para campañas de posverdad.

Globalización, democracia y lobby

Es difícil intentar comprender el impacto y la capacidad de viralización de las redes sociales sin mencionar, a la vez, la relevancia del contexto histórico en el que surgen.

El cambio de siglo significó para la humanidad dejar atrás un mundo dividido en bloques con dos sistemas de gobierno muy definidos: capitalismo y comunismo.

Conforme el capitalismo ganaba la batalla y las nuevas organizaciones internacionales nacidas después de la II Guerra Mundial se hacían con ciertas cotas de poder, la globalización inicia su veloz recorrido: comienzan los intensos movimientos de capitales a nivel internacional, basados en una gran cantidad de bienes de todo tipo. Entre ellos, y para la temática que nos ocupa, destacan por encima de todos Internet, los ordenadores y los dispositivos móviles.

Por otro lado, la globalización tiene un efecto positivo en la sociedad gracias a la mejora de los transportes, pues personas de todo el mundo entran en contacto e intercambian su forma de ver la vida, de resolver problemas vitales y, por supuesto, aquellas cuestiones más «de moda» en sus respectivos países, como lo fue el uso de Internet.

Sí es cierto que, actualmente, los propios ciudadanos se hacen conscientes de que la globalización también tiene sombras a las que hay que hacer frente, como el hecho de los Gobiernos supranacionales que, en ocasiones, parecen olvidarse de la gente de a pie, una expresión que llevamos observando desde hace unos pocos años en redes como Twitter y que impulsa a la sociedad hacia un debate más profundo sobre cómo debe organizarse bajo el actual contexto histórico.

Así, el concepto de *aldea global* acuñado por Marshall McLuhan en 1962¹ cobra un nuevo sentido, pues los contactos entre las diferentes sociedades que pueblan el planeta ya no son solo materiales, sino que afectan al modo de vida y, por supuesto, a la comunicación a través de los medios tradicionales como la televisión, la radio y los periódicos, y ahora también a través de la comunicación en de las redes sociales.

Por otro lado, como ya estamos avanzando, las plataformas digitales de las redes sociales, desde su configuración, educan por igual a todos los ciudadanos, sean del país que sean y tengan la cultura que tengan. Les ofrecen la posibilidad de mostrar toda su humanidad expresando cualquier pensamiento, deseo y emoción, sin filtro racional de ningún tipo más allá del que cada ciudadano desarrolla por sí mismo. Incluso, aunque en ciertos países como

¹ McLuhan, Marshall, *The Gutenberg Galaxy: The Making of Typographic Man*, Canadá: University of Toronto Press, 1962.

China o Turquía las redes sociales apliquen censura a algunos contenidos de tipo político, en general no hay censura de ningún tipo.

En este sentido, la democracia es clave para el desarrollo de las redes sociales como una herramienta de movilización social e incluso de propaganda, entre otras cuestiones porque nació de la mano de una de las mayores democracias del mundo. Su modo de ver las cosas se impuso de nuevo en este tipo de desarrollos tecnológicos y con ella dos de sus valores más relevantes: la igualdad y la libertad de expresión.

En las redes sociales da igual que seas político, deportista, famoso o un ciudadano cualquiera. Da igual que tengas pocos recursos o seas multimillonario. En las redes sociales se escucha a todos por igual y todos, por igual, pueden decir lo que quieran. Aunque si bien es cierto, mientras se escriben estas líneas el debate del si «todo vale» en las redes está abierto y comienza a dar ciertos frutos, como por ejemplo el bloqueo de aquellos perfiles que hagan apología del terrorismo, algo que le debemos al Dáesh, que fue quien nos impulsó a dicha reflexión. Sin lugar a dudas, aun nos queda mucho debate por delante y la historia dirá si veremos finalmente a las redes sociales, uno de los máximos referentes de la libertad de expresión, terminar totalmente desnaturalizadas y volviendo a sus inicios más propios de las relaciones humanas y el ocio que con cualquier otra temática.

Tal es el poder que han alcanzado estas plataformas que ya desde 2014 se asocian con otros gigantes como Google y Amazon para impulsar campañas de *lobby* que favorezcan regulaciones alineadas con sus intereses. De hecho, a finales del 2015 saltó la noticia de que Facebook había invertido 2,69 millones de dólares en actividades de *lobby* solo durante el segundo trimestre de ese mismo año².

Del usuario pasivo al «ciudadano interactivo»

Desde que revolucionaron Internet las redes sociales no han dejado de sorprendernos, tanto en la aparición de nuevos canales que innovan donde ya se pensaba que era imposible, como por ejemplo las redes sociales centradas en un formato concreto por ejemplo el vídeo o la imagen (como es el caso de la conocida YouTube o Instagram), así como por temáticas, como Catmoji, una red social de gatos originaria de Japón. Pero también nos han sorprendido con el uso que le damos los ciudadanos a las mismas: desde los ideales más elevados, como la ayuda a personas desesperadas, hasta los comportamientos sociales más oscuros como la pornografía infantil.

² LAPOWSKY, Issie. «What tech giants are spending millions lobbying for» [en línea], en *Wired*. 23 julio 2015. Disponible en web: <https://www.wired.com/2015/07/google-facebook-amazon-lobbying/>.

Aunque los primeros colonos fueron la gente joven «para hablar de sus cosas», el mundo de los negocios pronto vio una gran oportunidad como plataforma de publicidad y captación de clientes, especialmente para el *e-commerce*. Por su puesto, las *celebrities* también comprendieron muy rápido que desde las redes sociales podían conectar rápidamente con su público. Y ya, por último, cuando era evidente que se habían convertido en un fenómeno social, se subieron al carro de las redes las organizaciones internacionales, los políticos y diferentes áreas de Estado de diferentes países.

El usuario actual se relaciona con la comunidad virtual de igual a igual. Puede optar por una posición interactiva, donde el juego de acción-reacción es el lenguaje usado: intercambio de mensajes interrelacionados entre sí como en una cadena. El usuario interactivo reacciona a la vez que crea su propio contenido. En este tipo de relación prima la participación sobre la calidad de las publicaciones, que en numerosas ocasiones nada aportan y no son más que respuestas impulsivas a, también en demasiadas ocasiones, mensajes generados por bots.

Por otro lado, tenemos al usuario proactivo, que es el creador y controlador de principio a fin de todo el contenido que genera. No solo es desarrollador, sino también estratega en cómo y cuándo lanzar su contenido y mensaje para su mayor difusión y beneficio. Aquí la calidad es fundamental, por encima de la cantidad, ya que el prestigio del creador depende de ello.

La inmediatez que proporciona Internet hace que estos usuarios puedan también ejercer de auténticos transmisores de actualidad, reporteros del aquí y ahora a través de las redes, que no conocen de filtros ni de sesgos ideológicos.

Estos son los efectos del éxito del *social media* en convertir a un usuario pasivo, propio de los comienzos de Internet, en un usuario proactivo, el de hoy día.

Para comprender mejor la argumentación de este capítulo hagamos retrospectiva y detengámonos un momento para explicar la clave del cambio social que impulsó la transformación de la llamada web 1.0 a la web 2.0, hoy término obsoleto y que ha dado paso a un concepto que resume mejor la realidad de esta tecnología: *social media* o medios sociales.

La aparición de Internet es tratada por algunos autores e investigadores como una verdadera revolución en la forma de vivir de los ciudadanos de finales del siglo xx y principios del siglo xxi, algunos incluso la comparan con el descubrimiento del fuego o de la penicilina³.

³ GREGORIO, Paco, «Internet es como el fuego o la penicilina» [en línea], en *Diario de Sevilla*. 9 agosto 2017. Disponible en web: http://www.diariodesevilla.es/entrevistas/Internet-fuego-penicilina_0_1161783910.html.

En los comienzos, la 1.0 basaba todo su modelo de negocio en la generación de contenidos. Era una época en la que para comunicar y tener presencia en Internet era imprescindible reunir un equipo de personas especializadas en programación, diseño y generación de contenidos multimedia.

En esta época, la mayoría de los internautas visitaban varias «.com» que procuraban suministrar los mejores contenidos posibles para conseguir visitas continuadas a sus espacios web. Este modelo se acercaba más al viejo modelo de las antiguas revistas de ocio, divulgación y entretenimiento. Sin lugar a dudas, una de las más conocidas y que representó todo lo bueno y lo malo de esa época fue el conocido portal de noticias Yahoo⁴, que entre otras de las líneas de negocio que desarrolló terminó por convertirse en uno de los pocos buscadores que ha podido rivalizar con Google.

Esta Internet era una Internet unidireccional, donde los usuarios solo navegaban sin interactuar más allá de pulsar algún botón, especialmente en el caso de los juegos. Si bien es cierto que los foros servían como plataformas de interacción social, las cuales se convertían en las primeras comunidades virtuales en torno a un *hobby*, a un interés común o a un debate, lo cierto es que el diálogo entre el lector y el portal se hacía básicamente a través del email y de tú a tú. Poco tenía que ver realmente con la red «multicomunicación» en la que vivimos y operamos hoy día con conversaciones a dos, tres e infinitas bandas a través de múltiples canales a la vez.

Por otro lado, los usuarios se veían obligados a dedicar tiempo a localizar aquellos portales que parecían más interesantes porque, aunque se disponía de Altavista, un motor de búsqueda basado en la creación de repositorios de enlaces, la realidad es que se hacían necesarias publicaciones en papel al estilo de una guía donde se publicaban listados basados en la temática de contenidos de aquellos que resultaban más interesantes: motor, deportes, decoración, belleza, noticias, foros, etc.

Tras explotar la burbuja de las «.com», muere el negocio centrado en la generación de contenidos, que se transforma en el término que Tim O'Reilly hizo tan popular: la web 2.0⁵.

Detengámonos un momento en lo que significa e inspiran estas nuevas tecnologías. En la conferencia de 2005 junto a sus compañeros, O'Reilly Media apuntó qué condiciones deben cumplir las tecnologías 2.0, basadas en la

⁴ GREENBERG, Julia. «Once upon a time, Yahoo was the most important Internet company» [en línea], en *Wired*, 23 noviembre 2015. Disponible en web: <https://www.wired.com/2015/11/once-upon-a-time-yahoo-was-the-most-important-internet-company/>.

⁵ O'REILLY, Tim; PAHLKA, Jennifer. «The "Web Squared" Era» [en línea], en *Forbes*, 24 septiembre 2009. Disponible en web: <https://www.forbes.com/2009/09/23/web-squared-oreilly-technology-breakthroughs-web2point0.html#60d4ee695b53>.

idea de que «Tú controlas tu propios datos»⁶. Es la clave del meme que resume la tormenta de ideas de O'Reilly Media. Algunas de ellas serán vitales para el desarrollo y uso de las redes sociales:

- a) La comunidad como plataforma: Sin duda esta es una de las más relevantes. La comunidad de internautas y/o desarrolladores se convierte en el eje central de todos los nuevos desarrollos.
- b) Creación de una red de innovación y desarrolladores libres: Muy inspirado en la filosofía Open Source, es uno de los principios que da paso al desarrollo de la inteligencia colectiva⁷, por la cual la Red y sus usuarios funcionan como un único ente, colaborando individuos independientes entre sí para la aportación del conocimiento e información que conforma la red. Se trata de una de las disciplinas más relevantes de hoy día para todo tipo de áreas, no solo la tecnológica.
- c) Creación de negocios basados en *software* que permita difundir contenido: Este principio cambia completamente el enfoque anterior. Ahora el control del contenido ya no está en manos de unos pocos, la clave es el desarrollo de plataformas que permitan a cualquiera compartir con el mundo para crear esa comunidad.
- d) *Software* por encima de un solo aparato: principio que da origen al desarrollo de la nube o *cloud computing*. Esto impulsa, además, que el desarrollo del *software* sea mucho más sencillo y con orientación universal, que cualquiera pueda usarlo, sin las limitaciones propias de no saber programar.
- e) Aceptación del estado beta como una constante: Aunque parezca algo más relacionado con el desarrollo de la tecnología, la realidad es que dicho estado permite a las plataformas mejorar y adaptarse a los cambios que la comunidad va solicitando, como por ejemplo, el relacionado con el aumento de seguridad y privacidad. El conseguir que estos desarrollos diseñen arquitecturas que puedan ir modificándose con el paso del tiempo es absolutamente imprescindible y todo un reto. Además, estas modificaciones deben ir asociadas a una curva de aprendizaje relativamente sencilla para el usuario base de Internet.

Retomando el discurso, tiempo antes de la aparición de las redes sociales, Bill Gates se había propuesto que hubiera un ordenador personal en todas las casas (1975)⁸. A la par, la conexión a Internet se globalizaba a gran

⁶ O'REILLY, Tim, «Design Patterns and Business Models for the Next Generation of Software» [en línea], en *O'Reilly*, 30 septiembre de 2005. Disponible en web: <http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1#mememap>.

⁷ TAPSCOTT, Don; WILLIAMS, Anthony D. *Wikinomics: How mass collaboration changes everything*, Nueva York: Portfolio, 2016.

⁸ BEAUMONT, Claudine, «Bill Gates's dream: a computer in every home» [en línea], en *The Telegraph*. 27 junio 2008. Disponible en web: <https://www.telegraph.co.uk/technology/3357701/Bill-Gatess-dream-A-computer-in-every-home.html>.

velocidad⁹, de manera que ordenadores e Internet se convertían así en un tándem ideal para la rápida propagación de las nuevas tendencias en comunicación digital. Por otro lado, para quien no pudiera disponer de alguno de ellos, había a disposición de los ciudadanos los famosos negocios llamados cibercafés, donde mientras el cliente tomaba un café podía utilizar los ordenadores y la conexión a Internet que el propio negocio ponía a disposición de los clientes.

Como venimos comentando, la nueva etapa que decía adiós al modelo de negocio basado en la generación de contenidos y anuncios publicitarios se transformaba en una totalmente nueva, centrada principalmente en el desarrollo de nuevas aplicaciones que pudieran aprovechar dos de los grandes beneficios de Internet: conexión a cualquier hora y con cualquier parte del mundo.

Estas nuevas aplicaciones, cuyos principios básicos estaban inspirados bajo la idea de que cualquier ciudadano tuviera la posibilidad de generar sus propios contenidos, interactuar con otros ciudadanos y crear comunidades de conocimiento, conectan rápidamente con la necesidad de comunicación y expresión de la sociedad, generando algunas aplicaciones tan relevantes, y que aún utilizamos hoy día, como son la sindicación de contenidos, los blog, las wikis, la folcsonomía, y, por supuesto, las redes sociales.

Una cuestión de máxima relevancia para el tema que nos ocupa en este capítulo es el hecho de que en los desarrollos web 2.0 no se contempla la figura del editor, moderador o intermediario entre los contenidos y la publicación de los mismos, pues si recordamos los principios básicos, la idea es crear aplicaciones sin barreras de ningún tipo para los ciudadanos y la comunidad. Esa figura, que sí estaba muy presente en los tiempos del Internet 1.0, ya que seleccionaba los contenidos digitales en función de los criterios de calidad y expectativas de la audiencia, queda relegada ahora a la figura de los *content curator*¹⁰.

Los *content curator* son perfiles profesionales, requeridos solo por las grandes compañías y organizaciones, las nuevas revistas digitales y blogs de tendencia. Así pues, ¿qué pasa con el resto de millones de *posts*¹¹ que se publican cada semana? ¿Y de los millones y millones de mensajes, imágenes y vídeos que se vuelcan cada día en las redes sociales? ¿Quién está detrás de esos contenidos? La respuesta es sencilla: cualquiera de nosotros, porque nosotros somos «comunidad».

⁹ «Internet Growth Statistics» [en línea], en *Internet World Stats*. Disponible en web: <https://www.internetworldstats.com/emarketing.htm>.

¹⁰ Los *content curator* son perfiles profesionales preparados para buscar información y elaborar un discurso profesional, donde la validación de fuentes es la clave y la seriedad en la selección del lenguaje marca el estilo de cada contenido.

¹¹ «World posts written today» [en línea], en *Worldometers*. Disponible en web: <http://www.worldometers.info/blogs/>.

Con la aparición de los blogs apareció una forma ágil y cómoda de dar salida a la necesidad humana de hablar para el mundo, en parte por la arquitectura del desarrollo de estas plataformas, en forma de diario organizado por fechas, en parte porque crear una web seguía siendo solo para iniciados, ciudadanos de todo el mundo comenzaron a usarlos para expresar cualquier cosa, literalmente.

Nacían así los tan queridos diarios personales digitales. En ellos había desahogos, poesías, frustraciones, alegrías, ideas políticas, religiosas y todo tipo de curiosidades. Los blogs capturan audiencia y, a la vez, la derivan hacia otros con los que están enlazados en red. Los lectores pueden participar en un *post*¹² a través de los comentarios, unas veces buenos y otras totalmente fuera de lugar.

Gracias a la libertad para comentar cualquier cosa que se leía, se fragua una nueva generación de usuarios en la Red que descubría lo que significaba «no tener pelos en la lengua». Hablaran de lo que hablaran, nada podía pasar más allá de recibir un insulto. Por supuesto, el *blogger*¹³ podía borrar todo lo que considerara no apropiado en su blog.

En esta época inicial, conseguir muchos seguidores o lectores no era la mayor preocupación; tampoco lo era la calidad del contenido, entre otras cosas porque la mayoría de los usuarios no sabía de diseño gráfico, ni tampoco de investigación, redacción o desarrollo de contenidos digitales. Por otro lado, quedaba todavía lejos el interés por elaborar un discurso serio y cuidado, ya que, además, nadie pagaba por ello. Simplemente se daba salida a la expresión de uno mismo, sin preocupaciones más graves que el hecho de que apareciera algún *trol*¹⁴ en el blog.

La velocidad a la que se expandieron los blogs demostró de forma categórica el deseo de las personas por comunicarse y darse a conocer con voz propia, sin intermediarios, como podrían ser los medios de comunicación, la clase política o las instituciones públicas, considerados los antiguos portavoces de la sociedad.

En sus inicios, la red social de blogs estaba formada por gente «de la calle», y como tal el contenido de sus *post* se basaba en su día a día y su problemática: se intercambiaban consejos y construían conocimiento de forma colectiva. Cabe comentar que los inicios no estaban carentes de cierta ingenuidad, como la de un niño que da sus primeros pasos, pues el

¹² Nombre técnico para designar un artículo de un blog.

¹³ Nombre técnico para designar al propietario de un blog. En parte tiene su origen en la plataforma de generación de blogs de Google llamada Blogger.

¹⁴ Los *trols* son usuarios especializados en destruir la reputación de una comunidad virtual y/o de las personas y organizaciones. Sus motivaciones son muy variadas, desde la económica, con una visión mercenaria dispuestos a ser contratados por una compañía rival, hasta aquellos individuos que simplemente se divierten generando caos.

que escribía, escribía sus verdades, sus anhelos y compartía su conocimiento real. De hecho, este tipo de libertad de expresión estaba entre los principios de la comunidad de internautas¹⁵. Esta forma de utilizar la gran Red no pasó desapercibida entre los lectores, los cuales iban otorgando cada vez una mayor credibilidad a lo que decían otros ciudadanos frente a la que le conferían a los «medios oficiales o tradicionales». Al fin y al cabo... ¿quién entiende mejor al ciudadano de a pie que otro ciudadano de a pie?

Se crea así una sensación de libertad total de expresión en la comunicación digital, paradójicamente recuperando comportamientos sociales propios de los albores de la humanidad, donde el boca a boca permitía a las sociedades desarrollarse e introducir nuevas formas de hacer. Por otro lado, esta libertad de expresión permitía esconder la autoría detrás de un avatar¹⁶ que permitía ocultar la identidad real del usuario.

Poco tiempo después de la expansión de los blogs aparecen las redes sociales tal y como las entendemos hoy día. Una de las primeras fue Sixdegrees, cuya filosofía estaba basada en la idea de que todos estamos conectados en solo seis saltos¹⁷. Le siguieron My Space u Orkut, pero sin duda, si hubo una plataforma que revolucionó la nueva forma de comunicar fue la plataforma Facebook (el nombre la define como «libro de caras», es decir, de personas y, en definitiva, de perfiles). Con una visión totalmente internacional y de carácter global, Facebook nació de las manos de un equipo de trabajo liderado por Mark Zuckerberg. Se suponía que era un proyecto para conectar a estudiantes¹⁸ y que se pudieran mantener en contacto a pesar de la distancia o de estar en otro campus, pero el éxito basado en la curiosidad innata del ser humano por saber cómo le va al otro la convirtió en una de las herramientas más poderosas del mundo¹⁹.

¹⁵ GREER, James Gregory; DEOKAR, Amit V. «The Antecedents of Community Commitment in Online Community of Practice», en *Proceedings of the Nineteenth Americas Conference on Information Systems*. Chicago, Illinois. 15-17 agosto 2013.

¹⁶ El *avatar* es una imagen que representaba a un perfil en la red, se acompañaba de un *nick*, que era el nombre alternativo por el cual el internauta deseaba ser conocido. En la actualidad, gran parte de los que participan en Internet utilizan de avatar su propia foto y de *nick* su propio nombre.

¹⁷ Sixdegrees, <http://www.sixdegrees.com/>.

¹⁸ BEAHM, George (Editor). *The Boy Billionaire: Mark Zuckerberg in his own words*. Chicago: Agate B2 Publisher, 2012.

¹⁹ PEAK, Kenneth J. (Editor), «Encyclopedia of Community Policing and Problem Solving», en *SAGE Publications*, USA, 2013. STATISTA, «Most famous social network sites worldwide as January 2018, ranked by number of active users (in millions)» [en línea]. Statista, 2018. Disponible en web: <https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/>.

Las redes sociales son similares a los blogs, puesto que la arquitectura de la aplicación obliga a seguir una línea temporal que se llama *timeline*²⁰, es decir, cada contenido va asociado de forma inseparable a la fecha en la que se ha compartido. Sin embargo, su gran ventaja es que este tipo de plataforma es mucho más veloz, en tanto en cuanto no obligan a desarrollar un gran discurso. Sin embargo, sería raro que alguien creara un *post* en su blog con solo una línea de contenido.

Para educar a los usuarios en este nuevo tipo de comunicación, las propias aplicaciones sugieren tipos de contenido que se pueden compartir. Así, por ejemplo, un usuario puede resumir su estado anímico en las áreas organizadas para ello, que invitan a hacerlo con frases del tipo «Cuéntale al mundo cómo te sientes», «¿En qué estás pensando?», etc. Por otro lado, los perfiles de las plataformas contienen una serie de campos que suelen requerir de cierta actualización como el estado sentimental, dónde se trabaja, qué tipos de intereses se tienen actualmente, etc.

Por tanto, si en los blogs los usuarios deben elaborar cierto discurso, en las redes sociales ya no hace falta. Con manifestar ciertas emociones como «hoy estoy triste», «deseando que llegue el fin de semana», «hasta las narices de mi jefe» o «¡Mañana me caso!» se despertaba el interés de los que estaban conectados al perfil, de manera que los seguidores interactúan rápidamente para comentar su estado y/o compartir otros momentos, algo que, además, se vio potenciado cuando las redes sociales incorporaron las etiquetas²¹.

Con la introducción de este tipo de aplicaciones, y conforme los usuarios aprendían a utilizarlas, se produce una explosión de creatividad en la comunicación digital, enriquecida por la aparición de nuevos formatos de comprensión²² como las imágenes y los vídeos, que hacían más fácil compartir este tipo de recursos.

Toca detenerse un momento en la evolución de la comunicación digital. Una vez más, gracias a los principios del 2.0, aparecen también herramientas

²⁰ El *timeline*, conocido en la jerga del *social media* como «tl», es el muro donde se van publicando todos los mensajes de las redes sociales. Los creadores lo llamaron así porque en esencia es una línea de tiempo que muestra la trayectoria de cada perfil.

²¹ Las etiquetas en las redes sociales tienen su origen en la creación de la *folcsonomía*. Con ellas se puede mencionar a otros perfiles directamente permitiendo así compartir cualquier tipo de contenido. Se pusieron especialmente de moda gracias a Facebook, ya que permite subir fotografías grupales y etiquetar directamente a todos los que salen en la foto. Hoy día, las etiquetas también se utilizan para conseguir la atención de otros perfiles para un tema concreto. Por ejemplo, cuando se lanza un evento se puede etiquetar en la imagen de la convocatoria a múltiples perfiles a los que se quiere invitar. Esta técnica es muy utilizada en las movilizaciones sociales.

²² Los formatos de comprensión de imagen como el .jpg o .png, los de vídeo como el .mp4 o el divx y su versión open, el xvid y los de audio como el .mp3 permitieron desarrollar contenidos que no eran exigentes a la hora de ser compartidos en Internet, pues no ocupaban demasiado espacio y además, no tardaban en «subirse a la Red».

que permiten ser mucho más creativos, como es el caso de aquellas que facilitan la creación de infografías o la edición de pequeños vídeos, algo clave, por ejemplo, para las campañas de propaganda en las redes sociales. Nuevos conceptos, como los memes²³, demuestran que un discurso puede ser sintetizado en forma de una única imagen. Por otro lado, el éxito de las redes sociales basadas en contenidos en forma de imagen y vídeo como Instagram o YouTube demuestra una vez más la tendencia al cambio en los hábitos lectores de la población, como agudamente se describe en el libro titulado *¿Cómo leemos en la sociedad digital?*, presentado en 2017²⁴:

«Considerando la Red un espacio privilegiado de subjetivación [...] exploramos [...] cómo esas formas de textualidad [...] despliegan nuevos y estrechos vínculos con lo audiovisual, la sociabilidad distribuida de los medios sociales, la interactividad, la convergencia, la velocidad y la hiperabundancia. Este sistema emergente de relaciones hipertextuales hace presagiar efectos que están aún por comprenderse en su verdadera dimensión».

Un problema relevante que agrava la facilidad con la que se puede intoxicar a la opinión pública, ya que este tipo de contenidos se consume todavía más rápido que el texto e incitan a una interacción casi inmediata. De ahí su alta capacidad para generar una gran viralización²⁵, ya sea real o no el contenido que se está viralizando.

La pequeña revolución de la movilidad y la evolución de los dispositivos móviles

Paralelamente, tiene lugar otro fenómeno no menos revolucionario y que será de vital importancia para los nuevos usos que se les dan a las redes sociales.

A finales del siglo xx aparecen los primeros *smartphones* entre los que destacó el sistema Palm OS, que fue copiado por muchas compañías de telefonía móvil de la época. Estos dispositivos todavía no estaban conectados a la Red, pero ya permitían cierta libertad a sus usuarios como relacionar sus agendas o dibujar en la pantalla. Se introducía el concepto de que un teléfono podía servir para mucho más que para llamar y se educaba al usuario en el uso de otras funcionalidades para sus terminales más relacionadas con el movimiento de los dedos que con la voz.

²³ Imagen o texto, a menudo de contenido humorístico, que se comparte viralmente en las redes sociales durante un periodo breve.

²⁴ CRUCES, Francisco (Director). *¿Cómo leemos en la sociedad digital?* Lectores, booktubers y prosumidores, España: Fundación Telefónica y Editorial Ariel, 2017.

²⁵ El término viral se utiliza en las redes sociales para hacer referencia a aquellos contenidos que son consumidos por una gran cantidad de usuarios en un corto periodo de tiempo. El concepto está inspirado en el comportamiento de los virus.

A partir de 2001, con el nacimiento del 3G en Japón²⁶, Internet salta de las pantallas del ordenador a las pantallas de los dispositivos móviles. Se inicia un nuevo camino que culmina con la aparición de una nueva generación de *smartphones*. En esta fase, uno de los casos de éxito más relevantes fue la creación del sistema operativo para móvil llamado Android en 2008 por parte de la compañía Google²⁷. Inspirado en la filosofía Open Source y las comunidades libres de desarrolladores, facilitó a los grandes fabricantes cambiar las reglas del mercado de los teléfonos móviles convirtiéndolos definitivamente en pequeños ordenadores de bolsillo.

Como era de esperar, las aplicaciones 2.0 comenzaron a realizar nuevos desarrollos que permitieran su uso en estos terminales. Incluso nacen algunas totalmente nuevas, exclusivas para estos terminales, como las de mensajería instantánea como WhatsApp, Telegram o SnapChat. Por su parte, las principales redes sociales tampoco desaprovecharon la oportunidad de continuar su expansión invirtiendo en sus desarrollos para móvil. Incluso aparecen redes sociales exclusivas para estos dispositivos, como fue el caso de Instagram (nombre basado en *instante*), orientada a dar salida a la necesidad de muchos «ciudadanos interactivos» de capturar un momento y compartirlo con el mundo mientras sucede, y potenciando la vertiente informativa de todos estos usuarios que actúan más como periodistas de actualidad que como meros generadores de contenido.

Ahora, la oportunidad de compartir cualquier cosa pasada, presente o futura en las redes sociales adquirirá una nueva dimensión, puesto que el teléfono móvil está siempre a mano, en algunos casos, incluso llegando a convertirse en una adicción²⁸.

Este uso intensivo de los *smartphones* impulsa también el deseo de disponer de mayor velocidad y capacidad en la conexión de datos para los dispositivos móviles, lo que se traduce en la carrera hacia la conexión 5G.

Computación en nube, big data e inteligencia artificial

La primera aproximación al concepto de *nube* como una red de computadoras global que ofrece todo tipo de servicios, surge en los años sesenta. Sin embargo, es con compañías como Sales Force y Amazon entorno al año 2000 con las que se inicia la utilización de los servicios en nube de forma intensiva por parte de grandes compañías. Año tras año, la computación en nube o

²⁶ «First 3G mobiles launched in Japan», BBC News, 1 de Octubre de 2001, <http://news.bbc.co.uk/2/hi/business/1572372.stm>.

²⁷ RAO, M.N., «Fundamentals of open source of software», PHI Learning Pvt. Ltd., Delhi, 2014.

²⁸ YANG, Zheng, *Encyclopedia of Mobile Phone Behavior*. USA: IGI Global, 2015.

cloud computing se abre camino para convertirse en la mejor solución para todo tipo de organizaciones, sean del sector que sean.

Sin la nube, las redes sociales no tendrían sentido, pues su necesidad de almacenamiento de información, así como de procesamiento de los millones de datos que reciben al día, exige este tipo de servicio. Prueba de ello es el hecho de que ya en 2016 el top 20 de organizaciones que consumían los servicios en nube eran plataformas de *social media*²⁹, y entre ellas casi todas las principales redes sociales.

Top 20 Most Popular Consumer Apps in the Enterprise

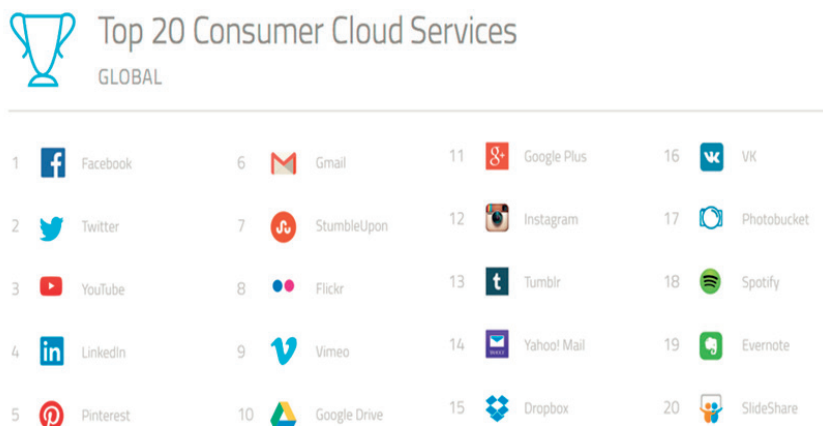


Imagen 2: Infografía de Sky Hih Networks sobre el uso del cloud computing.

La ingente capacidad que tienen los usuarios de Internet para crear contenido y contar sus historias ha impulsado una disciplina que sigue siendo realmente relevante: el *big data*. Esta disciplina trata el dato desde tres dimensiones principales (volumen, velocidad, variedad) y dos dimensiones que depuran el contenido para que realmente sea útil (veracidad y valor), que son las que permiten obtener un resultado que facilite la toma de decisión.

En relación a las redes sociales, el *big data* es el actor principal que facilita conocer qué interesa en un país, cuál es la opinión pública sobre un tema, quiénes son las personas de influencia, cuáles son las nuevas tendencias, etc. Si bien es cierto que uno de los grandes problemas que este tipo de

²⁹ Cook, Brandon. «The most popular cloud services rankings 2016» [en línea], en *Sky-highnetworks*. Disponible en web: <https://www.skyhighnetworks.com/cloud-security-blog/the-20-totally-most-popular-cloud-services-in-todays-enterprise/>.

plataformas han demostrado es la inocencia en relación a la dimensión *veracidad*, puesto que, hasta hace poco, se daba por sentado que lo que decía un perfil, era real. Igualmente, la potencia del análisis del *big data* puede exponer vulnerabilidades sociales para ser manipuladas por potencias extranjeras para sus propias intenciones.

La inteligencia artificial ha irrumpido en nuestras vidas a través de la robótica y es una de las disciplinas que más va a crecer en los próximos años. En las redes sociales la IA interviene en numerosos procesos, principalmente a través del uso de los bots. Lamentablemente, también hay usos no tan buenos de los mismos. A día de hoy, existen numerosos tipos de bots categorizados en función de su utilidad. Algunos de los «buenos» son, por ejemplo, *socialbots* o *chatsbots*, especializados en interactuar con los clientes; y algunos de los «malos» serían, por ejemplo, los *hacker bots* o *spam bots*, encargados de difundir publicidad masiva y virus informáticos.

Pero los bots «malos» pueden tener un alcance mucho mayor del que la comunidad se imaginaba en un principio. La facilidad con la que se pueden abrir perfiles falsos, facilita la creación de redes de bots integrados en las principales redes sociales para influir sobre diferentes poblaciones. De hecho, este es uno de los riesgos de la IA sobre la que alerta el Cambridge Risk Center en su informe *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*³⁰, donde se describe el futuro riesgo político de la IA como el riesgo derivado del «uso de tareas automáticas para monitorización masiva ciudadana, para operaciones de persuasión y operaciones de decepción. [...] Se esperan también ataques nutridos de la capacidad de analizar la personalidad, el humor y las creencias de las personas». En este sentido, las redes sociales se convierten tanto en una fuente de información que puede ser evaluada por la IA como en el vector de ataque a través del cual se difunda cualquier campaña de manipulación y propaganda, basada en comunicaciones muy centradas en el uso de las técnicas propias de la *posverdad*.

Como resultado de todos estos elementos de los que hemos estado hablando, nos encontramos con un ciudadano deseoso de participar en la sociedad y en la democracia, dispuesto a convertirse en ideólogo, político, historiador y por supuesto, también periodista.

La unión de todos estos pilares facilita la aparición de un nuevo concepto relacionado con la generación de contenidos: el *periodismo ciudadano*³¹, que si

³⁰ VV.AA., «The malicious use of Artificial Intelligence: Forecasting, Prevention and Mitigation», Centre for the study of Existential Risk, University of Cambridge, 21 de Febrero de 2018, <https://www.cser.ac.uk/resources/malicious-use-artificial-intelligence/>.

³¹ ESPIRITUSANTO, Óscar; GONZALO RODRÍGUEZ, Paula, «Periodismo ciudadano. Evolución positiva de la comunicación» [en línea], en *Revista Comunicar, Editorial Ariel y Fundación Te-*

bien nace en los inicios de la 2.0, gracias a la movilidad y las nuevas aplicaciones móviles ha adquirido una proyección global, pues permite a cualquier ciudadano registrar, con su cámara de móvil y sus redes sociales, lo que está pasando en cualquier parte del mundo, mucho antes, incluso que los medios denominados «tradicionales».

Política, relaciones internacionales y economía a golpe de tuit

Propaganda política y posverdad «transparente»

El éxito demostrado en el aumento de la visibilidad derivada de la presencia en las redes sociales ha generado la aparición de nuevos actores vinculados con la política en los últimos años. En los inicios de las redes sociales no hubiéramos pensado que podrían haber llegado a revolucionar su uso, pues nadie podía imaginar que se podría llegar a gobernar a golpe de tuit.

Seducidos ante la posibilidad de llegar a más gente con unos costes relativamente bajos, han decidido apostar por dedicar tiempo y recursos a estas plataformas. Así, con la aparición de estos nuevos actores políticos en las redes, se introducen nuevas motivaciones en la tipología de su uso que no se habían explorado hasta entonces de forma masiva: la defensa de los ideales políticos.

a) Viejos estilos de propaganda en nuevas plataformas

Un caso de estudio muy interesante sobre propaganda a la vieja usanza, pero en las nuevas plataformas digitales, es el protagonizado por el Gobierno israelí, uno de los primeros en dar el salto a utilizar las redes sociales para sus propios intereses, llegando a crear una «patrulla virtual de ciberguerreros»³².

En 2013, Israel consideró la creación de varias cuentas de Twitter como canales de propaganda directa, inundando esta red las veinticuatro horas del día con mensajes de todo tipo y en todos los idiomas. Los ciberguerreros de Israel dominaban perfectamente el lenguaje de Twitter, siendo capaces de optimizar la limitación de espacio, además de ser capaces de contaminar los *hashtags* de sus geografías clave con sus mensajes. De esta forma, si alguien quería consultar algo al respecto lo primero que encontraría en su búsqueda serían sus argumentos.

Estos son algunos ejemplos de aquella época:

lefónica. 2011. Disponible en web: <https://www.revistacomunicar.com/pdf/2011-12-15-libro-periodismo-ciudadano.pdf>.

³² GREENWOOD, Phoebe. «Israel invests millions in drive for elite “cyber warriors”» [en línea], en *The Telegraph*. 1 noviembre 2012. Disponible en web: <https://www.telegraph.co.uk/news/worldnews/middleeast/israel/9648820/Israel-invests-millions-in-drive-for-elite-cyber-warriors.html>.



FDI
@FDIonline

iNo te dejes engañar! La prioridad de **#Hamás** es el terror; ayudar a los civiles de **#Gaza** queda en segundo lugar goo.gl/ySiqZ

8:00 PM - 30 May 2013



IDF ✓
@IDFSpokesperson



New **#Hamás** Legislation: Gender Segregation for **#Gaza's** Schools ow.ly/jIg8e

9:00 PM - 3 Apr 2013

Imagen 3: Fuente, captura propia. Perfiles de los ciberguerreros de Israel en Twitter.

Si bien, cabe destacar para el capítulo que nos ocupa que en este estadio las acciones políticas se realizan de forma transparente y directa, por tanto los actores estaban identificados y los mensajes son claros. En definitiva, se conoce perfectamente su origen.

El grupo de ciberguerreros de Israel manejaba perfectamente una de las claves del éxito de este tipo de comunicación: la gestión de las emociones de los usuarios de las redes sociales. Este tipo de comunicación debe ser clara y directa y provocar al instante algún tipo de reacción como compartir el mensaje, realizar algún tipo de protesta o llevar a cabo lo que se pide.

Para conseguirlo, lo primero es identificar el tipo de perfil sociodemográfico al que nos vamos a dirigir, en definitiva, seleccionar los *targets*. La campaña tendrá un objetivo, pero para conseguirlo tal vez sea necesario dirigirse a diferentes tipos de usuarios.

Una vez realizado el perfil social de los receptores de los mensajes se elabora un discurso que facilite la integración inmediata del mensaje o mensajes de la campaña que se está llevando a cabo.

Por ejemplo, en el caso de los dos tuits de 2013 de los ciberguerreros de Israel, el primero se dirige a todas aquellas personas que consideran que los israelíes son invasores y asesinos, mientras que el segundo va dirigido a mujeres que luchan por los derechos y libertades de la mujer. Aunque los perfiles y la comunicación se dirigen a varios *target*, el objetivo es el mismo: convencer de que Hamás es el verdadero enemigo y el «malo».

b) Llamando a la movilización social

Sin duda, uno de los papeles más relevantes de las redes sociales en el ámbito político y social es su capacidad para difundir rápidamente un mensaje que permita movilizar a los ciudadanos. Por supuesto, las redes sociales también participan en el estadio inicial, el de alimentar la tensión social.

Dentro de esta categoría, si hubo un evento mundial que situó a las redes sociales en el punto de mira respecto a su poder de intervenir en la política y Gobierno de un Estado, fueron las revoluciones que se iniciaron en 2011, llamadas por aquel entonces Primaveras por el prestigioso periódico francés *Le Monde* en su artículo *Un printemps en hiver*³³.

Si bien la intención de este capítulo no es analizar el hecho histórico, del que hay abundante literatura, sí merece especial mención el uso que los ciudadanos de los distintos países árabes le dieron a las redes sociales, especialmente Twitter, para organizarse y movilizarse frente a sus respectivos Gobiernos.

En estos casos nos encontramos de nuevo con una construcción de mensajes dirigida a provocar una emoción como, por ejemplo, la ira contra los dirigentes de un país. Para analizar este tipo de uso de las redes se propone un ejemplo de un mensaje de Twitter realizado por un perfil cualquiera, opositor al expresidente de Egipto, Hosni Mubarak, en 2011, durante el periodo de tensión social.



Imagen 4: Fuente, captura propia. Perfil de un opositor al expresidente egipcio.

Este perfil no es famoso ni es de los más *influencer*³⁴; sin embargo, participa en la creación y difusión de la campaña contra el expresidente. Esta es una de las claves de este tipo de campañas. No solo es necesario que alguien con

³³ BEN JELLOUN, Tahar. «Un printemps en hiver» [en línea], en *Le Monde*. 22 enero 2011. Disponible en web: http://www.lemonde.fr/idees/article/2011/01/22/un-printemps-en-hiver_1469161_3232.html.

³⁴ Los *influencers* son perfiles en las redes sociales con gran alcance y capacidad de llegada al resto de la Red y, por tanto, capaces de movilizar a miles o cientos de miles de personas en aspectos muy diversos, desde crear tendencias en moda, nuevos comportamientos sociales o cómo llevar hacia la movilización política.

influencia y alcance movilice a los ciudadanos, sino que estas campañas solo tendrán éxito si, una vez lanzada la convocatoria, son los propios ciudadanos los que de forma espontánea desean participar en la difusión de la misma, a su manera.

En este aspecto, cobra sentido más que nunca lo planteado en las primeras páginas de este capítulo en relación al 2.0 como una forma de participación directa e involucración ciudadana en cada momento o situación de la sociedad. Y junto a ella, todo el poder de la comunidad a través de la inteligencia colectiva, que permite el desarrollo de nuevas ideas creativas que calen con el mensaje; algo que un grupo de opositores, por sí solos, nunca podría lograr, pues no tendrían tiempo ni recursos como para diseñar los cientos o miles de mensajes diferentes que se lanzan en este tipo de situaciones.

Por otro lado, este ejemplo nos sirve para ilustrar una cuestión que puede pasar desapercibida en el momento en el que tiene lugar la movilización y que, sin embargo, es de vital importancia para adelantar el éxito que tendrá o no y su alcance.

Llama la atención que el mensaje no está en el idioma local, sino en inglés. La intención es muy clara: conseguir involucrar a la comunidad internacional y a medios de comunicación extranjeros que permitan dar una proyección global al conflicto que pueda estar teniendo lugar.

Por tanto, este tipo de mensajes no habla para dentro de las fronteras, sino que está totalmente dirigido para captar la atención de otros países. En este sentido, además, utilizar los códigos culturales a los que la movilización desea dirigirse se hace imprescindible para que sea comprendido por el receptor del mensaje. En el caso de este tuit, se hace referencia a un código muy anglosajón, relacionado con sociedades que viven el capitalismo en su máxima expresión: la compra y venta de cualquier activo. La crudeza del mensaje incita rápidamente a la ira, pues a través de una inferencia rápida el lector pensará que los ciudadanos de un país están a la venta al mejor postor por culpa de su presidente. No contento con esta idea, que ya de por sí es hiriente y podría haber sido un tuit por sí mismo, continúa en pocas palabras con el hecho de que su presidente jamás ha gobernado, por lo que está a estrenar. Y aunque pudiéramos pensar que, debido a ello, la venta significaría la entrada de dinero para el país, remata con la idea de que gobernar Egipto es imposible y, por tanto, el valor de la misma sería bajísimo.

Mensajes de este tipo, en otros idiomas y durante una movilización social, permiten conocer parte de la estrategia de la misma, pues cuando ya se busca involucrar a agentes extranjeros se está buscando ayuda de forma global.

En este tipo de campañas, los convocantes están especialmente interesados en involucrar a otros medios de comunicación extranjeros con la intención de evitar la censura o el alineamiento ideológico de los medios de comunica-

ción nacionales y que puedan bloquear, en un momento dado, que la campaña realmente cale entre los ciudadanos.

En el caso de las revoluciones árabes, resultó ser la clave para centrar la atención de la comunidad internacional sobre lo que estaba teniendo lugar en Oriente Medio por aquel entonces. De hecho, muchos informes de los servicios de inteligencia de todas partes del mundo utilizaron la información que se suministraba a través de varias redes sociales como Facebook y Twitter para conocer la evolución de las movilizaciones y comprender las motivaciones y las tácticas que se estaban llevando a cabo, una información vital para tomar ciertas decisiones al respecto.

Por supuesto, esta transparencia de las movilizaciones en las redes significaba también una fuente fácil y barata para los grandes medios de comunicación, que aprovechaban cualquier *trending topic* en Twitter o mensajes virales para abrir sus noticiarios o alimentar sus *breaking news*, independientemente de que tuvieran o no periodistas desplazados.

Otra de las razones del éxito de las redes sociales en las movilizaciones es la inmediatez suministrada por el uso de las mismas en los dispositivos móviles. Esto permite convocar rápidamente a los ciudadanos y mantenerlos informados mientras la movilización tiene lugar. De nuevo, la inteligencia colectiva se pone al servicio de la propia sociedad que la genera para dirigirla, incluso aunque existan algunos perfiles con liderazgo temporal.

Conviene recordar el significado de Twitter: piar. El hecho de que sea un pájaro no es solo una licencia creativa, sino que responde al concepto del «pio, pio» de un pajarillo y su comportamiento grupal.

Con su arquitectura tecnológica, Twitter representa a una gran bandada de pájaros que no para de piar. Bandada que en un momento determinado se puede dividir en varias bandadas más pequeñas (los *hashtags* de la red) que son seguidas por los diferentes grupos de pájaros. Van tan rápido que, en un momento dado, pueden volver a juntarse, y dividirse de otra forma y volver a juntarse, y volver a separarse, etc. Hay que comprender que en el comportamiento de estas bandadas, los líderes pueden ir cambiando y ser temporales, y este dinamismo es lo que dota de una sensación de «realidad» a los que forman parte de la bandada, pues no lideran solo políticos, sino también gente «de la calle».

c) Twitter y la comunicación entre Gobiernos

Un interesante ejemplo del uso de Twitter como canal de comunicación gubernamental fue protagonizado en 2013 por el Gobierno egipcio de los Hermanos Musulmanes, uno de los primeros casos que se registran en las redes sociales de un Gobierno que se dirige a otro a través de una red social.

El Gobierno de los Hermanos Musulmanes utilizó una de sus cuentas oficiales de Twitter para acusar públicamente al Departamento de Estado de los

EE.UU. por lo que ellos consideraban una falta de respeto a la religión musulmana. El suceso había tenido lugar unas horas antes, en el que la que fue portavoz del Departamento de Estado, Victoria Nuland, realizó una serie de comentarios en un programa americano humorístico sobre el interrogatorio del Gobierno Egipcio a Bassem Youssef, un humorista que, supuestamente, había insultado al presidente Mursi³⁵.

Lo más llamativo no es el hecho del mensaje en sí, sino ver cómo los Hermanos Musulmanes de Egipto utilizaban perfectamente, por aquel entonces, los códigos de Twitter para dirigirse al Gobierno americano, llegando a mencionarle directamente a través de la «@» e incluyendo un *hashtag* bastante popular como era el «#FJP» (*Freedom and Justice Party*) para darle un carácter internacional a sus acusaciones.



#FJP: We strongly condemn @StateDept statements, which means USG is welcoming & condoning defamation of religion by some in Egyptian media

6:04 PM - 2 Apr 2013

Imagen 5: Fuente: Captura propia. Perfil de Ikhwanweb en Twitter.

Por otro lado, de nuevo, al hacerlo en el idioma del receptor del mensaje, los Hermanos Musulmanes activaban la estrategia de la condena pública ante lo sucedido según su visión de las cosas. De esta manera, las relaciones internacionales se transforman y proyectan a un nuevo escenario que puede tomar por sorpresa a los jefes de cualquier gabinete de comunicación, asesores políticos, etc.

Cabe destacar que el hecho de que los Hermanos Musulmanes estuvieran viendo el programa de televisión americano, también demuestra cómo los medios de comunicación más tradicionales, como la televisión, han entrado en el juego de las relaciones internacionales, pues unos comentarios pensados y dirigidos exclusivamente para el público americano son interpretados como una amenaza para uno de los protagonistas, del que no se esperaba que estuviera atento a los mismos.

³⁵ EFE, «La embajada de EE. UU. en Egipto polemiza en Twitter con el Gobierno de Mursi» [en línea], en *El País*. 4 abril 2013. Disponible en web: https://elpais.com/economia/2013/04/04/agencias/1365031886_990101.html.

La situación sobrepasó al Gobierno americano, que no estaba preparado para reaccionar, así que fue la misma embajadora de EE.UU. en Egipto la que tomó la decisión espontánea sobre cómo resolver la crisis. Pensó que borrar el perfil de la embajada en Twitter posiblemente prevendría una oleada de ataques contra el perfil y la posibilidad de que aumentara la tensión contra la embajada, incluso con movilizaciones de carácter presencial. Lo que ella no consideraba es que un acto como este podría haber sido interpretado también como un enfriamiento mayor de las tensas relaciones y causar un mal mucho mayor. Hoy en día, sin duda, se hubiese interpretado así. Finalmente, bajo petición del Gobierno americano, la cuenta se restauró sin más incidentes.

A pesar de lo extraño que pueda parecer este tipo de uso de las redes sociales en las relaciones internacionales hoy en día, seguimos encontrándonos con esta forma de medir fuerzas entre Estados. Sin duda, el presidente de EE.UU., Donald Trump, es un gran conocedor de los ritmos y comunicación al respecto, sorprendiéndonos todos los días con su particular forma de ver las cosas y convencer al pueblo americano.

Lo primero que hay que destacar es que el señor Trump no habla a través de la cuenta oficial del presidente en Twitter, @potus. No, Donald Trump prefiere utilizar su propia cuenta, @realdonaldtrump, para capitalizar el impacto de todos sus mensajes sobre su persona con la intención de aumentar su influencia, incluso cuando deje de ser presidente. También es una forma de intentar diluir ciertos mensajes impactantes que pueden ser analizados como «su punto de vista», pero no la «del presidente de los EE.UU.», que posteriormente escuchará a sus asesores y tomará la decisión más adecuada.

Tal es la relevancia de su cuenta a nivel mundial que un empleado de Twitter, «supuestamente por accidente» (pero que muy probablemente estuviera vengándose), borró este perfil en su último día de trabajo³⁶. Sin duda, borrar la cuenta de Donald Trump representa un acto clarísimo de activismo político.

El señor Trump sorprende todos los días con su manejo populista de las redes sociales, a través de los cuales es capaz de construir un mensaje para hablar tanto a los americanos que le han votado como al resto del mundo.

Uno de los mensajes más impactantes, que más sorprendió al mundo entero y que podría haber tenido consecuencias nefastas en este sentido tuvo que ver con la gestión de la crisis de Corea del Norte en uno de sus momentos más tensos. A raíz de unos comentarios amenazantes de Kim Jong-un sobre el avance del poder del armamento nuclear de su país, el señor Trump tuvo a bien responder lo siguiente:

³⁶ REDACCIÓN, «El empleado de Twitter que en su último día de trabajo desactivó la cuenta de Donald Trump» [en línea], en *BBC*. 3 noviembre 2017. Disponible en web: <http://www.bbc.com/mundo/noticias-41854972>.



Imagen 6: Fuente: Captura propia. Perfil de Donald Trump en Twitter.

De nuevo vemos una manifestación más de la comunicación basada en el intento de generar emociones. Es fácil imaginar que los votantes del señor Trump, al ver esta reacción, habrán sentido cierto júbilo al sentir que, sin duda, América es más poderosa que nadie. Esta comunicación es muy contundente, directa y «de la calle», algo que acerca al presidente a gran parte de sus ciudadanos, que pueden llegar a pensar de forma ilusoria que el señor Trump es «como ellos», que es un patriota y que les está defendiendo.

Por otro lado, el mensaje es tan sencillo, típico de estas comunicaciones, que es muy fácil de comprender por cualquier ciudadano sea cual sea su estrato social. Y, de hecho, esta es una de las grandes habilidades del presidente: reducir aspectos complejos a frases tan sencillas que las podría entender un niño, aunque estén plagadas de falsos supuestos o desprecien todos los matices que hacen que la situación sea mucho más compleja y tenga más impacto del que pueda aparentar en un principio.

Debemos ver en esta nueva tipología de uso, por parte de los dirigentes de cualquier país, un riesgo para las relaciones internacionales que bien pudieran derivar en crisis y conflictos muy complejos de resolver.

Hay que comprender que cuando se emite un mensaje de estas características a través de una red social no se emite bajo criterios de comunicación de «gabinete» como debería, sino que la espontaneidad y el carácter emocional de este tipo de mensajes claramente dirigidos a causar impacto y revuelo pueden tener consecuencias insospechadas en el receptor del mismo, quien puede emprender acciones no contempladas en el momento inicial del envío del mensaje. Además, dependerá también de la reacción del resto de la Red, pues en el momento en el que se hacen públicos estos mensajes, aparecen otros actores que pueden quebrar la estrategia inicial e incluso volverla contra nosotros.

d) Los perfiles de las redes sociales como un activo de un país

En este sentido otro gran personaje con presencia relevante en la gestión de la comunicación política en las redes sociales, especialmente en Facebook, fue la presidenta de Argentina Cristina Fernández de Kirchner, una gran fan del *social media*.

Buena conocedora de este tipo de medios, mantenía durante su presidencia sus cuentas de Twitter y Facebook muy activas, utilizándolas para ofrecer su punto de vista sobre todo lo que sucedía en Argentina.

Por ejemplo, en 2013 tuvo que asumir varias críticas por su gestión en las recientes inundaciones. Aprovechando que una de esas críticas se la habían hecho llegar a través de su cuenta en Facebook, decidió contestar públicamente sabiendo que tendría un impacto mayor sobre la población que contestando a través de un comunicado gubernamental.

Frases del tipo «Quiero contarte que llegamos a las familias del Arroyo Maldonado gracias a tu mensaje del sábado», «El responsable del grupo es Horacito [...], hijo de detenidos desaparecidos. Nunca conoció ni conocerá a sus padres» demostraban que la señora Fernández de Kirchner es una gran conocedora de la comunicación emocional y cercana propia de este tipo de plataformas. La respuesta tuvo una gran acogida porque la acompañó de varias fotografías que demostraban que sí había respondido inmediatamente con hechos, no solo palabras. En definitiva, convirtió una situación que podía haber dañado su reputación en una de la que salió todavía más reforzada.



Imagen 7: Fuente: Captura propia. Perfil de Cristina Fernández de Kirchner en Facebook.

Con su hiperactividad en las redes sociales, la señora de Kirchner, tras perder la presidencia en 2015, protagonizó un hecho que hasta entonces no había tenido lugar en las redes sociales y que abrió un debate en toda la comunidad, que se tuvo que plantear la pregunta: ¿De quién es el perfil en las redes sociales de un país?

Hasta ese momento, la cuenta oficial del Gobierno de Argentina en Twitter era @CasaRosadaAR. Sin embargo, tras perder la presidencia, la señora de Kirchner se apropió de la misma para convertirla en un tributo a los años de su presidencia³⁷.



Imagen 8: Fuente: Captura propia. Perfil de la Casa Rosada en Twitter.

El hecho histórico en las redes sociales lo convirtió en viral y dio la vuelta al mundo. De hecho, los nuevos inquilinos de la Casa Rosada se vieron forzados a abrir una nueva cuenta oficial en esta red social para representar al nuevo Gobierno del país³⁸.

Un deseo tan fuerte por parte de un político de no perder el control de las redes sociales demuestra que son conscientes de cómo esta herramienta puede controlar la opinión pública y convertirla en una herramienta afín a sus propios intereses políticos y personales. Este deseo plantea reflexiones profundas sobre la propiedad de las mismas y sobre quién debería tener el control gubernamental de unos perfiles que representan a todos los ciudadanos de un país. Sin duda, un manual de buenas prácticas se hace imprescindible para evitar casos como el de la señora Fernández de Kirchner.

³⁷ REDACCIÓN, «Diarios extranjeros ironizan con el cierre de la cuenta de Twitter de Casa Rosada» [en línea], en *Clarín*. 9 diciembre 2015. Disponible en web: http://www.clarin.com/mundo/Diarios-extranjeros-Twitter-Casa-Rosada_0_1482452054.html.

³⁸ REDACCIÓN, «El Gobierno abrió una nueva cuenta de Casa Rosada en Twitter» [en línea], en *La Nación*. 22 diciembre 2015. Disponible en web: <http://www.lanacion.com.ar/1856430-el-gobierno-abrio-una-nueva-cuenta-de-casa-rosada-en-twitter>.

Propaganda política y posverdad «enmascarada»

Cabe destacar que, en los mensajes propios de la *posverdad*, uno de los factores emocionales que más activan a la ciudadanía es el relacionado con su seguridad.

En las redes sociales, nada funciona mejor que todos aquellos mensajes que apelan al hecho de que las decisiones de políticos, Gobiernos, empresarios o agentes en el poder y/o con poder abusan de su posición para sus propios intereses y no protegen a sus ciudadanos o consumidores.

Si bien es cierto que tradicionalmente el miedo más profundo de todo ser humano es la muerte, en las últimas décadas, y muy relacionado con las grandes crisis, también se asocia la supervivencia a la supervivencia económica.

A raíz de la crisis del 2008 la brecha social entre ricos y pobres cada vez es mayor. Las clases medias se han visto mermadas, mientras las familias con mayor poder adquisitivo no solo se han reafirmado en sus fortunas, sino que las han aumentado dando la bienvenida, incluso, a nuevos miembros, tal y como demuestra el Informe Anual de la Riqueza en el Mundo 2015³⁹, realizado por las consultoras Capgemini y RBC Wealth Management.

Con la transformación digital, la robótica⁴⁰ y la globalización varios sectores de la población han visto cómo sus trabajos de toda la vida han ido desapareciendo o se han visto tan afectados que los jornales no dan para vivir como antes.

Estos sectores, sin embargo, perciben que la clase política solo busca enriquecerse al servicio del gran capital y, por tanto, no les representan.

Tanto o más importante como la transformación económica son los cambios sociales que se han producido en los últimos años, como consecuencia de diversos factores, para explicar la crisis política de las democracias occidentales.

La cada vez menor confianza en los organismos políticos y representativos⁴¹ se ve apuntalada no solo por los modos de encarar los cambios económicos, sino también por las crisis de refugiados que se vienen sucediendo desde 2015⁴²

³⁹ NARAYAN, Krishnan. «La población de individuos con elevado patrimonio y sus niveles de riqueza alcanzan nuevos máximos» [en línea], en *Capgemini*. 17 junio 2015. Disponible en web: <https://www.capgemini.com/es-es/news/la-poblacion-de-individuos-con-elevado-patrimonio-y-sus-niveles-de-riqueza-alcanzan-nuevos/>.

⁴⁰ COSTANTINI, Luca. «El mayor fabricante de móviles sustituye a 60.000 trabajadores por robots» [en línea], en *El País*. 27 mayo 2016. Disponible en web: https://elpais.com/economia/2016/05/27/actualidad/1464342646_679598.html.

⁴¹ EDELMAN. «2017 Edelman Trust Barometer» [en línea]. S.f. Disponible en web: <https://www.edelman.com/trust2017/>.

⁴² EUROPEAN COMMISSION. «The UE and the migration crisis» [en línea]. Julio 2017. Disponible en web: <http://publications.europa.eu/webpub/com/factsheets/migration-crisis/en/>.

y los numerosos ataques terroristas islamistas en suelo europeo⁴³, unido todo ello al sentimiento del electorado de inacción por parte de instituciones y partidos políticos.

Si bien durante décadas se habían considerado manifestaciones secundarias, todas estas circunstancias han sido el caldo de cultivo para el renacimiento de movimientos radicales y populistas en el ámbito social y político europeo, y actualmente su auge es innegable; pero han resurgido en forma de movilizaciones en la red o la creación de partidos políticos como un nuevo modo de atraer e involucrar a ciudadanos, en creciente desafección⁴⁴, en un uso inteligente de las redes sociales para amplificar su mensaje sin necesidad de una estructura tradicional compleja⁴⁵. Ahora se trata del activismo del presente: el activismo *online*.

De esta manera, se supera la concepción histórica que había caracterizado a estos movimientos en épocas pasadas de contestación a los poderes fácticos y contra el *establishment* político⁴⁶.

La política europea actual refleja esta tendencia: los partidos radicales tanto de extrema izquierda como de derecha se han hecho fuertes en Parlamentos como el sueco⁴⁷, austríaco⁴⁸ o danés⁴⁹, llegando a alcanzar el Gobierno Syriza en Grecia y Akel en Chipre⁵⁰, y también logrando representación en el Parlamento Europeo⁵¹.

⁴³ EUROPOL. «2017 EU Terrorism Report» [en línea] 15 junio 2017. Disponible en web: <https://www.europol.europa.eu/newsroom/news/2017-eu-terrorism-report-142-failed-foiled-and-completed-attacks-1002-arrests-and-142-victims-died>.

⁴⁴ FUNKE, Manuel; SCHULARICK, Moritz; TREBESCH, Christoph. «Politics in the Slump: Polarization and Extremism after Financial Crises, 1870-2014» [en línea], en *European Commission*. 23 septiembre 2015. Disponible en web: http://ec.europa.eu/economy_finance/events/2015/20151001_post_crisis_slump/documents/c._trebesch.pdf.

⁴⁵ MARTÍNEZ, Anna-Clara. «Las nuevas formas de participación política: del Internet a las Instituciones» [en línea], en *Debate* 21.1 julio 2015. Disponible en web: <http://debate21.es/2015/07/01/las-nuevas-formas-de-participacion-politica-de-internet-a-las-instituciones/>.

⁴⁶ VVAA. «Populism, Political Radicalism and Political Extremism: Normalisation and Contestation in Changing Democracies» [en línea], en *European Consortium for Political Research*, General Conference, University of Oslo. 6/7 septiembre 2017. Disponible en web: <http://extremism-and-democracy.com/wp-content/uploads/2017/09/ECPR-Oslo-S049-Final-Programme.pdf>.

⁴⁷ SVERIGES, Riksdag. «The Sweden Democrats [en línea]. S.l., s.f. Disponible en web: <http://www.riksdagen.se/en/members-and-parties/>

⁴⁸ NATIONALRAT. «Results of Austrian Parliamentary Election 2017: Freedom Party of Austria» [en línea]. S.l., s.f. Disponible en web: <http://www.austria.org/the-latest/2017/10/30/austrian-parliamentary-election-2017>.

⁴⁹ FOLKETINGET. «Members in each Party Group: The Danish People's Party» [en línea]. S.l., s.f. Disponible en web: http://www.thedanishparliament.dk/Members/Members_in_party_groups.aspx.

⁵⁰ KATSOURIDES, Yiannos. *Radical Left Parties in Government: The Cases of Syriza and Akel*. UK: Palgrave-Macmillan. 2016.

⁵¹ EUROPEAN PARLIAMENT, «MEPs Seats» [en línea]. S.f. Disponible en web: <http://www.europarl.europa.eu/meps/en/hemicycle.html>.

Son vistos como la alternativa natural a los partidos tradicionales, en evidencia tras su fracaso en la gestión de los nuevos desafíos sociales y económicos, y han sabido explotar muy bien, una vez más con la ayuda imponderable de las redes sociales, el temor a una inmigración sin control desde los países de Oriente Medio y su vinculación con la violencia⁵², los unos, y la política económica de corte conservador y neoliberal⁵³, los otros. Todo ello espoleado por unas instituciones europeas que son vistas como poco o nada resolutivas, paralizadas frente a las crisis surgidas y en plenos debates nacionales por la pérdida de soberanía ante una autoridad supranacional, junto a la falta de comunicación y conexión efectiva de las autoridades comunitarias con la ciudadanía⁵⁴.

En esencia, las mismas razones de base pueden explicar el triunfo de las posiciones más radicales y populistas en los Estados Unidos: crisis económica, situación de la inmigración y desconfianza en las instituciones⁵⁵. Desde la crisis, la población se ha visto bombardeada desde un sector de la clase política con continuos mensajes de ultranacionalismo, proteccionismo económico y chivo expiatorio en los inmigrantes⁵⁶, que han sido muy bien acogidos por una parte importante del electorado⁵⁷. El mejor reflejo es el discurso político del señor Trump, que aglutina estos postulados y que, como se ha visto anteriormente, no duda en compartir, cuando tiene a bien, a través de todas las opciones que la Red pone a su alcance y sin filtro alguno, para alborozo de sus votantes y estupefacción de sus detractores⁵⁸.

⁵² GUIBERNAU, Montserrat. «Migration and the rise of the radical right» [en línea], en *Barrow Cadbury Trust Policy Network*, UK 2010. Disponible en web: <http://www.policy-network.net/uploadedFiles/Publications/Migration%20and%20the%20rise%20of%20the%20far%20right.pdf>.

⁵³ MARCH, Luke. «The European radical left and the international economic crisis» [en línea], en *OpenDemocracy*. 5 febrero 2013. Disponible en web: <https://www.opendemocracy.net/luke-march/european-radical-left-and-international-economic-crisis-opportunity-wasted>.

⁵⁴ MONTI, Mario. «Salvar Europa» [en línea], en *El País*. 3 febrero 2016. Disponible en web: https://elpais.com/elpais/2016/02/03/opinion/1454497691_517516.html

⁵⁵ PEW RESEARCH CENTER. «Trust in government» [en línea]. 23 noviembre 2015. Disponible en web: <http://www.people-press.org/2015/11/23/1-trust-in-government-1958-2015/>.

⁵⁶ MASON & HOLLAND. «Trump's U.N. speech shows nationalism instincts firmly intact» [en línea], en *U.S. News*. 19 septiembre 2017. Disponible en web: <https://www.usnews.com/news/top-news/articles/2017-09-19/trumps-un-speech-shows-nationalist-instincts-firmly-intact>.

⁵⁷ REDACCIÓN. «Presidential Election Results: Donald J. Trump wins» [en línea], en *The New York Times*. 9 agosto 2017. Disponible en web: <https://www.nytimes.com/elections/results/president>.

⁵⁸ ROBINSON, Eugene. «This is getting worse» [en línea], en *The Washington Post*. 30 noviembre 2017. Disponible en web: https://www.washingtonpost.com/opinions/this-is-getting-worse/2017/11/30/65c255fc-d616-11e7-b62d-d9345ced896d_story.html?utm_term=.8145b1c31075.

Bajo este contexto resulta sencillo alimentar cualquier tensión basada en engaños y mentiras, ante las cuales el sentido común se sorprende al ser consciente de que hay ciudadanos que son capaces de creérselas. Para conseguirlo, por ejemplo, se exagera la realidad. En este tipo de campañas, se selecciona algún dato real y se amplifica y exagera de tal forma que se convierte en un mensaje completamente sesgado, pero que capta la atención y la emoción de los ciudadanos rápidamente.

En un contexto de este tipo, es fácil detectar cuáles son los puntos débiles de una sociedad para atacarla y manipularla desde la base.

En este sentido, se han registrado dos hechos que pasarán a la historia por su relevancia y por cómo se alcanzaron los objetivos de quienes estaban detrás.

Europa, como constructo conceptual muy joven, todavía tiene mucho camino que recorrer en cuanto a lo que quiere para sí misma y para sus ciudadanos. En este sentido, el ritmo de integración es muy diferente y parece mostrar cierto desconocimiento por parte de algunos ciudadanos, de lo que significa Europa o lo que Europa puede hacer por ellos. Prueba de ello, es el último Informe sobre la Ciudadanía de la UE de 2017⁵⁹, donde la Comisión pone el acento en la necesidad de «Promover y aumentar la participación ciudadana en la vida democrática de la UE», puesto que observa poca intención de voto para elecciones europeas por parte de algunas sociedades. De este porcentaje bajo en la intención de voto se puede concluir que ciertos ciudadanos consideran a los organismos de Gobierno de la UE entidades alejadas que les gobiernan e impactan sobre sus vidas, pero sobre los que los ciudadanos no tienen ninguna influencia.

Evidentemente, una percepción de este tipo genera un gran descontento que puede ser alimentado rápidamente con mensajes propagandísticos de todo tipo.

Un ejemplo claro ha sido el del Brexit. No es objetivo de este capítulo abordar las causas y consecuencias de este hecho histórico que obliga a Europa a replantearse su evolución, pero sí resulta relevante destacar cómo se ha podido manipular a cierta parte de la sociedad inglesa para que votara salir de la misma.

Si bien es cierto que «la culpa» no es de las redes sociales, estas han colaborado a aumentar la tensión y el descontento entre quienes ya lo estaban. Y este tipo de tácticas pueden ser directas o indirectas.

Por ejemplo, una de las proclamas para el Brexit es el control de personas que circulan libremente por Europa. Apelando a la seguridad física, una de las justificaciones para dicho control, además de la tradicional de «nos roban el trabajo», es el aumento del terrorismo de radicales yihadistas en for-

⁵⁹ PARLAMENTO EUROPEO, «Informe sobre la ciudadanía de la UE: Fortaleciendo los derechos de los ciudadanos en una Unión de cambio democrático (2017/2069(INI))» [en línea]. 30 noviembre 2017. Disponible en web: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A8-2017-0385+0+DOC+XML+V0//ES>.

ma del grupo terrorista Dáesh. La inferencia que se pretende es clara: todos los musulmanes son terroristas.

En esta línea, tras los atentados de Londres de 2017, uno de los mensajes en Twitter que más impactó fue el de una cuenta llamada @SouthLoneStar, que en apariencia parecía americana en tanto en cuanto hablaba un inglés americano, el avatar era un americano vestido al estilo de los cowboys y además se hacía llamar «Texas Lone Star».

El mensaje contenía todos los elementos propios de la *posverdad*: una «medio verdad» exagerada para provocar una emoción relacionada con la ira contra la comunidad musulmana.



Imagen 9: Fuente, The Guardian. Mensaje que se hizo viral tras los atentados de Londres.

Debido al impacto que tuvo su foto, la mujer fue entrevistada y reconoció estar aterrorizada y en *shock* en ese momento. Por otro lado, varios testigos afirmaron que antes de la toma de la foto la habían visto ayudando a las víctimas. Sin embargo, sus palabras no tuvieron tanta fuerza como este tuit, incluso a pesar de describir la realidad.

La misma cuenta de Texas Lone Star continuó alimentando la tensión con otros mensajes como «Espero que después de que UK vote el Brexit comience a limpiar su país de la invasión musulmana!»⁶⁰.

La sorpresa acaeció varios meses después de que investigadores de la Universidad de Edimburgo analizaran cientos de perfiles involucrados en mensajes a favor del Brexit. Los investigadores concluyeron que este perfil, que parecía y se comportaba como un estadounidense del sur, apuntaba a un control desde Rusia, y que pertenecía a lo que hoy se denomina *granja de trolls*⁶¹ o *fábrica de trolls*. Si fuera así, significaría que Rusia ha incluido en sus campañas de propaganda y decepción el uso intensivo de las redes sociales para manipular, intervenir o alterar la opinión de los ciudadanos de aquellos países o áreas geográficas que considera que impactan sobre su estrategia geopolítica.

En este sentido, investigadores de EE.UU. y Reino Unido encontraron 45 mil mensajes prorrupción con Europa realizados desde cuentas falsas rusas durante las 48 horas antes de la votación del referéndum para el Brexit⁶².

Otra gran sorpresa mundial en esta línea fueron las investigaciones de la Comisión Federal de Comercio de EE.UU. sobre el uso de cincuenta millones de datos personales de Facebook por parte de la consultora Cambridge Analytics⁶³, alineada con el entorno del señor Trump. Estos datos, que facilitaban un perfilado exhaustivo de los usuarios de Facebook, fueron utilizados para influir desde EE.UU. en el Brexit a través de la compra de anuncios en la propia Red. Algo por lo que el mismísimo creador, Mark Zuckerberg, tuvo

⁶⁰ VV.AA., «Russia used hundreds of fake accounts to tweet about Brexit, data shows», The Guardian, 14 de Noviembre de 2017 <https://www.theguardian.com/world/2017/nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets>.

⁶¹ Las *granjas de trolls* son una extensión del concepto de *granjas de servidores*, lugares que reúnen gran cantidad de servidores al servicio de las compañías, como por ejemplo las granjas de servidores de Amazon. El concepto alude a la posibilidad de que determinados Gobiernos estén desarrollando cientos de miles de perfiles falsos en las redes sociales para manipular la opinión pública.

⁶² LOMAS, Natasha, «Study: Russian Twitter bots sent 45k Brexit tweets close to vote» [en línea], en *TechCrunch*. 15 noviembre 2017. Disponible en web: <https://techcrunch.com/2017/11/15/study-russian-twitter-bots-sent-45k-brexit-tweets-close-to-vote/>.

⁶³ MCKINNON, John D. «FTC Probing Facebook over data use by Cambridge Analytica» [en línea], en *The Wall Street Journal*. 20 marzo 2018. Disponible en web: <https://www.wsj.com/articles/ftc-probing-facebook-over-data-use-by-cambridge-analytica-1521561803>.

que pedir disculpas a Reino Unido a través de un comunicado publicado en los principales periódicos del país⁶⁴.

¿Hasta qué punto este tipo de mensajes pudieron influir en la votación? A pesar de las sospechas de numerosos investigadores, la respuesta es desconocida. Sin duda, los ciudadanos de hoy en día deciden tener el control sobre la información que reciben, informándose por su cuenta, especialmente a través de lo que cuentan otros ciudadanos, y en este sentido las redes sociales tienen mucho que aportar. Si bien es cierto que este comportamiento está muy estudiado ya en el ámbito comercial, del que emanó el concepto *prosumer*; no está tan claro en el ámbito político e ideológico.

A pesar de todo, otro hecho histórico de estas características, como fue el de las elecciones presidenciales americanas del señor Trump, podría servir para avanzar que, si bien la manipulación de las redes sociales por sí mismas no implican el cambio de opinión de forma inmediata, sí puede resultar ser un factor más que los ciudadanos tienen en cuenta para terminar de convencerse.

El ejemplo de la supuesta injerencia rusa en las elecciones de EE.UU. que ayudaron al presidente Trump a conseguir el poder es un ejemplo de campaña muy bien pensada, diseñada y ejecutada; incluso aunque haya sido descubierta, pues cumplió su cometido: intoxicar a Hilary Clinton como candidata y potenciar al señor Trump.

Hasta el momento lo que sabemos es que la campaña consistió en la creación de cientos de perfiles falsos en las redes sociales, así como en la compra de anuncios en Facebook y Google para potenciar la visita a sitios web que incluían, desde filtraciones, hasta supuestas filtraciones creadas para engañar.

Uno de los ejemplos más interesantes al respecto de la injerencia fue investigado por The New York Times y FireEye⁶⁵ (reputada firma de ciberseguridad americana).

Uno de los mensajes que fueron promovidos en Facebook como un anuncio llevaba directamente a una web llamada DCLeaks. La web alojaba varias filtraciones relacionadas con Wikileaks realizadas por el grupo cibercriminal ruso Fancy Bear⁶⁶.

⁶⁴ AGENCIAS. «Mark Zuckerberg pide perdón por la filtración de datos mediante un anuncio en la prensa británica» [en línea], en *El Mundo*. 25 marzo 2018. Disponible en web: <http://www.elmundo.es/internacional/2018/03/25/5ab77df1468aeba35e8b464d.html>.

⁶⁵ SHANE, Scott. «Rusia creó perfiles falsos de estadounidenses para influenciar en las elecciones» [en línea], en *The New York Times en español*. 19 septiembre 2017. Disponible en web: <https://www.nytimes.com/es/2017/09/19/rusia-facebook-perfiles-falsos-elecciones-eeuu/>.

⁶⁶ REDACCIÓN. «¿Se perdió entre los correos de Podesta? Claves de la gran filtración de WikiLeaks sobre Hillary Clinton» [en línea], en *RT en español*. 13 octubre 2016. Disponible en web: <https://actualidad.rt.com/actualidad/221089-clinton-wikileaks-correos-tanda-claves>.

De nuevo, para que las filtraciones tuvieran el mayor impacto posible entre el *target* seleccionado, era imprescindible poner en conocimiento de los ciudadanos americanos la existencia de la web. Así pues, como si de una marca cualquiera se tratase, los creadores de la misma demostraron un gran conocimiento de las técnicas de marketing digital y compraron espacio en los anuncios de Facebook y Google para promocionar la existencia de la web.

Uno de los anuncios era un tanto sorprendente, pues cierta educación sobre cómo funcionan habría hecho pensar a los usuarios de Facebook que era extraño que un padre cualquiera, supuestamente llamado Melvin Redik, hubiera pagado para dar a conocer la web. Sobran palabras ya para recordar que de nuevo se recurre a los códigos culturales del receptor del mensaje para incitarle a hacer clic.

Investigaciones posteriores de los servicios de inteligencia americanos demostraron que DCLeaks formaba parte de la trama rusa diseñada para influir en las elecciones de EE.UU. a favor del señor Trump⁶⁷.



Melvin Redick ► **BREAKING NEWS - WORLD**

June 8, 2016 · 🌐

These guys show hidden truth about Hillary Clinton, George Soros and other leaders of the US. Visit #DCLeaks website. It's really interesting!
<http://dcleaks.com/>



Imagen 10: Fuente, The New York Times.

En estos dos casos urge recordar la importancia de la validación de la información que se difunde a través de las redes sociales, información

⁶⁷ REDACCIÓN. «Following the links from Russian hackers to the U.S. election» [en línea], en *The New York Times*. 6 enero 2017. Disponible en web: <https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html>.

que, ya sea inconscientemente o con total premeditación, puede ser totalmente falsa.

Las redes sociales y la manipulación de la economía

Quizá al lector le sorprenda esta perspectiva; sin embargo, a lo largo de la historia de las redes sociales han existido varias situaciones, algunas han pasado desapercibidas, que demuestran todo el potencial de las mismas para influir sobre la economía de un país o un área geográfica.

Por ejemplo, ¿hasta qué punto la información de las redes sociales puede alimentar los algoritmos que determinan cómo irá la bolsa o la economía? ¿El resultado del colectivo, ya sea de perfiles reales o de bots, podría dominar la economía?

Johan Bollen, Huina Mao y Xiao-Jun Zeng, de las universidades de Indiana y Manchester, publicaron en 2010⁶⁸ el resultado de su investigación realizada sobre los comentarios recopilados entre febrero y diciembre de 2008 con la intención de demostrar la posibilidad de predecir el comportamiento del índice Dow Jones en función de los comentarios y mensajes publicados en Twitter, con especial atención al comportamiento emocional de felicidad, calma o tristeza.

El resultado de su estudio fue realmente sorprendente: demostraron la correlación entre los mismos, pudiendo predecir el movimiento diario del Dow Jones con una exactitud del 87%, aunque, como ellos mismos expresan en las conclusiones de su trabajo, no pudieron demostrar las causas del cambio de humor en los mensajes de Twitter, que posteriormente llevaban al cambio en el valor de las cotizaciones. Pero sí pudieron demostrar cómo la cotización variaba, como máximo, tres días después del cambio de humor generalizado en Twitter.

El FBI sí que lo tenía muy claro cuando en 2012 activó la Operación Perfect Hedge⁶⁹, centrada en la investigación de la manipulación del valor de varios fondos americanos. La agencia americana, además de su investigación *offline*, tuvo muy en cuenta cómo se habían manipulado los valores a través de los mensajes oficiales en las cuentas de Twitter de estos fondos.

Siguiendo con esta línea, otro caso muy sonado del FBI que también llegó a los tribunales de EE.UU. tuvo que ver con la acusación, en 2015, de varias

⁶⁸ BOLLEN, Johan; MAO, Huina; ZENG, Xiao-Jung. «Twitter mood predicts the stock market» [en línea], en *Journal of Computational Science*. Marzo 2011. Disponible en web: <https://arxiv.org/abs/1010.3003>.

⁶⁹ GOLDSTEIN, Matthew; ABLAN, Jennifer. «FBI uses Twitter social media to look for securities fraud» [en línea], en *Reuters*. 26 noviembre 2012. Disponible en web: <https://www.reuters.com/article/net-us-investment-summit-fbi/fbi-uses-twitter-social-media-to-look-for-securities-fraud-idUSBRE8AP0EX20121126>.

compañías americanas contra un ciudadano escocés de 62 años. El hombre utilizaba Twitter para difundir noticias falsas desde múltiples cuentas con diferentes alias para hacer bajar los precios de los valores de las compañías en la bolsa. Según la sentencia publicada por el Departamento de Justicia americano, el daño causado por este ciudadano y la estructura que desarrolló para conseguir la manipulación, se podía cuantificar en que las compañías demandantes habían perdido más de un millón de dólares por sus prácticas fraudulentas⁷⁰.

Las motivaciones para manipular la bolsa o la economía de un país son muy variadas. Si bien es cierto que hasta este momento se ha planteado la ambición y avaricia como motivación principal para manipular los valores al antojo de los delincuentes y obtener un buen rédito económico, existen otras motivaciones más relacionadas con la ideología o la intención de dañar a países considerados enemigos.

En este sentido, uno de los mayores sustos que sufrió Wall Street fue el 23 de abril de 2013. El delito fue cometido por el grupo ciberterrorista denominado Syrian Electronic Army (SEA), que usó como vector de ataque a una de las agencias de comunicación más respetadas del mundo, The Associated Press.

La Syrian Electronic Army intentó uno de los mayores *hack* de su historia con la intención de provocar el caos en su enemigo natural, EE.UU. Para conseguirlo, entendieron que atacar directamente a los perfiles en redes sociales de la Casa Blanca no generaría gran impacto, pues posiblemente estaban muy bien protegidos y cualquier *defacement*⁷¹ en los mismos sería corregido inmediatamente. Así pues, ante la pregunta de qué otros actores americanos se podían volver contra su propia nación, tomó la decisión de hackear el perfil de Twitter de la reputada agencia de noticias The Associated Press.

El hackeo consistió en publicar un mensaje falso que generaría una crisis inmediata en el país: «Dos explosiones en la Casa Blanca. Obama está herido». Los ciberterroristas sabían que un mensaje como este generaría pánico y desconcierto, pues atacaba directamente a su mayor representante y hacía sentir a los americanos que no estaban seguros.

⁷⁰ THE UNITED STATES DEPARTMENT OF JUSTICE. «Scottish citizen indicted for Twitter-based stock manipulation scheme» [en línea], en *Office of Public Affairs*. 5 noviembre 2015. Disponible en web: <https://www.justice.gov/opa/pr/scottish-citizen-indicted-twitter-based-stock-manipulation-scheme>.

⁷¹ Técnica utilizada por los *hackers* políticos y terroristas por la cual modifican el aspecto de una web, un blog o una red social con sus proclamas con la intención de que todos los visitantes a la misma se expongan a ellas. De esta manera, consiguen que su mensaje llegue directamente a los ciudadanos alineados con los perfiles que han sido hackeados.



Imagen 11: Fuente, The Telegraph.

Como era de esperar, el mensaje creó pánico en Wall Street durante los pocos minutos que se tardó en validar la información.

El índice bursátil descendió en picado 150 puntos, creando un *minicrash* y haciendo perder a la bolsa 139 billones de dólares⁷².

Una vez confirmada que la noticia era falsa y había sido un hackeo de la cuenta, la bolsa recuperó la normalidad. Sin embargo, el gráfico de la caída del Dow Jones cuando saltó la noticia falsa, refleja muy bien los efectos que este tipo de ciberataques, en los que una vez más se construye un mensaje falso pero que puede llegar a ser creíble, pueden provocar en la sociedad.



Imagen 12: Fuente, The Telegraph.

⁷² FOSTER, Peter. «'Bogus' AP tweet about explosion at The White House wipes billions off US markets» [en línea], en *The Telegraph*. 23 abril 2013. Disponible en web: <https://www.telegraph.co.uk/finance/markets/10013768/Bogus-AP-tweet-about-explosion-at-the-White-House-wipes-billions-off-US-markets.html>

El impacto de la *posverdad* en las redes sociales y en las emergencias: seguridad y defensa

Las redes sociales comenzaron en la calle; luego se sumaron las grandes marcas, con la intención de acercarse a los ciudadanos; casi a la par también se incorporaron los políticos, que veían en estas plataformas una manera de expresarse directamente sin la reinterpretación de sus palabras por los medios de comunicación; posteriormente, se sumaron los organismos públicos y el Estado, y finalmente se incorporaron aquellas áreas relacionadas con emergencias, seguridad y defensa. De ellos, quizá las emergencias sean aquellas que han desembarcado con más fuerza, gracias a la poderosa capacidad de comunicación en una situación delicada.

Se proponen algunos ejemplos de los usos de las redes sociales en estas áreas, sobre las que también impacta la *posverdad*.

Catástrofes naturales

Sin duda, pocas situaciones son tan críticas como las emergencias y las emergencias en las catástrofes naturales. En situaciones como estas es necesario responder rápidamente, y para conseguirlo la comunicación es clave.

Una de las mejores versiones de las redes sociales está en relación con el uso de estas como herramienta de socorro. Los ciudadanos pueden conectar con los servicios de emergencias enviando mensajes de socorro junto a una geoposición, y también se pueden mantener informados de la evolución de la emergencia.

En 2010, tras uno de los terremotos más virulentos de Chile, el centro de recursos de Yahoo! decidió investigar el comportamiento de la difusión de los mensajes informativos suministrados por los propios usuarios de la red social Twitter que disponían de información de primera mano sobre el terremoto.

Tras analizar los resultados, se dieron cuenta de que debían dedicar una parte de su investigación al análisis de la difusión de falsos rumores que contaminaban la realidad de lo que estaba sucediendo. Gran parte de las conclusiones fueron extraídas tras la elaboración de esta tabla:

Table 4: Classification results for cases studied of *confirmed truths* and *false rumors*.

Case	# of unique tweets	% of re-tweets	# of unique "affirms"	# of unique "denies"	# of unique "questions"
Confirmed truths					
The international airport of Santiago is closed	301	81	291	0	7
The <i>Viña del Mar International Song Festival</i> is canceled	261	57	256	0	3
Fire in the Chemistry Faculty at the University of Concepción	42	49	38	0	4
Navy acknowledges mistake informing about tsunami warning	135	30	124	4	6
Small aircraft with six people crashes near Concepción	129	82	125	0	4
Looting of supermarket in Concepción	160	44	149	0	2
Tsunami in Iloca and Duao towns	153	32	140	0	4
TOTAL	1181		1123	4	30
AVERAGE	168,71		160,43	0,57	4,29
False rumors					
Death of artist Ricardo Arjona	50	37	24	12	8
Tsunami warning in Valparaíso	700	4	45	605	27
Large water tower broken in Rancagua	126	43	62	38	20
Cousin of football player Gary Medel is a victim	94	4	44	34	2
Looting in some districts in Santiago	250	37	218	2	20
"Huascar" vessel missing in Talcahuano	234	36	54	66	63
Villarrica volcano has become active	228	21	55	79	76
TOTAL	1682		502	836	216
AVERAGE	240,29		71,71	119,43	30,86

Tabla 1. Fuente: Twitter Under Crisis: Can we trust what we RT? .

El resultado fue sorprendente: la cifra total de mensajes falsos (1682) superaba con creces a la de aquellos mensajes confirmados (1181).

Cabe esperar que en una situación de emergencia haya una gran confusión, por lo que cierto porcentaje de estos mensajes falsos eran errores. Sin embargo, los investigadores también pudieron demostrar la existencia de mensajes de trols, dispuestos a «jugar» con la vida de las personas.

A pesar de todo, como se ha expuesto varias veces en este capítulo, la red social funciona como una entidad con su propia inteligencia, por lo que otro de los datos que recopilamos fue especialmente relevante: el número de perfiles que afirmaban que el mensaje era cierto (1123) era muchísimo mayor que los perfiles que afirmaban que los rumores falsos eran correctos (502).

Además, en esta misma línea, resultó que había más mensajes que negaban la veracidad de una noticia falsa (836) frente a aquellos que negaban una noticia verdadera (4).

En el 2010 era mucho más fácil que el periodismo ciudadano propio de la comunidad sirviera como mecanismo de control a los bulos o las noticias falsas, tuvieran el origen que tuvieran.

Sin embargo, hoy día ya no es tan fácil que la propia comunidad pueda ejercer de fuente de validación. La intrusión de redes con miles de bots crea una especie de cortafuego que dificulta especialmente la labor. Salvo que el ciudadano esté presente, su perfil tenga alcance y sepa redactar de manera correcta lo que está viendo o conoce, la red de bots cubrirá la situación como una neblina que no deja pasar la luz.

A cambio, hoy día prácticamente todos los organismos públicos tienen presencia en las redes. Esto facilita la concienciación al ciudadano de que, en situaciones de emergencia, solo se fie de fuentes fiables, con la potestad de

organizar a la ciudadanía y actuar rápidamente como, por ejemplo, Protección Civil, el Ejército, etc.

Crimen, cibercrimen y mercenarios en redes sociales

Como era de imaginar, los criminales también encontraron en las redes sociales una vía para llevar a cabo sus fechorías, utilizando técnicas de ingeniería social muy cercanas a las técnicas de propaganda y *posverdad*, que es relevante conocer y estudiar por la inspiración que pudiera generar, aunque en este capítulo solo se pretende avanzar unas líneas generales sobre lo que se presentará en profundidad en posteriores.

Desde el ámbito de la seguridad, los principales problemas se relacionan con el acoso infantil, los robos y los secuestros; entre otras cosas, gracias al hecho de que la ciudadanía suele compartir más información sensible de la que imagina. En este sentido sorprende, por ejemplo, encontrar en YouTube un videoclip de Johnny Escutia⁷³, un rapero mexicano que narra unas instrucciones de cómo secuestrar a alguien y pedir un rescate, haciéndolo parecer muy fácil. Si bien es cierto, que el vídeo puede ser irónico, también lo es la exactitud del proceso de secuestro y obtención del rescate. Un vídeo que empieza con las siguientes instrucciones: «Óyeme, escúchame, te daré unos consejos; hazte una cuenta falsa de Facebook para estafar a pendejos, ponte nombre de mujer y fotos de una perra que se ve bien, busca amigos que tengan dinero y haz confianza después de un tiempo [...].», demuestra lo fácil que podría llegar a ser que un ciudadano caiga en la trampa.

El salto de la ficción a la realidad en México es muy pequeño. Si el lector busca en Google «secuestros en Facebook» podrá leer innumerables noticias de casos que reflejan la credulidad de los ciudadanos ante la comunicación digital. Y, sin duda, puede destacarse el caso de un grupo criminal que llevó a cabo este tipo de actos creando una cuenta falsa de una tal Tania Valencia⁷⁴, a través de la cual consiguieron realizar varios secuestros.

Además del ámbito de la seguridad, sin duda los cibercriminales son quienes más éxito están teniendo en el uso de las redes sociales con fines económicos.

Los *phishing* de toda la vida se transforman para adaptarse a estas plataformas que, como nos obligan a vivir en la «inmediatez», juegan con una menor reflexión por parte del usuario que hace clic⁷⁵.

⁷³ YOUTUBE. «Secuestros con Facebook (versión sin censura)» [en línea]. 30 julio 2011. Disponible en web: https://www.youtube.com/watch?v=KJOul2ocfxl&has_verified=1.

⁷⁴ REDACCIÓN. «Secuestradores engañaban a víctimas por Facebook» [en línea], en *Excelsior*. 19 febrero 2015. Disponible en web: <http://www.excelsior.com.mx/comunidad/2015/02/19/1009221>.

⁷⁵ FRENKEL, Sheera. «Hackers hide cyberattacks in social media posts» [en línea], en *The New York Times*. 28 mayo 2017. Disponible en web: https://www.nytimes.com/2017/05/28/technology/hackers-hide-cyberattacks-in-social-media-posts.html?_r=0.

Realizan los acercamientos a las víctimas a través de dos tácticas principales:

- a) Suplantando la identidad de una persona o una organización, pública o privada.
- b) Creando redes de bots para difundir enlaces con *software* malicioso a través de la Red.

Un ejemplo muy típico de la suplantación de identidad, no solo para *phishing* sino también para estafa, es el de la *sextorsión*. Aprovechando aquellas redes que facilitan la grabación de vídeo, se hacen pasar por «una amiga bebida dispuesta a desnudarse» o por el «hombre de tu vida que quiere sentirte cerca». Los estafadores invitan a las víctimas a grabarse desnudos y en actos sexuales y una vez que disponen del vídeo, extorsionan a la víctima ante el miedo de que el vídeo será publicado⁷⁶.

Respecto a la red de bots, el desarrollo de técnicas de ingeniería social avanzadas puede hacer que una víctima caiga rápidamente en la trampa para un *software* malicioso. Por ejemplo, jugar con la obsesión de la reputación de las personas en Internet puede generar la inquietud suficiente como para aceptar la invitación de un buen samaritano como este:

A screenshot of a Twitter message. The text reads: "FYI this profile on twitter [bit.ly/VD8L22](https://twitter.com/bit.ly/VD8L22) is spreading nasty blogs around about you". Below the text, it says "16 ene 13 04:53 p.m.". The message is displayed in a light gray box with a thin border.

FYI this profile on twitter [bit.ly/VD8L22](https://twitter.com/bit.ly/VD8L22) is spreading nasty blogs around about you
16 ene 13 04:53 p.m.

Imagen 13: Fuente, captura propia de un perfil yihadista. Mensaje intimidatorio.

Otra tipología de delito asociada a la reputación tiene que ver con los mercenarios que son contratados para contaminar con comentarios a favor o en contra de un producto o servicio, o también perfiles de influencia chantajistas que amenazan a las marcas con publicar contenido contra las mismas si no se cede a sus deseos.

En 2013 se produjo en EE.UU. la detención de varias personas asociadas a diecinueve empresas que llevaban más de un año operando en Internet bajo la falsa apariencia de ser una agencia especializada en *marketing online*. El caso se denominó Operation Clean Turf⁷⁷ y destapó un mercado jugoso de opiniones falsas, ya que no solo se instaba a los empleados de estas empresas a

⁷⁶ HICKEY, Shane. «Cyber criminals move to exploit 'safe' social media spaces» [en línea], en *The Guardian*. 5 diciembre 2016. Disponible en web: <https://www.theguardian.com/money/2016/dec/05/cyber-criminals-exploit-safe-spaces-social-media-sites-blackmail>.

⁷⁷ NEW YORK STATE OFFICE OF THE ATTORNEY GENERAL. «A.G. Schneiderman announces agreement with 19 companies to stop writing fake online reviews and pay more than \$350000 in fines» [en línea]. 23 septiembre 2013. Disponible en web: <https://ag.ny.gov/press-release/ag-schneiderman-announces-agreement-19-companies-stop-writing-fake-online-reviews-and>.

mentir, sino que contrataron profesionales *freelance* en países como Filipinas, Bangladesh y Europa del Este. Los comentarios se pagaban al peso, entre uno y diez dólares por comentario. Hoy día, con el desarrollo de los bots, pueden llevarse varias de estas campañas de engaño a la vez sin el mínimo esfuerzo y sin necesitar de una red de empleados y *freelance* como apoyo.

Terrorismo: el Dáesh en las redes sociales y contrapropaganda

Si bien es cierto que, desde el principio, las redes sociales sirvieron también para difundir mensajes políticos asociados a la extrema izquierda y la extrema derecha⁷⁸, el consenso es total para reconocer el mérito al grupo terrorista Dáesh del uso de las redes como un arma de guerra.

Toda la habilidad de los nativos digitales puesta al servicio de una de las ideologías más violentas de los últimos tiempos. Sin duda, una gran revolución al utilizar códigos propios de las guerras medievales, como la decapitación de «infieles», junto a los códigos de comunicación digital más innovadores.

Todo pensado y bien calculado para impactar sobre los ciudadanos de Occidente y llevar la guerra a su mente, haciéndose presentes en cualquier momento y lugar con mensajes aterradores como, por ejemplo, los mensajes intimidatorios sobre cómo preparaban para la guerra a sus hijos, mientras los hijos de los occidentales «van de fiesta y se emborrachan». Una temática abordada por los seguidores del grupo terrorista con gran frecuencia, no solo por parte de los hombres y padres, sino también de las mujeres y madres del Dáesh.



Imagen 14: Fuente, captura propia. Mensajes de orgullo de una de las «madres» más conocidas del Dáesh.

⁷⁸ SAN MARTÍN, José. «La coartada intelectual de la Extrema Derecha europea», en *Revista Claves de Razón Práctica*. N.º 223. Julio/agosto 2012.



Al Britaniyya @UmmKhatab__ · Jun 28

Look at my little mujahid this kid is the funniest man love him to much pic.twitter.com/36TkPwjKXJ

↩ Reply ↻ Retweet ★ Favorite

Flag media

Imagen 15: Fuente, captura propia. Vídeo del Dáesh para captación, inspirado en el videojuego Call of Duty.

También la forma de reclutar guerreros y apoyos cambió completamente con el uso que les dieron a las redes sociales. Estas se utilizaron de forma exhaustiva tanto en comunicaciones directas con los potenciales, a los que iban convenciendo poco a poco a través de mensajes privados o grupos cerrados en Facebook con tácticas propias de una secta, como en campañas de comunicación masivas, dirigidas por el fallecido ministro de Información, Abu Mohamed al Furqan⁷⁹. Estas últimas se llevaban a cabo con la intención de inundar las redes sociales no solo para provocar terror en el «enemigo», sino también con el objetivo de activar a grupos potenciales de forma rápida y eficaz. Un caso muy conocido tuvo lugar con la sinergia entre la revista digital del Dáesh, Dabiq⁸⁰ (hoy en día transformada en Rumiya), y su difusión en todas las redes sociales que dominaban para que llegara a cuanta más gente, mejor. Sin miedo ni respeto ninguno por que cayera en manos enemigas, mas todo lo contrario.

Siguiendo con la captación a través de redes sociales, cabe destacar, para comprender mejor su dominio de las mismas, el hecho de que una de las

⁷⁹ CARRIÓN, Francisco. «El IS confirma la muerte de su ministro de Información» [en línea], en *El Mundo*. 10 octubre 2016. Disponible en web: <http://www.elmundo.es/internacional/2016/10/10/57fbff35e2704ef86b8b45b4.html>

⁸⁰ BALLESTEROS MARTÍN, Miguel Ángel. «La estrategia del Dáesh a través de su revista Dabiq» [en línea], en *Instituto Español de Estudios Estratégicos*. 13 septiembre 2017. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_analisis/2017/DIEEEA51-2017_Estrategia_Dáesh_Revista_Dabiq_MABM.pdf

piezas del vídeo propagandístico más relevantes se inspiró en la saga de videojuegos Call of Duty⁸¹. Demostrando una vez más su gran comprensión del perfil al que dirigían sus campañas de comunicación, esta pieza de vídeo sigue un discurso propio de la propaganda más elaborada, acompañada de música, infografías muy actuales y un argumento bien dirigido a convencer a jóvenes dispuestos a rebelarse y unirse a la «comunidad» para combatir «el mal».



Imagen 16: Fuente, Call of Duty.



Imagen 17: Fuente, elaboración propia. Esquema del uso de redes sociales por parte del Daesh.

⁸¹ Infinity Ward, Treyarch y Sledgehammer Games (Desarrolladores), «CALL OF DUTY», <https://www.callofduty.com/es/>

Hasta la aparición del Dáesh, la censura en estas plataformas era algo impensable en las democracias occidentales; sin embargo, la exposición constante a los mensajes propagandísticos basados en la crueldad de sus actos obligó a una reflexión profunda y seria sobre qué se podía considerar «libertad de expresión» y qué no, afectando así a la política de uso de los perfiles en las redes sociales.

No es nuestra intención profundizar en este capítulo sobre el uso de las redes sociales por parte del Dáesh, que da para varios monográficos. Sin embargo, sí resulta de interés para el objetivo de este capítulo plantear el esquema general de la estrategia de comunicación del grupo terrorista en las redes para alcanzar sus objetivos.

En términos generales, se podría concluir que la comunicación se centraba en tres objetivos estratégicos:

Objetivo	Convencer	Asustar	Demostrar
Idea fuerza	<i>“Con nosotros serás feliz”</i>	<i>“Tenemos fuerza de combate para ganar”</i>	<i>“Vivimos bajo la verdad y vosotros bajo una mentira”</i>
Táctica	Comunicación propia de una secta	Mensajes para intimidar	Propaganda tradicional

Imagen 18: Fuente, captura propia. Fragmento del manual de Anonymous para luchar contra el Dáesh en las redes sociales.

Igual de sorprendente fue la reacción de miembros de la comunidad de las redes sociales y, posteriormente, de los diferentes Gobiernos del mundo.

El caso de Anonymous contra Dáesh circula todavía hoy por la red social de Twitter. El conocido grupo hacktivista decidió reaccionar por su cuenta al hecho de que las plataformas no censurasen los mensajes de captación del grupo terrorista, así como tampoco los vídeos violentos como los de las decapitaciones. Con ayuda de otros tantos *hackers* de la comunidad que sentían que sus redes estaban siendo contaminadas, iniciaron varias campañas bajo el lema «#OpISIS» con la intención de erradicar todos los perfiles de apoyo al grupo terrorista. Incluso crearon un manual⁸² para fomentar la participación ciudadana en el movimiento, muy a

⁸² CUTHBERTSON, Anthony. «Anonymous#OpParis: Hacktivists publish 'noob's guide' for fighting Isis online» [en línea], en *International Business Times*, 17 noviembre 2015. Disponible en web: <https://www.ibtimes.co.uk/anonymous-opparis-hacktivists-publish-noobs-guide-fighting-isis-online-1529173>.

pesar de varios servicios de inteligencia de diferentes países, que estaban aprovechando la comunicación «en abierto» de los terroristas para elaborar sus estrategias de seguridad.

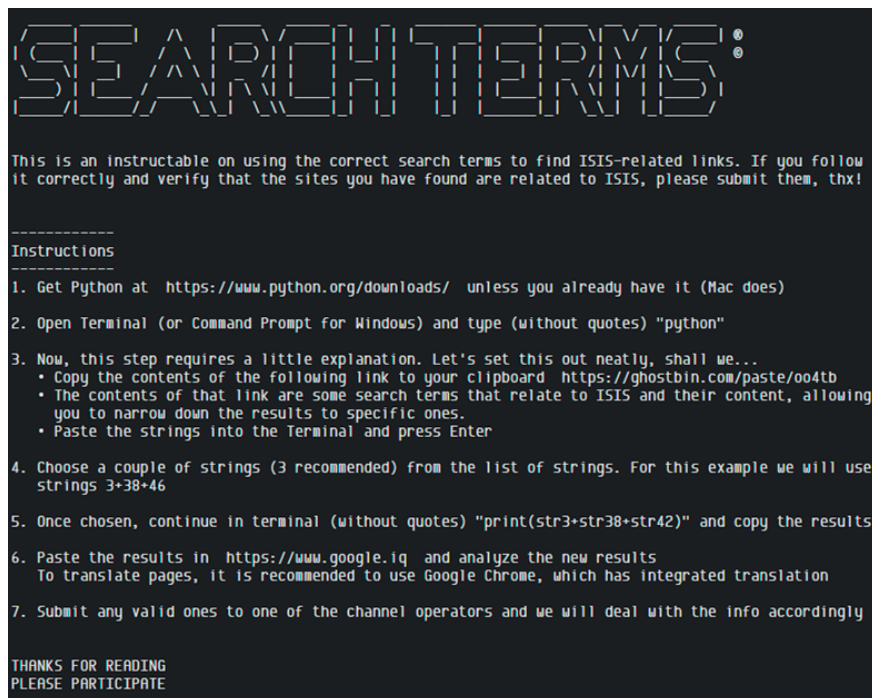


Imagen 19: Fuente, captura propia de Twitter. ISIS-chan dirigiéndose a sus fieles y explicando cómo cortar bien el melón.

Aunque la acción se inició desde la propia comunidad para defender su espacio digital, pronto nacieron varias iniciativas gubernamentales para combatir al Daesh en las redes, incluyendo a la ONU, quien consideró que las plataformas digitales también debían responsabilizarse en la lucha antiterrorista, algo hasta la fecha totalmente inédito⁸³.

Otro ejemplo muy bueno de contrapropaganda surgió desde Japón. Crearon un personaje cómico llamado ISIS-chan, una chica jovial y apasionada que organiza un ejército de melones. Un concepto totalmente inspirado en los típicos dibujos de Anime tan icónicos de este país.

ISIS-chan va vestida con las ropas del grupo terrorista, y es dibujada e infiltrada en las redes sociales para cumplir con varios objetivos:

⁸³ ORTEGA DOLZ, Patricia, « La ONU quiere implicar a Twitter y Facebook contra los yihadistas», El País, 28 de Julio de 2015, https://elpais.com/internacional/2015/07/28/actualidad/1438080089_353641.html.

- a) Contaminar las búsquedas en los buscadores como Google y las búsquedas en las redes sociales. De esta manera, cuando alguien sensible a dejarse convencer buscaba información, se encontraba con ISIS-chan haciendo tonterías. Objetivo: hundir el SEO del Dáesh.
- b) Eliminar toda trascendencia en las fotografías que el grupo terrorista difundía en las redes. Los creadores de la campaña recopilaban las fotografías más vistas y realizaban un montaje muy gracioso con ISIS-chan, asumiendo, además, que las cabezas cortadas eran melones japoneses, tremendamente cotizados en el país. Y que el hecho de que la líder de este ejército de melones sea una mujer, irritaría al Dáesh. Objetivo: diluir la sensación de amenaza.
- c) Contaminar los *hashtags* que utilizaba el Dáesh para comunicarse con sus seguidores y fieles, dificultando así su comunicación.

Algunos ejemplos de la contrapropaganda de ISIS-chan:

De todas maneras, no sería la primera vez que la comunidad reacciona contra grupos terroristas. Otro caso muy peculiar tuvo lugar en 2013 cuando el



Imagen 20: Fuente, captura propia de Twitter. ISIS-chan dirigiendo su ejército con camiones llenos de melones para el ataque del melón.



Imagen 21: Fuente, captura propia de Twitter. Seguidores de ISIS-chan demostrando su dominio del melón.



Imagen 22: Fuente, captura propia. Solicitud de contaminación de hashtag de Al Qaeda.

investigador y experto en contraterrorismo yihadista J.M. Berger solicitó a la comunidad que le ayudaran a *trolea* una campaña de inteligencia colectiva abierta por Al Qaeda para recoger ideas para sus campañas de propaganda en los medios de comunicación. La comunidad participó ofreciendo

ideas muy ácidas y bloqueando toda la capacidad de Al Qaeda de alcanzar su objetivo:

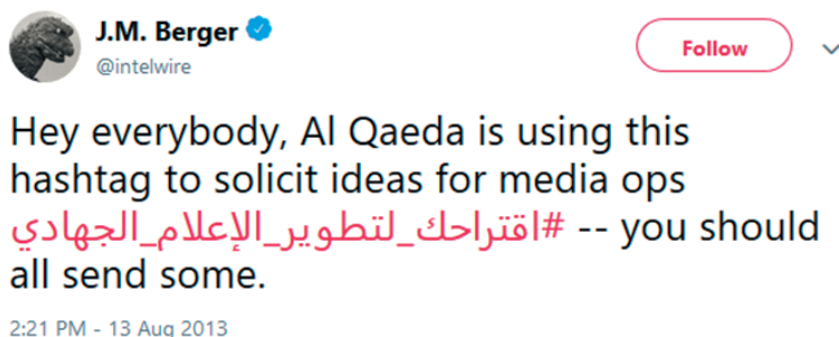


Imagen 23: Fuente, captura propia. Una de las imágenes patrióticas de la campaña en redes sociales «Soldado ahora es tu turno» (Venezuela).

Las Fuerzas Armadas como objetivo

Existen dos casos muy interesantes relacionados con el uso de las redes sociales que impactan directamente sobre las Fuerzas Armadas y que se deben tener cuenta con la intención de preparar a las mismas para posibles situaciones de este tipo, de corte similar o en sus posibles variantes.

El primero de ellos tiene lugar durante el conflicto en Afganistán, en 2012. Entre las tácticas de inteligencia de los insurgentes, se despliegan varias maniobras en las redes sociales a través de la generación de decenas de perfiles falsos basados en mujeres con la intención de obtener información de los soldados de la OTAN presentes en el territorio.

Los insurgentes realizaban una monitorización exhaustiva de las redes en busca de soldados que comentaran su presencia actual o próxima en la zona, captaban su atención bajo estos perfiles falsos de mujeres y conseguían obtener información personal y relevante del soldado que posteriormente utilizaban tanto para conocer las maniobras de la OTAN como para amedrentar a los soldados a través del uso psicológico del miedo al daño a su familia⁸⁴.

Fue Australia quien detectó este tipo de prácticas, sobre las que alertó a través de un informe donde demostraba que los soldados no eran conscientes de la información que suministraban a través de las redes, pues no vinculaban el uso de estas al concepto de seguridad.

⁸⁴ BEN FARMER, Kabul. «Taliban pose as women to friend soldiers on Facebook» [en línea], en *The Telegraph*. 11 septiembre 2012. Disponible en web: <https://www.telegraph.co.uk/news/worldnews/asia/afghanistan/9535862/Taliban-pose-as-women-to-friend-soldiers-on-Facebook.html>.

Para luchar contra el desconocimiento y el riesgo derivado del mismo, crearon una guía específica sobre cómo debe proceder el personal de defensa en las redes sociales⁸⁵, algo imprescindible hoy día en cualquier organización de este tipo.

El segundo de los casos que merece una mención especial es el realizado por la oposición venezolana en 2014 con la intención de rebelar al Ejército venezolano contra el presidente Maduro.

La peculiaridad de esta campaña radica en que para conseguir que el mensaje fuera viral se buscó alcanzar dos *trending topic* (TT) encadenados en Twitter, algo inédito hasta la fecha para un objetivo como este.

El primer TT venía acompañado del *hashtag* «#VenezuelaMuereTuCallas». El objetivo estaba muy bien definido: utilizando toda una batería de imágenes y vídeos conmovedores que buscaban demostrar las penurias que atraviesan los venezolanos bajo el Gobierno de Maduro, se conseguía llamar la atención de prácticamente todo el país.

Una vez con la atención puesta en este TT, se introducía el mensaje real con el objetivo final que se esperaba conseguir a través del *hashtag* «#SoldadoAhoraEsTuTurno», que también se convirtió en TT amplificado gracias al anterior.



Imagen 24: Fuente, captura propia. Una de las imágenes patrióticas de la campaña en redes sociales «Soldado ahora es tu turno» (Venezuela).

«Soldado ahora es tu turno» es un ejemplo claro de campaña de propaganda contra las Fuerzas Armadas. En línea con los típicos mensajes

⁸⁵ AUSTRALIAN GOVERNMENT. «Use of social media by Defence personnel» [en línea], en *Department of Defence*. 16 enero 2013. Disponible en web: <https://www.defglis.com.au/resources/SocialMediaPolicy.pdf>.

de panfleto contra las «fuerzas enemigas», utiliza los medios digitales para «mover conciencias» y procurar su objetivo: que el Ejército se volviera contra Maduro con la intención de «liberar al pueblo de su yugo».

Para conseguirlo, la campaña iba acompañada una pieza de vídeo⁸⁶ elaborada según las normas y reglas básicas de la propaganda y que seguía un guión muy elaborado, donde se había cuidado, incluso, el ritmo de la banda sonora para motivar las emociones justas que llevaran a la reacción deseada:

- a) Despertar conciencias: Mostrando la crudeza de los actos del presidente Maduro y de cómo utiliza las fuerzas y cuerpos de seguridad contra ciudadanos inocentes y desarmados.
- b) Reconocimiento de grupo: Mostrando cómo otros soldados ya se han unido a la causa contra el presidente.
- c) Apelar al sentido de estado: Apelando a los mensajes de socorro y ayuda de una ciudadanía que está totalmente desprotegida ante el «tirano».

Si bien es cierto que el uso de la propaganda en una guerra contra las fuerzas enemigas es un clásico, no lo es tanto el uso de los medios y canales digitales para conseguirlo. Por ello, cada vez se hace más relevante incluir procesos que permitan evitar riesgos y amenazas derivados de las nuevas formas de comunicar a las que todavía no se es resiliente.

Tácticas utilizadas para combatir la propaganda y la manipulación a través de la posverdad

Algunos ejemplos de cómo distintos países con diferentes regímenes y Gobiernos han abordado la lucha contra la manipulación en las redes sociales:

- a) Táctica del bloqueo: Aniversario de Tiananmen, China. Los censores toman la decisión de bloquear el acceso a medios sociales como Twitter o Flickr para evitar posibles altercados por la celebración del 20 aniversario de lo sucedido en 1989. Además, se prepara un bloqueo especial también para los medios extranjeros de manera que si se detecta que están hablando del aniversario se corte automáticamente la noticia⁸⁷.
- b) Táctica del miedo: Turquía se mantiene en una fina línea entre permitir el uso o prohibir su uso. Si bien, hasta la fecha, ha decidido que no las prohibirá, sí las vigila muy de cerca para conocer en profundidad todo lo que dicen sus ciudadanos con la intención de procesarles o mul-

⁸⁶ YOUTUBE. «Soldado, ahora es tu turno...!» [en línea]. 9 marzo 2014. Disponible en web: <https://www.youtube.com/watch?v=qGT4iQcdAAo>.

⁸⁷ REYNOLDS, Paul. «Censura en el aniversario de Tiananmen» [en línea], en *BBC Mundo*. 2 junio 2009. Disponible en web: http://www.bbc.co.uk/mundo/internacional/2009/06/090602_1552_tiananmen_internet_jg.shtml.

tarles en función de lo que digan⁸⁸. Para ejercer más control, decidió prohibir la apertura de cuentas falsas o enmascaradas por motivos de seguridad, de manera que los ciudadanos turcos que quieran usarlas deberán identificarse, como si fuera una extensión de su identidad real en la red⁸⁹.

- c) Táctica de «el Gran Hermano»: Posiblemente la táctica más utilizada en los países occidentales y democráticos. Sin duda, uno de los casos estrella es el sucedido con el programa PRISM planteado por la NSA de EE.UU. Este programa diseña una estrategia de escuchas generalizadas en toda Internet e incluye peticiones específicas del Gobierno americano a las grandes plataformas como Facebook y Google para que les permitan acceder a contenido privado de usuarios que consideran «de riesgo»⁹⁰. Sin embargo, como es de esperar, no solo EE.UU. utiliza este tipo de vigilancia digital; según Le Monde, Francia también tiene un programa de estas características⁹¹.
- d) Táctica de «la siembra»: Esta es más bien una táctica de construcción de una realidad alternativa. Está dirigida a modificar la percepción y reputación, por ejemplo, de un país en Internet y con ello obtener todos los beneficios que una buena reputación ofrece a quien la tiene: mejora en el turismo, aumento en la compra de sus productos y servicios, mejora en las condiciones financieras internacionales, etc. Para ello, EE.UU. comenzó destinando en 2013 630 000 dólares para comprar «fans»⁹². Por supuesto, esta misma táctica puede ser utilizada para crear una mala reputación contra aquellos países o sectores de países que resulten ser competidores o enemigos.

⁸⁸ EFE. «Un pianista turco condenado a 10 meses de cárcel por criticar el islam en Twitter» [en línea], en *El País Internacional*. 15 abril 2013. Disponible en web: http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587_412492.html.

⁸⁹ «Fake social media accounts to be prevented: Turkish deputy PM» [en línea], en *Turkish Weekly*. 21 junio 2013. Disponible en web: <http://www.turkishweekly.net/news/152201/fake-social-media-accounts-to-be-prevented-turkish-deputy-pm.html>.

⁹⁰ GREENWALD, GLENN & McASKILL, Ewen. «NSA Prism program taps in to user data of Apple, Google and others» [en línea], en *The Guardian*. 7 junio 2013. Disponible en web: <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>.

⁹¹ FOLLOROU, Jacques; JOHANNÈS, Franck. «Révélations sur le Big Brother français» [en línea], en *Le Monde*. 4 julio 2013. Disponible en web : http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html.

⁹² ZHANG, Moran. «US State Department Facebook 'Likes': DOS Spent \$630,000 On Buying Fans» [en línea], en *International Business Times*. 4 julio 2013. Disponible en web: <http://www.ibtimes.com/us-state-department-facebook-likes-dos-spent-630000-buying-fans-1334457#>.

Capítulo cuarto

La disrupción digital en el contexto de las guerras híbridas

Javier Lesaca Esquiroz

Resumen

Las guerras híbridas son la principal amenaza para la estabilidad de una nación Estado como España. Las ofensivas asimétricas pueden provenir por parte de otros Estados, pero también por parte de grupos de naturaleza subnacional y no estatal. Las batallas por condicionar y manipular de manera artificial la opinión pública representan un arma cada vez más poderosa para erosionar la cohesión social de un país y el pacto social que une a los ciudadanos con sus instituciones públicas. La evidencia y el análisis científico demuestran que, en los últimos cinco años, las operaciones ofensivas de disrupción comunicativa por parte de Gobiernos y de grupos violentos y extremistas han aumentado en cantidad y en complejidad. La investigación y monitorización de estos intentos de desestabilización de la opinión pública demuestra que existe una metodología de la disrupción que consiste en los siguientes procesos: a) detección de las vulnerabilidades sociales de un país; b) creación de una narrativa que fomente estas vulnerabilidades en la opinión pública; c) implementación de una red de medios de comunicación propios, y d) utilización automatizada y tramposa de las plataformas de comunicación social. Los Estados deben entender la naturaleza de esta amenaza y construir capacidades que permitan hacerle frente con eficacia.

Palabras clave

Guerra híbrida, interrupción, comunicación, desinformación, opinión pública.

Abstract

Hybrid warfare are the main threat to the stability of a nation-state like Spain. Asymmetric offensives may come from other states, but also from subnational and non-state groups. The battles to artificially manipulate the public opinion of a given country represent an increasingly powerful weapon to erode the social cohesion of a country and the social contract that links citizens with their public institutions. Evidence and scientific analysis reveal that, in the last five years, the offensive operations of communicative disruption by governments and violent and extremist groups have increased in quantity and complexity. The investigation and monitoring of these attempts to destabilize public opinion shows that there is a methodology of disruption that consists of the following processes: a) detection of social vulnerabilities in a country; b) creation of a narrative that fosters these vulnerabilities in the public opinion; c) implementation of a network of own communication media; d) automated and cheating use of social communication platforms. States must understand the nature of this threat and build capacities that allow it to face it effectively.

Keywords

Hybrid warfare, disruption, communication, disinformation, public opinion.

La revolución tecnológica y sus implicaciones en la gobernanza

En el año 2013, los ejecutivos de Google Eric Schmidt y Jared Cohen eran optimistas con respecto al papel que las nuevas tecnologías de la información iban a jugar en la construcción y formación de la opinión pública. Según estos autores, las nuevas plataformas digitales servirían para construir una sociedad más y mejor informada: «Las personas que traten de perpetuar mitos sobre religión, cultura, etnicidad o cualquier otra cosa tendrán que luchar por mantener sus narrativas a flote entre un mar de nuevas audiencias informadas»¹. Sin embargo, la realidad está constatando que las narrativas basadas en mitos se han adaptado con gran pericia al nuevo entorno digital y están saliendo a flote con éxito «en el mar de nuevas audiencias informadas».

El caso del Estado Islámico o Dáesh, entre otros, ha sido un ejemplo paradigmático de la eficaz adaptación de las narrativas mitológicas al nuevo contexto informativo digital. Estado Islámico entendió, desde su nacimiento en el año 2013, la comunicación como un pilar clave de su estrategia. En este sentido, este grupo yihadista siguió el comportamiento de los movimientos populistas tradicionales, que siempre han entendido la estrategia de comunicación como una de sus principales armas. Como explica Silvio Waisbord:

«Lo mediático siempre obsesionó al populismo, aun cuando los medios masivos eran la prensa, el cine y la radio a mediados del siglo xx. El populismo siempre estuvo convencido de que su éxito político requiere tener una sensibilidad extrema a los medios y replantear su funcionamiento de acuerdo con objetivos políticos... Para el populismo, los medios siempre fueron esencialmente instituciones políticas que deben ser colocados en el centro de la acción de Gobierno»².

Mishra considera en este sentido que el grupo terrorista Dáesh forma parte de la lista de movimientos populistas contemporáneos que están utilizando las nuevas plataformas de la comunicación como parte esencial de su proyecto político. Según este autor:

«Las mentes malignas de [sic] Dáesh se han dispuesto con particular energía a utilizar este mundo interdependiente en beneficio propio; en sus manos, Internet se ha convertido en un arma propagandística de devastadora eficacia para la yihad mundial. Pero los demagogos de todos los colores, desde Recep Tayyip Erdogan en Turquía, pasando por Narendra Modi en la India y Marine Le Pen en Francia, hasta Donald

¹ SCHMIDT, Eric; COHEN, Jared. *The New Digital Age: Transforming Nations, Business, and Our Lives*. Vintage Books. 2013. p. 35.

² WAISBORD, Silvio. *Vox Populista*. Gedisa. 2014. p. 17.

Trump en Estados Unidos, han pescado en aguas revueltas del cinismo, el aburrimiento y el descontento»³.

A pesar de su optimismo inicial, Eric Schmidt y Jared Cohen ya reconocían en el año 2013 que la revolución tecnológica estaba emparejada a una revolución en el ámbito de la gobernanza cuyas consecuencias eran y siguen siendo imprevisibles:

«La tecnología empodera a todas las partes involucradas y permite a los actores más pequeños tener impactos muy grandes. Y esos actores no necesitan ser oficiales o no oficiales. Por lo tanto, estamos convencidos de que es posible que se formen Estados virtuales y que sacudirán el entorno digital de los estados *[sic]* físicos en el futuro»⁴.

La previsión de Schmidt y Cohen tiene unas profundas implicaciones no solo para las instituciones públicas, sino para el actual orden mundial de Gobierno, basado precisamente en las relaciones entre Estados. La hipotética desaparición de los actuales Estados nación por modelos de «Estados virtuales» implica pensar en un sistema de gobierno, de relaciones internacionales y de convivencia completamente nuevo, desconocido y carente de certezas o seguridades jurídicas y legales. Un entorno ideal para el surgimiento de nuevos actores de poder que, en muchos casos, no tienen entre sus prioridades el reforzamiento de los modelos de democracia liberal basados en el respeto de los derechos y libertades de los ciudadanos. Mishra coincide en mostrar su pesimismo ante el prolongando declive de las actuales y tradicionales formas de gobierno que se está viviendo desde comienzo del siglo xxi:

«La globalización, caracterizada por capitales móviles, comunicaciones aceleradas y rápida movilidad, ha debilitado velozmente las formas anteriores de autoridad en todas partes, tanto en las democracias sociales de Europa como en los despotismos árabes, y ha generado una serie de nuevos e imprevisibles actores internacionales, desde nacionalistas ingleses y chinos, piratas somalíes, traficantes de seres humanos y *hackers* anónimos hasta Boko Haram. Las ondas de choque que emanaron de la crisis económica de 2008, del Brexit y de las elecciones presidenciales norteamericanas de 2016 confirmaron que, como escribió Hannah Arendt en 1968, por primera vez en la historia, todos los pueblos de la tierra tienen un presente común»⁵.

Existe un consenso académico en señalar que las expectativas generadas por la disrupción de las redes sociales en el siglo xxi en el ámbito de la comunicación han irrumpido con fuerza en un complejo escenario político. La tecnología que nació con la promesa de fortalecer el debate público, mejorar la calidad democrática de los Gobiernos y acercar a los ciudadanos con sus

³ MISHRA, Pankaj. *La edad de la Ira*. Galaxia Gutenberg. 2017. p. 17.

⁴ SCHMIDT, Eric; COHEN, Jared. *Op. cit.*, p. 35.

⁵ MISHRA, Pankaj. *Op. cit.*, p. 16.

administraciones e instituciones públicas se ha revelado como una de las principales amenazas de las propias estructuras de Gobierno. Esta afirmación no supone negar el potencial positivo y las constructivas aportaciones que las nuevas tecnologías están realizando en el ámbito de la mejora de la gobernanza. Estas reflexiones solo pretenden alertar del potencial destructivo que tienen estas herramientas si se utilizan con el objetivo de anular, debilitar o sustituir los actuales modelos de gobierno por nuevos modelos de poder que pueden conducir a un inexplorado e inquietante orden mundial. Tal vez, como reconoció el filósofo alemán Jürgen Habermas en una entrevista el 6 de mayo de 2018, «Es posible que con el tiempo aprendamos a manejar las redes sociales de manera civilizada»⁶.

De la misma forma que el nacimiento de la imprenta fue el detonante de los profundos cambios políticos, religiosos y sociales que se vivieron en Europa a partir del siglo xv, en especial del auge de la nación Estado⁷, la irrupción de las nuevas tecnologías de la comunicación puede estar provocando un nuevo fenómeno social y político con implicaciones en las raíces mismas de la democracia y la nación Estado⁸. Peter Dahlgren alertó en 2005 de las complejas consecuencias que tendría Internet en las democracias⁹. Cuatro años más tarde, Manuel Castells confirmó que «el proceso de formación y ejercicio de las relaciones de poder se transforma radicalmente en el nuevo contexto organizativo y tecnológico derivado del auge de las redes digitales de comunicación globales»¹⁰.

Castells considera que el principal cambio comunicativo que se produjo a comienzos del siglo xxi fue la llegada de lo que define como los «medios de auto comunicación de masas»¹¹. Según señalan Miskimmon, O'Loughlin y Roselle, las reflexiones de Castells sugieren que «la comunicación ha cambiado cómo funciona el poder»¹². Para este grupo de autores, «Internet y las plataformas de comunicación social han permitido a cualquier persona narrar y comunicar lo que considere, algo que antes estaba reservado a las élites»¹³.

⁶ HERMOSO, Borja. «Entrevista a Jürgen Habermas» [en línea], en *El País*. 6 mayo 2018. Disponible en web: https://elpais.com/elpais/2018/04/25/eps/1524679056_056165.html.

⁷ ANDERSON, Benedict. *Imagined Communities*. Londres: Verso. 1983.

⁸ DAHLGREN, Peter. *Media and Political Engagement*. Cambridge: Cambridge University Press. 2009.

⁹ DAHLGREN, Peter. «The Internet, Public Spheres, and Political Communication: Dispersion and Deliberation» [en línea]. 2005. Disponible en web: <http://www.tandfonline.com/doi/abs/10.1080/10584600590933160>.

¹⁰ CASTELLS, Manuel. *Comunicación y poder*. Madrid: Alianza Editorial., 2009.

¹¹ CASTELLS, Manuel. «Communication, Power and Counter-Power in the Network Society». *International Journal of Communication* 1, n.º 1, 2007.

¹² MISKIMMON, Alistair; O' LOUGHLIN, Ben; ROSELLE, Laura. *Strategic Narratives. Communication Power and the New World Order*. Routledge. 2013. p. 2.

¹³ Ibidem.

Otros autores como Moisés Naim se muestran más escépticos sobre el verdadero papel que Internet está teniendo en la transformación de las relaciones de poder y de gobierno. Naim considera que:

«La degradación del poder no se debe a Internet ni a las tecnologías de la información en general [...] Es innegable que Internet, las redes sociales y otras herramientas están transformando la política, el activismo, la economía y, por supuesto, el poder. Pero ese papel, importante, se exagera y malinterpreta con demasiada frecuencia. Las nuevas tecnologías de la información son eso, herramientas, que para causar efecto necesitan unos usuarios que, a su vez, tienen objetivos, dirección y motivación. Facebook, Twitter y los SMS contribuyeron de manera crucial a fortalecer a los manifestantes en la Primavera Árabe. Pero los manifestantes y las circunstancias que les impulsaron a salir a la calle nacieron de situaciones dentro y fuera de sus países que no tenían nada que ver con Twitter o Facebook»¹⁴.

Según destaca Naim:

«El primer y más importante motor de la protesta fue la realidad demográfica de los jóvenes en países como Túnez, Egipto y Siria, personas más sanas y mejor preparadas que nunca, pero sin trabajo y profundamente frustradas[...]Sería un error tanto negar la función crucial que tienen las tecnologías de la información, en particular las redes sociales, en los cambios que estamos presenciando, como considerar que esos cambios son consecuencia exclusivamente de la adopción generalizada de estas tecnologías»¹⁵.

La revolución tecnológica, por tanto, podría entenderse como el combustible que ha avivado y escalado la hoguera de frustración ciudadana y crisis institucional que había prendido de manera global. El caso del Daesh es, una vez más, paradigmático de esta situación. La marginación y falta de encaje político de la población Suní en Irak y Siria, junto con las altas tasas de corrupción, desempleo juvenil y deficiente prestación de servicios públicos provocaron un creciente malestar y aumento de la desconfianza ciudadana ante sus instituciones. Sin embargo, para entender la rapidez con la que este malestar escaló, provocó movilizaciones y se canalizó hacia propuestas violentas y extremistas hay que incluir en la ecuación variables e indicadores tecnológicos. En este sentido, resulta muy valioso entender que en Irak, el país donde surgió Estado Islámico a finales del año 2013, el 92,2% de los adultos del país tiene teléfono móvil; un tercio de los ciudadanos (34,1%) ha usado el móvil para conectarse a Internet durante la última semana; el 40,3% de los ciudadanos encuestados reconoció haberse conectado a Internet durante la última semana; un 73,9% de los usuarios de Internet consume con frecuen-

¹⁴ NAÍM, Moisés. *El fin del poder*. Debate. Octubre 2013. p. 35.

¹⁵ NAÍM Moisés. *Op. cit.*, p. 36.

cia programas de televisión, noticias, vídeoclips, deportes y películas. y el 30% de los encuestados también reconoció haber usado las redes sociales durante la última semana¹⁶.

La revolución tecnológica ha dotado y «armado» a un gran número de ciudadanos de unas herramientas que les permiten, con mayor facilidad que nunca, marcar agenda, crear encuadres e influir en el proceso de conformación de la opinión pública «sin tener que pasar por las puertas de los medios de comunicación tradicionales», tal y como explicaba Nacos en 2002¹⁷. Esta situación es la que ha generado el nuevo fenómeno comunicativo de *auto-comunicación de masas* al que aludía Castells en 2009, un fenómeno «que incrementa de forma decisiva la autonomía en la medida en la que los usuarios se convierten en emisores y receptores del mensaje»¹⁸.

Silvio Waisbord también advierte del profundo cambio estructural que ha vivido el sector de los medios de comunicación y las consecuencias que estos cambios tienen en las relaciones de poder. Waisbord considera que:

«Los desarrollos tecnológicos posteriores en la primera mitad del siglo xx, el cine, la radio y la televisión ampliaron la condición de medios masivos como instituciones que controlaron el flujo unidireccional de información y contenidos. Los medios, como categoría, se identifican con la presunta unidad de industrias y tecnologías a gran escala que detentan una posición única y un poder notable [...]».

Sin embargo, la revolución tecnológica que se vivió a comienzos del siglo xxi cambió completamente estas reglas de juego. Tal y como indica Waisbord:

«En años recientes este orden de los medios masivos se ha resquebrajado, principalmente, debido a innovaciones tecnológicas que posibilitan la comunicación por fuera de las estructuras clásicas, masivas, de las viejas tecnologías e industrias[...] La digitalización y el crecimiento de Internet provocaron la explosión de medios y resquebrajaron divisiones tajantes entre comunicación interpersonal y masiva¹⁹».

Estas dos circunstancias (crisis de credibilidad y empoderamiento tecnológico) han dinamitado el escenario tradicional de configuración de la opinión pública. De igual modo, se ha debilitado la hegemonía que poseían los Gobiernos para generar y transmitir verticalmente enfoques y encuadres hegemónicos. Esta situación es aprovechada por grupos posmodernos subnacionales (algunos extremistas y violentos), movimientos sociales y grupos

¹⁶ Gallup. «Broadcasting Board of Governors. Media Use in Irak and Irak Kurdistan» [en línea]. Marzo 2015. Disponible en web: <https://www.bbg.gov/wp-content/media/2015/03/Irak-brief-FINAL.pdf>

¹⁷ Nacos, Brigitte L. *Mass-Mediated Terrorism*, Rowman & Littlefield Publishers. Londres: Inc. 2002.

¹⁸ CASTELLS, Manuel. *Op. cit.*, s.p.

¹⁹ WAISBORD, Silvio. *Op. cit.*, p. 26.

de presión (identificados o encubiertos) para comunicarse de manera directa con sus audiencias mediante novedosas técnicas de *marketing* e influir en la opinión pública de una manera eficaz. A diferencia de los medios de comunicación tradicionales, el nuevo escenario de comunicación no está basado en la transmisión de datos y hechos, sino en la difusión eficaz de historias conmovedoras, subjetividades y sentimientos, lo que conforma una opinión pública menos informada y más manipulable.

Los hechos han demostrado que el uso de Internet, las plataformas digitales sociales y las técnicas de *marketing* digital directo han reconfigurado la manera en que se crea la opinión pública y han alterado los papeles que tradicionalmente tenían asignados instituciones políticas y administrativas, medios de comunicación y ciudadanos. Es decir, la relación triangular entre los principales agentes de la comunicación se ha modificado. Este cambio en la forma en que se construye la opinión pública ha tenido efectos directos en el ámbito de las políticas públicas, de la gobernanza y, tal y como demuestra el caso de la estrategia de comunicación puesta en marcha por el Daesh desde verano de 2014, también en el ámbito de la propia modernidad.

Una estrategia de comunicación erigida sobre la base de una narrativa transmedia²⁰ atractiva y distribuida directamente a las audiencias potenciales puede fortalecer las adhesiones hacia un grupo subnacional de carácter violento y extremista. La calidad y la cantidad de estas adhesiones pueden incluso convertirse en una amenaza que compita de manera directa con la legitimidad de una nación Estado. Los casos de Irak y de Siria son ejemplos paradigmáticos que serán analizados con detalle en los próximos capítulos.

El público general, los responsables gubernamentales y los medios de comunicación de masas formaban un triángulo de intereses relacionados que tradicionalmente ha contribuido a la formación de la opinión pública²¹. La relación que se establecía entre estos actores y el modo en que entre ellos se generaban y se difundían los enfoques de las noticias quedó reflejada en el modelo de activación por cascada descrito por Robert M. Entman, quien determina el proceso de construcción de la realidad a través de significados e interpretaciones (encuadres) y cómo se difunden estos encuadres desde los niveles más altos de la Administración política y bajan hasta el público y los ciudadanos con la complicidad de los medios de comunicación²².

Entman reconoce asimismo que, excepcionalmente, los encuadres pueden ascender desde el nivel más bajo de la cascada hasta las élites administrativas y políticas. En cualquier caso, este modelo, así como todas las teorías tradicionales de la comunicación, ha explicado el campo de creación de la

²⁰ LESACA, Javier. *Op. cit.*, s.p.

²¹ NACOS, Brigitte L. et al., Inc., Nueva York, 2002.

²² ENTMAN, Robert M. *Projections of Power*. Chicago: The University of Chicago Press, 2004.

opinión pública como un escenario bien definido, con unos actores y unos papeles también fijados y delimitados.

El debate sobre el monopolio en la creación de enfoques y representaciones hegemónicas en la opinión pública es de enorme trascendencia a la hora de entender los procesos históricos que forjaron la modernidad y la posmodernidad. Edward Said considera que la creación de la *civilización occidental* se realizó en gran parte en base a las representaciones que la modernidad creó sobre *Oriente*. Según Said:

«Oriente ha ayudado a definir Europa (u Occidente), como una imagen, idea, personal y experiencia de contraste. El Oriente forma parte integral de la civilización y cultural europea. El orientalismo representa esta parte cultural e ideológica que tiene forma de discurso y que ha sido apoyado por instituciones, vocabulario, académicos, imágenes, doctrinas y burocracias coloniales²³».

Este autor considera que la creación deliberada de mensajes por parte de Occidente para crear una imagen hegemónica de Oriente tenía una clara intencionalidad política por parte de los países modernos:

«El orientalismo puede ser analizado como un elemento institucionalizado para tratar con "Oriente", hacer análisis sobre él, declaraciones autorizadas, describirlo, enseñar, ocuparlo y dominarlo: en resumen, Orientalismo como un estilo occidental para dominar, reestructurar y tener autoridad sobre "Oriente"²⁴».

Sin embargo, la guerra de encuadres, representaciones y construcción de prejuicios y estereotipos culturales con fines políticos no se ha producido simplemente de una «supuesta cultura occidental» hacia una «supuesta cultura oriental» (islámica, según la categorización de Samuel P. Huntington). Es un hecho cierto y demostrado que los principales líderes islamistas también dedicaron gran parte de sus esfuerzos a caricaturizar una imagen de Occidente también con objetivos políticos; más concretamente, con el fin de atacar a naciones Estado de la modernidad. Buen ejemplo de ello son las declaraciones de Hassan Al Banna a comienzos del siglo xx difundiendo una imagen prejuiciosa y negativa de los países europeos: «Importaron a sus mujeres medio desnudas a nuestra región, junto con sus licores, sus teatros, sus salones de danza, sus entretenimientos, sus historias, sus periódicos, sus novelas sus juegos estúpidos y sus vicios»²⁵. La caricaturización de occidente como una cultura decadente y moralmente corrompida ha sido una constante en el discurso islamista durante el siglo xx y el siglo xxi. El propio

²³ SAID, Edward. *Orientalism*. Vintage Books. New York: A Division of Random House. S.f. p. 2.

²⁴ Ibidem, p. 3.

²⁵ KAPLAN, Roy H. *Understanding Conflict and Change in a Multicultural World*. Rowman & Littlefield. 2014. p. 156.

Estado Islámico hereda la dialéctica de Hassan Al Banna: el 24 de noviembre de 2015 el Dáesh publicó un vídeo en el que ridiculizaba a los presidentes estadounidenses llamándoles «corruptos, mentirosos y fornicadores»²⁶.

La imprenta favoreció la creación de la modernidad: habilitó a los Estados el monopolio para crear imágenes propias y ajenas y construir comunidades imaginadas basadas en la razón, la ilustración, el pensamiento científico, la libertad individual y el imperio de la ley. La revolución tecnológica del siglo xxi ha robado a las naciones Estado el monopolio sobre la creación de imágenes, encuadres y estereotipos hegemónicos para definirse a sí mismas y definir «al otro». Y lo que aún es más intrigante, las nuevas tecnologías de la comunicación han habilitado a grupos antimodernos, cuya agenda pasa por romper con la herencia de la modernidad a crear imágenes y enfoques eficaces entre la opinión pública.

Schmidt y Cohen, en la reflexión que realizaron en el año 2013 sobre los potenciales escenarios de gobierno que podía generar la revolución tecnológica, ya advertían de esta particular guerra de encuadres y narrativas entre naciones Estado y naciones digitales:

«Grupos que carecen de una forma de Estado pueden elegir recrear una en el mundo digital. Aunque no tenga la misma legitimidad que un Estado real, la oportunidad de establecer soberanías virtuales puede ser, en los mejores casos, un paso útil hacia un estado [*sic*] real, y en los peores casos, la escalada de un conflicto que puede conducir hacia un complicado enfrentamiento civil»²⁷.

El Dáesh ha corroborado estas previsiones. El califato se ha establecido como una «institución virtual» con claras aspiraciones a transformarse en una institución real. Para ello ha declarado una guerra híbrida y asimétrica con batallas físicas sobre el terreno, acciones terroristas en el extranjero contra la población civil y ofensivas virtuales de comunicación digital que han logrado retar y desestabilizar no solo a los Estados de Irak y Siria, sino también a decenas de países de África, Asia, Europa e incluso Estados Unidos, Canadá o Australia.

La disrupción comunicativa como arma en el contexto de las guerras híbridas

Las guerras híbridas nacieron hace más de 2500 años. El general chino Sun Tzu, nacido en el año 544 antes de Cristo, ya dejó por escrito que «el arte de la guerra es el engaño»²⁸. Según Tzu, la «mayor excelencia en la guerra no consiste en ganar cada batalla, sino en someter al enemigo sin entrar en

²⁶ Al Hayat Media Center. *No Respite*. 24 noviembre 2015.

²⁷ SCHMIDT, Eric & COHEN, Jared. *Op. cit.*, p. 101.

²⁸ SUN Tzu (s. V a. C. /2013). *El arte de la guerra*. Ed. Medí. S.f.

batalla»²⁹. El militar prusiano nacido en 1780, Carl Von Clausewitz, también coincidió en señalar que la guerra era un concepto que iba mucho más allá del combate militar y del uso de la fuerza entre dos ejércitos. La definición que Clausewitz hace de la guerra gira entorno a dos ideas: que la guerra es una extensión de la búsqueda del interés humano, expresada a través de objetivos políticos; y que la búsqueda de esos objetivos políticos a veces implicaba el uso de la fuerza³⁰.

El mayor estadounidense Amos C. Fox en su estudio sobre las guerras híbridas considera que la definición de «uso de la fuerza» que realiza Clausewitz haría referencia hoy en día «no solo al ámbito del enfrentamiento físico, sino que incluiría los dominios de la información, el ciberespacio, el espacio electromagnético»³¹.

El investigador español Josep Baqués también considera al militar prusiano como uno de los precursores modernos de las actuales guerras híbridas. Según Baqués, la definición de guerra híbrida se ajusta a:

«La célebre trinidad de Clausewitz, según la cual el éxito de una campaña militar depende en buena medida de la conexión entre tres elementos fundamentales, esto es, la elite [*sic*] política (que el prusiano equipara a la “razón” que dirige la guerra), las fuerzas armadas [*sic*] (que equipara a la “voluntad” de luchar y vencer) y la propia sociedad (que equivaldría a la “pasión” o a la “emoción”). Por lo tanto, las brechas que puedan abrirse entre cualquiera de los vértices constituyen un auténtico Talón [*sic*] de Aquiles para toda parte de cualquier conflicto»³².

A finales del siglo xx, en el año 1999, dos generales chinos avanzaron ya con mayor precisión la complejidad y naturaleza poliédrica de los futuros enfrentamientos bélicos. Según Qiao Liang y Wang Xiangsui:

«Podemos mencionar una serie de medios y de nuevos métodos utilizados para luchar en una guerra no militar. Algunos de estos métodos existen, pero otros existirán en el futuro. Estos medios y métodos de guerra incluyen una guerra psicológica (difundir rumores que intimiden al enemigo y destruyan su estado de ánimo) y la guerra de comu-

²⁹ Ibídem.

³⁰ CARL VON CLAUSEWITZ. *On War*. Trans. HOWARD, Michael & PARET, Peter. Princeton, NJ: Princeton University Press. 1987. p. 75.

³¹ MAJ AMOS C. FOX. «Hybrid Warfare: The 21st Century Russian Way of Warfare» [en línea], en *School of Advanced Military Studies United States Army Command and General Staff College*. Fort Leavenworth, Kansas. 2017. Disponible en web: <http://www.dtic.mil/dtic/tr/fulltext/u2/1038987.pdf>.

³² BAQUÉS QUESADA, Josep. «Las guerras híbridas: un balance provisional» [en línea], en *Instituto Español de Estudios Estratégicos*. Enero 2015. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_trabajo/2015/DIEET01-2015_GuerrasHibridas_JosepBaques.pdf. Pág 5.

nicación (manipular lo que los ciudadanos ven y oyen para liderar la opinión pública)»³³.

Existe, por tanto, un consenso académico en reconocer la antigüedad del concepto de guerra como un fenómeno que va más allá del enfrentamiento físico en un campo de batalla. Como bien señala Pedro Sánchez Herráez, han existido

«una gran cantidad de conflictos en los cuales se han empleado de manera combinada fuerzas y procedimientos regulares e irregulares como medio esencial para alcanzar la victoria; suelen citarse de manera recurrente la Guerra [*sic*] de Independencia de los Estados Unidos, la guerra contra la invasión francesa de España en 1808, la guerra de la China comunista de Mao, la Guerra de Vietnam»³⁴.

Sin embargo, como señala Moisés Naim:

«El poder de las armas no convencionales en una guerra se ha disparado en los últimos años. De hecho, en la actualidad, cuando las naciones Estado van a la guerra, el poder militar abrumador cuenta menos que antes. Las guerras son cada vez más asimétricas, con el enfrentamiento de grandes fuerzas militares contra otras más pequeñas y heterodoxas: rebeldes, movimientos separatistas, grupos insurgentes, milicias. Además, cada vez es más frecuente que las gane el bando con menos poder militar».

Naim hace mención a un estudio hecho en Harvard que señala que, en las guerras asimétricas que estallaron entre 1800 y 1849, el bando más débil (en número de soldados y armamento) alcanzó sus objetivos estratégicos en el 12% de los casos. Sin embargo, en las guerras que estallaron entre 1950 y 1998, el bando más débil prevaleció con más frecuencia, el 55% de las veces. Por diversas razones, el resultado de los conflictos asimétricos actuales tiene más probabilidades de decidirse en función de las estrategias políticas y militares de los bandos que de la pura fuerza militar. Es decir, un ejército moderno y de gran tamaño ya no basta para garantizar que un país pueda alcanzar sus objetivos estratégicos³⁵.

El final del siglo xx y el comienzo del siglo xxi están asistiendo con mayor frecuencia a la reedición de la historia bíblica que cuenta la victoria de David frente a Goliat. Los Estados nación cada vez tienen más dificultades para enfrentarse a enemigos no identificados o camuflados que minan los cimientos

³³ LIAN, Qiao; XIANGSUI, Wang. *Guerra irrestricta*. S.l. 1999. S.p.

³⁴ SÁNCHEZ HERRÁEZ, Pedro. «La Nueva Guerra Híbrida: un somero análisis estratégico» [en línea], en *Instituto Español de Estudios Estratégicos*. S.f. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEEA54-2014_NuevaGuerraHibrida_PSH.pdf. Pág 4.

³⁵ NAÍM, Moisés. *Op. cit.*, p. 23.

de las instituciones públicas en nuevos escenarios de batalla, como la opinión pública, donde la superioridad de fuerza no supone un valor añadido.

En su reflexión sobre los actuales enfrentamientos bélicos, Pankaj Mishra considera que:

«Las guerras convencionales entre Estados empequeñecen ante las guerras entre terroristas y contraterroristas, insurgentes y contrain-surgentes: y hay además guerras económicas, financieras y cibernéticas, guerras por y a través de la información, guerras por el control del comercio y drogas y la emigración, y guerras entre milicias urbanas y grupos mafiosos. Los futuros historiadores acaso vean en semejante caos descoordinado el comienzo de la tercera —y la más larga y más extraña— de todas las guerras mundiales: una guerra que se asemeja, por su ubicuidad, a una guerra civil global»³⁶.

Los exdirectivos de Google Schmidt y Cohen también asumieron en el año 2013 que la guerra y los conflictos violentos utilizarían las nuevas tecnologías para combatir contra los Estados en nuevos campos de batalla. Según estos autores:

«La tecnología es una herramienta que genera igualdad de oportunidades y ofrece recursos muy poderosos para que las personas logren sus objetivos: algunos de ellos muy constructivos, otros de una inimaginable fuerza destructora. La verdad innegable es que la conectividad también beneficia a grupos terroristas, violentos y extremistas. La actividad terrorista del futuro incluirá aspectos físicos y virtuales, desde el reclutamiento a la implementación de actos terroristas»³⁷.

Ya en el año 2005, la Estrategia de Defensa Nacional de Estados Unidos mencionaba una serie de amenazas emergentes e identificaba retos de «carácter irregular». Según este documento, el pensamiento de seguridad estaba transformándose: de ser una «mera lucha de guerra de naciones» hacia una guerra contra «una lista de enemigos más amplia: irregulares, terroristas catastróficos y amenazas disruptivas, que tratan de usurpar y desplazar la hegemonía y el poder americano a través de disrupciones tecnológicas»³⁸.

Sin embargo, tal y como señalan Miguel García Guindo y Gabriel Martínez-Valera, no fue hasta ese año 2005 cuando se acuñó por primera vez la definición contemporánea de *guerra híbrida*. Mattis y Hoffman, en su artículo

³⁶ MISHRA, Pankaj. *Op. cit.*, p. 14.

³⁷ SCHMIDT, Eric; COHEN, Jared. *Op. cit.*, p. 151.

³⁸ HOFFMAN, Frank G. «Hybrid Warfare and Challenges, Joint Forces Quarterly» [en línea], en *Small Wars Journal*, n.º 52. 2009. Disponible en web: <http://smallwarsjournal.com/documents/jfqhoffman.pdf>. HOFFMAN, Frank G. «Conflicts in the 21st Century: The Rise of Hybrid Wars» [en línea], en *Potomac Institute for Policy Studies*. Arlington, Virginia. 2007. P. 13. Disponible en web: http://www.potomac institute.org/images/stories/publications/potomac_hybridwar_0108.pdf

Future Warfare: The Rise of Hybrid Wars, al hablar de los Estados Unidos, advertían de que la superioridad de este último crearía una lógica que impulsaría a los actores estatales y no estatales a abandonar el modo tradicional de hacer la guerra y a buscar una capacidad o algún tipo de combinación de tecnologías y tácticas que les permitiera obtener una ventaja sobre su adversario. Una lógica que no encontraba acomodo en la clasificación de las amenazas emergentes que apareció en la Estrategia Nacional de Defensa de los Estados Unidos publicada en marzo de ese mismo año, y que, como se ha señalado anteriormente, distinguía entre tipos de guerra tradicional, irregular, catastrófica y disruptiva³⁹. Por su parte, Pablo Sánchez Herraiz considera como hito de «nacimiento» de la guerra híbrida el conflicto que en 2006 enfrentó a Israel y Hezbolá, guerra en la cual esta formación islámica no pudo ser derrotada o salió vencedora, según sean las fuentes consultadas frente a las poderosas y bien adiestradas Fuerzas de Defensa Israelíes (FDI)⁴⁰.

Miguel García Guindo y Gabriel Martínez-Valera consideran que el concepto de guerra híbrida, proviene del término *guerra compuesta*, que se le atribuye al historiador Tomas Huber (1996) y que describe el fenómeno de las fuerzas regulares e irregulares que combaten de manera coordinada.

«Huber explica la guerra compuesta a modo de marco intelectual para entender el fenómeno de las fuerzas convencionales, (regulares) y las fuerzas no convencionales (irregulares) que operan bajo dirección unificada a fin de lograr el estado final deseado. El autor analiza la coordinación y la relativa simultaneidad de estas fuerzas que operan de manera cohesionada, pero nunca fusionadas o combinadas, en el campo de batalla»⁴¹.

El militar estadounidense Daniel Lasica señaló en el año 2009 que lo que persiguen (las guerras híbridas) es dominar el arte operacional sin restricciones a base de sobrepasar las fronteras y las leyes cognitivas y morales de la guerra que sustentan el pensamiento de defensa de los países occidentales⁴². Lasica defiende que el actor que recurre a la guerra híbrida saca provecho del concepto de Estados Unidos (asentado en los tratados de Jomeini)

³⁹ GARCÍA GUINDO, Miguel; MARTÍNEZ-VALERA GONZÁLEZ, Gabriel. «La guerra híbrida: nociones preliminares y su repercusión en el planeamiento de los países y organizaciones occidentales» [en línea], en *Instituto Español de Estudios Estratégicos*. 15 febrero 2015. P. 4. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_trabajo/2015/DIEET02-2015_La_Guerra_Hibrida_GUindo_Mtz_Glez.pdf.

⁴⁰ SÁNCHEZ HERRÁEZ, Pedro. «La Nueva Guerra Híbrida: un somero análisis estratégico» [en línea], en *Instituto Español de Estudios Estratégicos*. 2014. P. 3. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_analisis/2014/DIEEA54-2014_NuevaGuerraHibrida_PSH.pdf.

⁴¹ GARCÍA GUINDO, Miguel; MARTÍNEZ-VALERA GONZÁLEZ, Gabriel. *Op. cit.*, S.p.

⁴² LASICA, Daniel (2009). *Strategic Implications of Hybrid War: A Teory of Victory*. Fort Leavenworth, Kansas School of Advanced Military Studies, United States Army Command and General Staf College.

sobre una teoría estratégica de victoria basada en la derrota de la voluntad de lucha del adversario, lo que no ha sucedido en las últimas guerras de Irak y Afganistán ni en los conflictos de Hizb Allah (2006) y Hamás (2009 y 2013), estas dos últimas contra las Fuerzas de Defensa Israelíes (IDF, en sus siglas en inglés)⁴³.

La OTAN, en la declaración emitida tras la cumbre de Cardiff (Gales, 4-5 de septiembre de 2014) menciona expresamente el término *amenazas de guerras híbridas* y *amenazas híbridas* en diferentes epígrafes. En dicho documento se expresa la necesidad de poder hacer frente a este tipo de retos, para lo cual, se señala, la Alianza necesita poseer las herramientas y procedimientos necesarios para disuadir y responder de manera efectiva a estas amenazas, así como las capacidades para reforzar a las fuerzas de cada nación⁴⁴.

La OTAN también incide en la importancia de desestabilizar de las guerras híbridas:

«Los conflictos híbridos incluyen movilizar recursos en múltiples sectores para desestabilizar el funcionamiento de un estado [*sic*] y polarizar su sociedad. A diferencia de la guerra convencional, el “centro de gravedad” en la guerra híbrida es una población objetivo. El adversario trata de influenciar a los responsables políticos influyentes y a los principales responsables de la toma de decisiones. El agresor a menudo recurre a acciones clandestinas, para evitar la atribución o la retribución. Sin dejar el rastro de una pistola humeante»⁴⁵.

Países como España ya han reconocido oficialmente la amenaza para la seguridad que supone este nuevo tipo de guerras. La Estrategia de Seguridad Nacional elaborada por el Gobierno de España en el año 2017 incluye de manera explícita la amenaza de acciones híbridas como uno de los principales retos de seguridad a los que debe de hacer frente el país. Este documento define las *acciones híbridas* de la siguiente manera:

«Se trata de acciones combinadas que pueden incluir, junto al uso de métodos militares tradicionales, ciberataques, operaciones de manipulación de la información, o elementos de presión económica, que se han manifestado especialmente en procesos electorales. La finalidad últi-

⁴³ Ibidem.

⁴⁴ NATO (OTAN), «Wales Summit Declaration, Press Release (2014) 120» [en línea]. 5 septiembre 2014. Párrafos 13 y 104. Disponible en web: http://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=en.

⁴⁵ PINDJAK, Peter. «Deterring hybrid warfare: a chance for NATO and the EU to work together?» [en línea], en OTAN. 2014. Disponible en web: <https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/EN/index.htm>.

ma que se persigue es la desestabilización, el fomento de movimientos subversivos y la polarización de la opinión pública»⁴⁶.

La definición del Gobierno de España reconoce también que este tipo de amenaza puede venir tanto por parte de «agentes estatales» como «no estatales», y que combinan el empleo de «medios militares con ataques cibernéticos, elementos de presión económica o campañas de influencia en las redes sociales»⁴⁷. La Estrategia de Seguridad Nacional de España sitúa el origen de estas nuevas amenazas en el complejo contexto sociopolítico y económico que se define en el primer capítulo de este trabajo. El Gobierno de España considera que:

«Ligado en gran medida a la situación de crisis económica de estos años, el auge de grupos con visiones proteccionistas [sic] y nacionalistas exclusivistas es una de las notas dominantes en este periodo. Este fenómeno se ha aprovechado de factores de fondo como la desaceleración del crecimiento económico, la desigualdad o la polarización social e identitaria, y ha adquirido una mayor relevancia internacional y estratégica. La influencia de movimientos exclusivistas crece por el uso masivo de las redes sociales. Asimismo, la manipulación de la información por parte de agentes externos ejerce de factor de influencia en la era de la *posverdad*, con efectos negativos en la cohesión social y la estabilidad política»⁴⁸.

Miguel García Guindo y Gabriel Martínez-Valera González también subrayan que el uso (o el mal uso) de la comunicación se está consolidando como una de las principales armas en el contexto de las guerras híbridas. Estos autores consideran que los actores de guerra híbrida

«explotan hábilmente las limitaciones impuestas a las fuerzas de las grandes potencias occidentales. Entre estas se incluyen las reglas de enfrentamiento, la voluntad política, la cobertura del conflicto por los medios de comunicación, las tradiciones militares, las normas de la guerra, así como los límites cognitivos y geográficos»⁴⁹.

García Guindo y Martínez-Valera González destacan también el creciente papel de

«los esfuerzos de propaganda destinados tanto a la población local, a la del adversario, como a la Comunidad Internacional [sic] [...] Este tipo de esfuerzos deben socavar la legitimidad del oponente para ejecutar las operaciones militares, modelan la agenda interna e internacional,

⁴⁶ GOBIERNO DE ESPAÑA. *Op. cit.*, p. 16.

⁴⁷ GOBIERNO DE ESPAÑA. *Op. cit.*, p. 32.

⁴⁸ GOBIERNO DE ESPAÑA. *Op. cit.*, p. 34.

⁴⁹ GARCÍA GUINDO, Miguel; MARTÍNEZ-VALERA GONZÁLEZ, Gabriel. *Op. cit.*, s.p.

presentan un marco interpretativo alternativo de referencia y, sobre todo, minan la fortaleza pública del contrario»⁵⁰.

Como se explicará en las siguientes páginas, el uso de la comunicación como elemento de disrupción en un contexto de guerras híbridas es un proceso complejo que requiere implementar una metodología determinada. Uno de los principales elementos para irrumpir de manera eficaz a través de la comunicación es la creación de relatos o narrativas. Félix Arteaga destacó en el año 2010 la importancia de la guerra de relatos y narrativas en el nuevo contexto bélico a la hora de modular la audiencia doméstica o global. Según Arteaga, la clave del enfrentamiento «está en la percepción». Por ello:

«Las partes enfrentadas han tenido que adaptar su estrategia militar a la batalla de las ideas buscando los “relatos”, las narraciones del conflicto que les favorezcan. Lo que ocurre en el enfrentamiento armado es importante, pero lo es mucho más la habilidad que se tiene para narrarlo. La batalla entre narraciones tiene un frente local, donde la acción armada debe ganarse el favor de la población y, sobre todo, evitar que perciba al bando contrario como ganador. Esa misma batalla se libra también en la retaguardia, donde las opiniones públicas alejadas geográficamente de la realidad del conflicto siguen el enfrentamiento a través de las narraciones gubernamentales, mediáticas o insurgentes. La percepción cuenta más que la realidad y el nuevo centro de gravedad consiste en generar una percepción tan desfavorable del contrario que desmovilice su voluntad de prevalecer y la confianza de quienes lo apoyaban»⁵¹.

Las guerras híbridas de agentes nacionales

Como se ha señalado anteriormente, la amenaza de las guerras híbridas puede provenir por parte de agentes estatales y por parte de agentes no estatales. La Estrategia de Seguridad Nacional de España menciona de forma explícita dos países especialmente activos en reconfigurar el escenario internacional. Este informe considera que está creciendo «la competición entre actores estatales, con distintas visiones sobre la seguridad y sobre el papel de las instituciones multilaterales. Potencias como China y Rusia han adoptado un papel más activo en el escenario internacional y proyectan su poder más allá de su entorno regional»⁵².

⁵⁰ Ibídem.

⁵¹ ARTEAGA, Félix. «Terrorismo, contrainsurgencia y opinión pública», en JORDÁN, Javier; Pozo, Pilar; G. GUINDO, Miguel (coords.) *Terrorismo sin fronteras: actores, escenarios y respuestas en un mundo global*. Navarra: Editorial Aranzadi. 2010. pp. 213-230.

⁵² GOBIERNO DE ESPAÑA. *Op. cit.*, p. 31.

Rusia ha sido uno de los países que más ha desarrollado el concepto de guerras híbridas o, en palabras, de la doctrina militar rusa, «guerras no declaradas» y «guerras no lineales». En febrero de 2013 el general Valery Gerasimov, jefe del Estado Mayor de las Fuerzas Armadas de la Federación Rusa, publicó un artículo en la revista *Military Industrial Kurier* en el que describía una nueva forma de entender la guerra y la paz en el siglo XXI. Según este militar ruso, «las guerras ya no se van a declarar y, una vez comenzadas, seguirán procedimientos no familiares»⁵³.

Según este general ruso, impulsor de la denominada *doctrina Gerasimov*, un Estado próspero puede «en cuestión de meses e incluso días, transformarse en una zona de terrible conflicto armado; sufrir una intervención extranjera y hundirse en una red de caos, catástrofes humanitarias y guerra civil». Gerasimov, que basa su reflexión en el estudio de las Primaveras Árabes, considera que:

«El papel de los medios no militares para lograr objetivos políticos y estratégicos ha crecido y, en muchos casos, han excedido el poder de la fuerza de las armas en su eficacia. Los métodos más utilizados en un conflicto están cada vez más relacionados con el uso de la información política y económica, las medidas humanitarias y otras medidas no militares, aplicadas de manera coordinada con protesta ciudadanas [*sic*]. Todo esto se complementa con medios militares de carácter oculto, que incluyen el uso de acciones informativas y las acciones de las fuerzas de operaciones especiales»⁵⁴.

Can Kasapoglu, investigador del Colegio de Defensa de la OTAN, explica en un artículo publicado en noviembre de 2015 que nuestra estrategia de «guerras híbridas» o «guerras no lineales de Rusia» comenzó a tomar forma tras los «catastróficos resultados de la primera guerra ruso-chechena entre 1994 y 1996»⁵⁵. Kasapoglu considera que las nuevas técnicas de guerra híbrida de Rusia comenzaron a aplicarse en 2008 con la guerra entre Rusia y Georgia, pero cobraron especial relevancia en la guerra de Ucrania y durante la anexión de la península de Crimea en marzo de 2014⁵⁶.

⁵³ COALSON, Robert. «Top Russian General Lays Bare Putin's Plan for Ukraine» [en línea], en *Huffington Post*. S.f. Disponible en web: https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

⁵⁴ COALSON, Robert. «Top Russian General Lays Bare Putin's Plan for Ukraine» [en línea], en *Huffington Post*. S.f. Disponible en web: https://www.huffingtonpost.com/robert-coalson/valery-gerasimov-putin-ukraine_b_5748480.html.

⁵⁵ KASAPOGLU, Can. «Russia's Renewed Military Thinking: Non-Linear Warfare and Reflexive Control» [en línea], en *Research Division. NATO Defense College*. Rome. N.º 121. Noviembre 2015. Disponible en web: <http://cco.ndu.edu/Portals/96/Documents/Articles/russia%27s%20renewed%20Military%20Thinking.pdf>.

⁵⁶ *Ibidem*.

En su reflexión sobre estos nuevos métodos bélicos, Kasapoglu recuerda que las guerras informativas y psicológicas que Rusia utilizó durante su campaña híbrida en Ucrania en 2014 no eran del todo nuevas, y recuperan la teoría soviética del control reflexivo. La *teoría de control reflexivo* se define como un medio de transmitir a un adversario información previamente preparada para inclinarlo a tomar voluntariamente una decisión predeterminada deseada por el iniciador de la acción⁵⁷. Es decir, consistiría en hacer llegar al adversario informaciones manipuladas o descontextualizadas que fuercen a que este adversario tome de manera voluntaria decisiones en contra de sus propios intereses.

Timothy L. Thomas explica que el concepto de control reflexivo ha existido «mucho más tiempo que los conceptos de guerra de información y operaciones de información». Según este autor, este concepto se desarrolló en la literatura militar soviética en los años setenta. En ese momento, V. A. Lefebvre, que estaba trabajando dentro del contexto y la lógica de un juego reflexivo, definió el control reflexivo como «un proceso por el cual un enemigo transmite a su oponente las razones o bases para tomar de manera voluntaria decisiones equivocadas»⁵⁸.

Según un informe del Real Instituto Elcano, el concepto de control reflexivo está enfocado en Rusia en la actualidad «a influenciar en aspectos como la filosofía, sociología, psicología, pedagogía, *inteligencia artificial*, computación, asuntos militares, inteligencia, contrainteligencia y muchas otras áreas»⁵⁹.

«La estrategia rusa de control de la información pasa por estar más interesada en los aspectos cognitivos, cuyo objetivo es localizar el eslabón más débil y explotarlo. Son usadas operaciones de desacreditación moral y psicológica (PSYOPS), usando o manipulando datos biográficos, hábitos, deficiencias psicológicas, etc.»⁶⁰.

El Centro de Excelencia de Comunicaciones Estratégicas de la OTAN reconoce en un informe elaborado en el año 2014 que Rusia «ha demostrado su voluntad de modernizar las herramientas de la era soviética y adaptarlas al complejo entorno informativo actual»⁶¹. Este informe de la OTAN considera

⁵⁷ THOMAS, Timothy L. «Russia's Reflexive Control Theory and the Military» [en línea], en *Journal of Slavic Military Studies*. N.º 17. 2004. P. 237-256. Disponible en web: https://www.rif.edu/~w-cmmc/literature/Thomas_2004.pdf.

⁵⁸ *Ibidem*.

⁵⁹ REAL INSTITUTO ELCANO [en línea], en *Ciber Elcano* n.º 10. Enero 2016. Disponible en web: http://www.realinstitutoelcano.org/wps/wcm/connect/d26694804b495a16a1e0e-3c12a87c07d/Ciber_Elcano_Num10.pdf?MOD=AJPERES&CACHEID=1452614978930.

⁶⁰ *Ibidem*.

⁶¹ NATO. «Analysis of Russia's Information Campaign Against Ukraine. Examining non-military aspects of the crisis in Ukraine from a strategic communications perspective» [en línea], en *Strategic Communications Centre of Excellence*. 2014. Disponible en web: <https://www.stratcomcoe.org/analysis-russias-information-campaign-against-ukraine>.

que la campaña de información y comunicación «fue central para las operaciones de Rusia en Ucrania». Según la OTAN:

«La campaña informativa y de acción militar desarrollada por Rusia corresponde a las características de una nueva forma de guerra donde las líneas entre paz y guerra, fuerza militar extranjera y grupos locales de autodefensa son borrosas y el espacio principal de batalla se ha movido desde el terreno físico a la guerra por las mentes y los corazones de las poblaciones en disputa».

La OTAN concluye que Crimea «puede considerarse un campo de entrenamiento para Rusia para testear esta nueva forma de guerra híbrida y asimétrica, que combina una campaña intensiva de información, la guerra cibernética y el uso de fuerzas especiales»⁶².

El mayor estadounidense John R. Davis reconocía en un artículo publicado en una revista de la OTAN que las acciones híbridas de Rusia en 2014 en Ucrania pillaron a la OTAN y al mundo «por sorpresa»⁶³. Este militar estadounidense considera que uno de los principales éxitos de Rusia en su campaña en Ucrania fue «el uso de operaciones de información y psicológicas orientadas a apoyar la causa rebelde, incitar a la violencia y movilizar a sus audiencias cuando fuera necesario»⁶⁴. Al mismo tiempo, esta estrategia estaba encaminada a atemorizar, intimidar y provocar la inacción de las audiencias enemigas. John R. Davis presta especial atención al sofisticado proceso de elaboración de narrativas que implementó Rusia en su campaña de información. Según Davis, los medios rusos emplearon diferentes estrategias narrativas para diferentes audiencias: «Una narrativa estaba encaminada a lograr un apoyo internacional a los intentos rusos por lograr una solución pacífica a la crisis en Ucrania. Otra narrativa estaba encaminada a las audiencias internas y pro rusas [*sic*] de Ucrania, donde se promovía el nacionalismo y el victimismo»⁶⁵.

Las técnicas informativas de Rusia en el contexto de las guerras híbridas no han dejado de sucederse en diferentes puntos del mundo desde el año 2014. En el año 2016, un informe financiado por la oficina del primer ministro de Finlandia advertía de las campañas de información provenientes de Rusia para desestabilizar los Estados Bálticos. Este estudio, elaborado por Bettina Renz y Hanna Smith, considera que «los principales medios que Rusia adoptará para crear inestabilidad y socavar la moral en un estado [*sic*] adversario estarán relacionados con la guerra de la información». Los autores

⁶² Ibídem.

⁶³ DAVIS JR., John R. «Continued Evolution of Hybrid Threats» [en línea], en *The Three Swords Magazine. Joint Warfare Centre. NATO*. 2015. S.p. Disponible en web: http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf.

⁶⁴ Ibídem.

⁶⁵ Ibídem.

consideran que las campañas de información rusas en los Estados Bálticos se enfocan en la difusión de falsedades, en socavar la moral creando divisiones entre las diferentes agrupaciones étnicas, lingüísticas y políticas dentro de estos estados o mediante una insatisfacción general con el gobierno. El informe cita expresamente unas declaraciones del general ruso Valery Gerasimov que reconoce que «el objetivo es hacer uso de la oposición interna del adversario como un frente de lucha permanente»⁶⁶.

Este informe hace una especial mención a la estrategia de los medios rusos para aprovecharse a su favor de los regímenes liberales y de respeto a la libertad de expresión que impera en los Estados Bálticos. Renz y Smith consideran que la guerra de información rusa «hace uso para sus propios fines de la presencia de libertad de expresión en los estados *[sic]* democráticos». Esta situación provoca que «los Estados bálticos quedan en una situación de indefensión ante la producción de propaganda de Moscú, que está diseñada para dividir sus estados *[sic]*». El informe, en este sentido, cita a Pomerantsev y Weiss cuando denunciaron que «el Kremlin ha aprendido sistemáticamente a utilizar los principios de las democracias liberales contra ellas». Renz y Smith concluyen que las guerras asimétricas «están consiguiendo que los propios sistemas democráticos se están convirtiendo en una vulnerabilidad contra ellos mismos por culpa de las acciones rusas»⁶⁷.

Existen abundantes indicios para sospechar que las tácticas de guerras híbridas implementadas por Rusia en Ucrania o en los Estados Bálticos no han sido una excepción. Desde el año 2014 hasta la actualidad, diversos investigadores e instituciones han denunciado y demostrado el uso de prácticas informativas desestabilizadoras por parte de agentes rusos en diversos países de Europa y de América. Los investigadores Edward Lucas y Peter Pomerantsev aseguran, en un estudio publicado en agosto de 2016, y consideran que el uso por parte de Rusia de la información como arma no es nuevo, «pero la sofisticación y la intensidad están aumentando»⁶⁸. Según estos autores: «Occidente comenzó a darse cuenta de que la desinformación representa una seria amenaza para Estados Unidos y sus aliados europeos, principalmente los “estados *[sic]* de primera línea” —Polonia, los Estados bálticos, la República Checa, Eslovaquia y Ucrania—, pero también para Europa occidental y Norteamérica». Lucas y Pomerantsev aseguran que:

⁶⁶ RENZ, Bettina; SMITH, Hanna. «Russia and Hybrid Warfare. Going Beyond the Label» [en línea], en *Papers Aleksanteri*. Enero 2016. S.p. Disponible en web: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=0ahUKEw-j0k_CHh9bYAhUic98KHWNJBgYg2MAI&url=https%3A%2F%2Fwww.stratcomcoe.org%2Fdownload%2Ffile%2Ffid%2F4920&usg=AOvVaw2HUcl2dQ3JTA8CEjs1yQaT.

⁶⁷ Ibidem.

⁶⁸ LUCAS, Edward; POMERANZEV, Peter. «Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe» [en línea], en *Center for European Policy Analysis*. Agosto 2016. S.p. Disponible en web: <http://cepa.org/reports/winning-the-information-war>.

«En todo el mundo occidental, el Kremlin promueve el discurso conspirativo y utiliza la desinformación para contaminar el espacio de información, aumentar la polarización y socavar el debate democrático. Las acciones de Rusia aceleran la disminución de la confianza en las alianzas y organizaciones internacionales, instituciones públicas y medios de comunicación»⁶⁹.

Lucas y Pomerantsev coinciden con Renz y Smith en considerar que el principal objetivo de estas campañas de guerra de comunicación es el de aumentar las tensiones internas de los países que son objetivos de estos ataques:

«A diferencia de la propaganda soviética, los métodos contemporáneos de guerra de información de Rusia no promueven la agenda del Kremlin. En cambio, están calibrados para confundir, desconcertar y distraer. Rusia trata de erosionar el apoyo público a los valores euroatlánticos para aumentar su propio poder relativo. Explota las tensiones étnicas, lingüísticas, regionales, sociales e históricas, y promueve las causas antisistema, extendiendo su alcance y dándoles una falsa apariencia de legitimidad»⁷⁰.

Un claro ejemplo de esta táctica de erosión de los valores europeos se pudo constatar en la precampaña italiana, donde, según una información publicada por Bloomberg, el medio de comunicación ruso Sputnik fue uno de los principales responsables de fomentar el discurso antinmigratorio en Italia⁷¹.

Siguiendo la teoría soviética del control reflexivo, las nuevas guerras de comunicación de Rusia en el contexto de las guerras híbridas estarían destinadas a proveer a la opinión pública de los países adversarios de informaciones falsas, confusas o descontextualizadas con el objetivo de que los ciudadanos tomen de forma voluntaria las peores decisiones para sus propios intereses y los intereses de sus países.

Confundir y desestabilizar a la opinión pública estadounidense parece que fue el objetivo de la estrategia de disrupción rusa en la campaña electoral estadounidense de 2016. Según se desprende de la investigación que hizo pública el pasado 16 de febrero el Departamento de Justicia de Estados Unidos, trece ciudadanos rusos y tres compañías del mismo país fueron oficialmente acusadas de poner en marcha una sofisticada red de información diseñada para alterar las elecciones estadounidenses de 2016 y favorecer al candidato Donald Trump. Según indica el informe del Departamento de Justicia, en el conocido como *informe Mueller*, la campaña comenzaba desde unas oficinas en San Petersburgo en Rusia, se distribuía en redes sociales americanas y, en última instancia, in-

⁶⁹ Ibídem.

⁷⁰ Ibídem.

⁷¹ BLOOMBERG. «Russia Helped Shape Italy's Twitter Obsession With Immigrants» [en línea]. 1 marzo 2018. Disponible en web: <https://www.bloomberg.com/news/articles/2018-03-01/russia-helped-shape-italy-s-twitter-obsession-with-immigrants>.

fluenciaba en los estados clave de las elecciones presidenciales. La investigación también señala que la maquinaria rusa robó identidades de ciudadanos estadounidenses y agitó debates sociales controvertidos como la inmigración, el debate racial o la religión con el objetivo de dividir a la población estadounidense. Según indicó Rod J. Rosenstein, el fiscal general que ha llevado el proceso, «las pruebas confirman que conspiradores rusos quieren promover la discordia en Estados Unidos y minar la confianza pública en la democracia»⁷².

La revista *The Economist* publicaba el 24 de febrero de 2018 un extenso análisis de la guerra informativa rusa a raíz del denominado *informe Mueller*; coincidía en el análisis hecho público por los investigadores estadounidenses y señalaba que los objetivos de estas campañas de guerra de comunicación tienen un objetivo a largo plazo que consiste en debilitar las democracias occidentales, deteriorando la confianza de los ciudadanos en sus instituciones y dividiendo y enfrentando a la población. *The Economist* señala directamente a los medios de comunicación rusos como RT y Sputnik de servir de plataformas para difundir la desinformación. Así mismo, apunta a instituciones rusas como el IRA (Agencia para la Investigación de Internet) de poner en marcha herramientas automatizadas (bots) para la difusión de mensajes de manera masiva en redes sociales. El artículo de *The Economist* cita un informe de noviembre de 2017 del Centro Stratcom de la OTAN donde señala que el 70% de los mensajes en lengua rusa sobre la OTAN en los Estados Bálticos está generado por bots. Asimismo, hace referencia a un estudio realizado por la consultora 89Up durante la campaña del Brexit en Reino Unido en 2016 que indica que los mensajes distribuidos por los bots rusos durante este proceso electoral tuvieron una audiencia potencial de diez millones de perfiles digitales⁷³.

Las guerras de comunicación puestas en marcha por Rusia en el contexto de los conflictos híbridos no parece que hayan llegado a su fin. Al contrario, la evidencia demuestra que estas técnicas se encuentran en su momento más álgido. Los portavoces del Comité de Inteligencia del Senado de Estados Unidos advirtieron el 4 de octubre de 2017 que las operaciones desinformativas rusas «seguirán activas y determinadas a sembrar el caos en diversos procesos electorales durante los próximos meses y años»⁷⁴.

⁷² APUZZO, Mat; LAFRANIERE, Sharon. «13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign» [en línea], en *The New York Times*. 16 febrero 2018. Disponible en web: https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html?rref=collection%2Fnewseventcollection%2Frussian-election-hacking&action=click&contentCollection=politics®ion=stream&module=stream_unit&version=latest&contentPlacement=54&Págtype=collection.

⁷³ THE ECONOMIST. «The discord amplifier» [en línea]. 24 febrero 2018. Disponible en web: <https://www.economist.com/news/briefing/21737297-mueller-indictment-reveals-some-kremlins-tactics-russian-disinformation-distorts>.

⁷⁴ FANDOS, Nicholas. «Senate Intelligence Heads Warn That Russian Election Meddling Continues» [en línea], en *The New York Times*. 4 octubre 2017. Disponible en web: <https://www.nytimes.com/2017/10/04/us/politics/senate-intelligence-committee-russia-election-trump.html>.

La creciente actividad desestabilizadora rusa utilizando medios informativos quedó también patente el 10 de enero de 2018 con la publicación de un informe del Senado de Estados Unidos donde se constataban de manera probada casos de injerencias en Ucrania, Georgia, Montenegro, Serbia, Bulgaria, Hungría, Letonia, Lituania, Estonia, Dinamarca, Finlandia, Noruega, Suecia, Holanda, Reino Unido, Francia, Alemania, España e Italia⁷⁵.

Las guerras híbridas de agentes no nacionales

El fenómeno de las guerras híbridas no está vinculado en la actualidad exclusivamente a enfrentamientos entre naciones Estado: grupos de carácter subnacional han comenzado a implementar con éxito campañas híbridas contra Estados con el objetivo de erosionar sus instituciones y causar la máxima desestabilización. Estas amenazas híbridas provenientes de agentes no estatales también incluyen acciones de disrupción digital y comunicativa. La Estrategia de Seguridad Nacional del Gobierno de España considera que:

«Además de la difusión de poder a nivel estatal, se observa, gracias a la tecnología y a la creciente conectividad, una importante traslación de poder hacia actores no estatales. Individuos y grupos emergen como actores relevantes, que ganan influencia y mutan el orden tradicional de Estados. Así, una de las tendencias notables es la frecuencia con que el terrorismo yihadista ha golpeado en los últimos años en varias regiones, incluyendo Europa»⁷⁶.

El caso del Dáesh es un ejemplo nítido de cómo un grupo no estatal, mediante una guerra de carácter híbrido, puede lograr desestabilizar decenas de países en distintos continentes mediante la aplicación de campañas bélicas sobre el terreno, acciones violentas irregulares (terrorismo), acciones de cibercrimen y campañas de disrupción comunicativa.

La revista Atlantic, en un artículo de noviembre de 2016, ya consideró al grupo terrorista Estado Islámico como un fenómeno exitoso de disrupción digital:

«Durante mucho tiempo se ha celebrado el poder de Internet para unir a las personas. Sin embargo, resulta que esta misma tecnología está siendo convertida en un arma de guerra. Los teléfonos inteligentes y las redes sociales han alterado claramente las reglas del conflicto violento, desde el reclutamiento hasta las crónicas en el campo de batalla. Pero los mayores efectos de esta tecnología pueden ser aún más

⁷⁵ COMMITTEE ON FOREIGN RELATIONS UNITED STATES SENATE. «Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security» [en línea]. 10 enero 2018. Disponible en web: <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>.

⁷⁶ GOBIERNO DE ESPAÑA. *Op. cit.*, p. 31.

importantes, y contribuyan *[sic]* expandir las causas y la incidencia de la guerra, así como su alcance. Las plataformas de los medios sociales refuerzan las narrativas de “nosotros contra ellos”, exponen a las personas vulnerables a ideologías violentas e inflaman los odios largamente latentes. Crean oleadas masivas de opinión popular que son casi imposibles de predecir o controlar»⁷⁷.

Scott Jasper y Scott Moreland también incluyeron en diciembre de 2014 a Estado Islámico como un ejemplo de «amenaza híbrida» y destaca entre las estrategias de este grupo terrorista su uso de la «propaganda y las guerras de información»⁷⁸. En septiembre de 2014, el presidente de los Estados Unidos, Barack Obama, apoyó esta terminología cuando advirtió que el Estado Islámico representaba un nuevo tipo de desafío: una especie de híbrido no solo de la red terrorista, sino de las ambiciones territoriales y algunas estrategias y tácticas de un ejército⁷⁹.

El Comité de Servicios Armados de la Cámara de Representantes de Estados Unidos incluyó al Dáesh como un ejemplo de guerra híbrida, dentro de otros ejemplos clásicos citados con frecuencia:

«La guerra entre Israel y Hezbollah en el verano de 2006, la evolución de ISIS [Estado Islámico de Irak y Siria] en los últimos algunos *[sic]* años, con encriptación, drones, capacidades de precisión y continuo derramamiento de sangre en el este de Ucrania, sugieren que nuestro pronóstico de amenazas híbridas en el medio del espectro del conflicto, un anuncio violento híbrido, no estaba muy lejos. Quizá imperfecto, pero no muy lejos la predicción»⁸⁰.

La metodología de la disrupción comunicativa

La disrupción digital y comunicativa se ha consolidado como una eficaz arma de guerra que es necesario definir e identificar como una disciplina diferente

⁷⁷ EMERSON T. BROOKING; P.W. SINGER. «War Goes Viral. How social media is being weaponized across the world» [en línea], en *The Atlantic*. Noviembre 2016. Disponible en web: <https://www.theatlantic.com/magazine/archive/2016/11/war-goes-viral/501125/>.

⁷⁸ JASPER, Scott; MORELAND, Scott. «The Islamic State is a Hybrid Threat: Why Does That Matter?» [en línea], en *Small Wars Journal*. 1 diciembre 2014. Disponible en web: <http://smallwarsjournal.com/jrnl/art/the-islamic-state-is-a-hybrid-threat-why-does-that-matter>.

⁷⁹ OBAMA, Barack H. (President of the United States). «President Obama: What Makes Us America» [en línea]. 60 Minutes interview with Steve Croft at the White House, en *Central Broadcasting Network (CBS)*. Washington DC. 28 septiembre 2014. Disponible en web: <http://www.cbsnews.com/news/president-obama-60-minutes/>.

⁸⁰ House of Representatives. Committee on Armed Services. One Hundred Fifteenth Congress. First Session. «The Evolution of Hybrid Warfare and Key Challenges». 22 marzo 2017. Disponible en web: <https://www.gpo.gov/fdsys/pkg/CHRG-115hhrg25088/pdf/CHRG-115hhrg25088.pdf>.

a las ofensivas y ataques cibernéticos. Los ataques cibernéticos contra infraestructuras o intereses estratégicos de un Estado también son acciones propias de una guerra híbrida, pero sus metodologías, objetivos y consecuencias son distintos a las acciones de disrupción digital y comunicativa.

Las instituciones públicas y empresas cuentan en la actualidad con múltiples recursos para responder con rapidez y eficacia ante un ataque contra sus sistemas digitales. Tal y como se demostró con el ciberataque provocado por el virus Wannacry en mayo de 2017, los Estados, las empresas y los ciudadanos de los países afectados tardaron minutos, incluso segundos en recuperar su normal funcionamiento. A pesar de la magnitud del ataque, las consecuencias quedaron reducidas a pérdidas financieras que fueron asimiladas con relativa facilidad por las partes afectadas.

Las acciones de disrupción digital y comunicativa, por el contrario, tienen como objetivo alterar a largo plazo la convivencia y las relaciones entre los ciudadanos y las instituciones públicas de un Estado, así como romper el contrato social que sostiene un Estado de derecho. Las consecuencias políticas, sociales y económicas pueden ser de gran magnitud y sus efectos durar durante generaciones.

Las acciones de hackeo de la opinión pública mediante ataques de disrupción digital y comunicativa siguen un patrón constante, tanto en acciones ofensivas por parte de Estados nación como por parte de grupos subnacionales no estatales como el Dáesh. Esta metodología está asentada sobre cuatro pilares que incluyen la combinación de diversas disciplinas, como la sociología, la política, la literatura, el periodismo y la tecnología. Los cuatro pasos que se requieren para implementar una exitosa campaña de disrupción digital y comunicativa para desestabilizar la opinión pública de una nación Estado son los siguientes:

a) Análisis y detección de vulnerabilidades sociales y políticas de un país

La disrupción comunicativa, tal y como se ha demostrado en los diversos casos probados de guerra híbrida por parte de Rusia, está basada en explotar las debilidades internas de un país. El hackeo de la opinión pública no consiste en comenzar nuevos frentes o incendios en la política interna de un país considerado como adversario. La estrategia está enfocada en arrojar combustible y retroalimentar debates y confrontaciones políticas que polarizan una sociedad. En el caso de Estados Unidos, la supuesta disrupción comunicativa generada por Rusia alimentó debates políticos y sociales previos ya existentes. Por su parte, el grupo terrorista Dáesh realizó un profundo análisis social y político de las comunidades suníes de Irak y Siria con el objetivo de detectar y explotar las principales vulnerabilidades de estos Estados y proponer una narrativa encaminada a generar un nuevo contrato social con los ciudadanos suníes de estos países.

b) Creación de narrativas transmedia

Una vez detectadas las principales vulnerabilidades de un sistema político, los responsables de la acción disruptiva crean unos guiones y unas narrativas eficaces y transmedia capaces de generar una resonancia cultural y una movilización entre sus audiencias potenciales. Estas narrativas están pensadas para ser distribuidas a través de diferentes formatos y diferentes personajes y se adaptan a las particularidades culturales y estéticas de las audiencias a las que van dirigidas.

c) Creación de una red de medios propios

La distribución de contenidos del *marketing* digital se asienta desde la primera década del siglo *xxi* en una triple estrategia llamada «medios propios, medios pagados y medios ganados». Existe un consenso generalizado en el sector de la comunicación al aceptar que la combinación de estos tres elementos es la base para la difusión eficaz de los contenidos de una campaña de *marketing*.

d) Los medios propios hacen referencia a las plataformas y canales de comunicación que una marca o un producto crea para comunicarse de manera directa con sus audiencias; los medios pagados hacen referencia a los anuncios y espacios pagados que la marca inserta en canales de comunicación ajenos, y los medios ganados hacen referencia a las informaciones, comentarios o comunicaciones no pagadas que agentes usuarios y agentes influyentes realizan sobre la marca.

e) Las narrativas construidas para canalizar y retroalimentar los conflictos socioeconómicos y políticos de un Estado nación son introducidas en el debate digital a través de una red de medios propios controlados jerárquicamente por los responsables de la disrupción. Los fenómenos de disrupción digital y comunicativa están vinculados con la pérdida de influencia y de credibilidad de los medios de comunicación tradicionales en todas partes del mundo. Esta pérdida de influencia se ha producido por dos motivos. El primero de ellos está ligado a la crisis económica y social que sacudió a gran parte de los países europeos, americanos y de Oriente Medio en el año 2008 y que erosionó la confianza que los ciudadanos tenían hacia los actores tradicionales de comunicación: agentes políticos y medios de comunicación. Por otro lado, la revolución tecnológica que se produjo en las mismas fechas permitió a nuevos agentes de comunicación comunicar y hacer llegar sus mensajes a sus audiencias potenciales sin tener que pasar por el papel mediador de los medios de comunicación tradicionales. De esta manera, agentes disruptores estatales y no estatales han creado en los últimos años diversas plataformas y grupos de comunicación propios que, en el actual y caótico panorama de conformación de la opinión pública, compiten casi en igual-

dad de condiciones con medios de comunicación tradicionales con decenas de años de prestigio y excelencia. Un caso paradigmático de estas redes de plataformas de medios propios vinculados a un Estado son los entramados mediáticos rusos RT, Ruptly y Sputnik. En el caso de grupos no estatales como el Dáesh, la estrategia se ha repetido con la misma lógica: este grupo terrorista ha difundido sus narrativas a través de una red de medios propios en diversas plataformas y formatos.

f) Creación de canales de distribución automatizados

El último paso de la disrupción es la distribución directa, automatizada y segmentada de las narrativas a las audiencias potenciales en entornos digitales. Para ello, los responsables de la acción comunicativa cuentan con estrategias en redes sociales de cuentas automatizadas (bots) que difunden con gran magnitud y segmentación los mensajes, sin esperar a que el usuario llegue de manera voluntaria a la plataforma donde está publicado el contenido. Se ha demostrado la existencia de estas herramientas automatizadas de distribución en casos de injerencias de actores estatales⁸¹, así como de actores no estatales⁸².

La disrupción comunicativa del Dáesh

El caso del grupo terrorista Estado Islámico es un perfecto ejemplo, un caso de disrupción digital y comunicativa en el contexto de una guerra híbrida de un agente no estatal contra diversas naciones Estado. El Dáesh implementa con claridad y eficacia los cuatro elementos que son necesarios para ejecutar con eficacia una campaña de disrupción digital. La estrategia de disrupción comunicativa del califato tiene elementos y metodologías coincidentes con estrategias similares puestas en marcha por grupos estatales. De hecho, una de las principales conclusiones del análisis de la estrategia de comunicación del Dáesh desde el año 2014 hasta el año 2018 es que gran parte de su narrativa está pensada para destruir el contrato social en Irak y en Siria y, al mismo tiempo, proponer un nuevo contrato social tomando como referencia y modelo las estructuras de las naciones Estado modernas.

⁸¹ LESACA, Javier. «Why did Russian social media swarm the digital conversation about Catalan Independence?» [en línea], en *Washington Post*. 22 noviembre 2017. Disponible en web: https://www.washingtonpost.com/news/monkey-cage/wp/2017/11/22/why-did-russian-social-media-swarm-the-digital-conversation-about-catalan-independence/?noredirect=on&utm_term=.126764742aa3.

⁸² BERGER, J.M.; MORGAN, Jonathon. «The ISIS Twitter Census. The Brookings Project on U.S. Relations with the Islamic World» [en línea], en *Brookings*, Analysis Paper. N.º 20. Marzo 2015. Disponible en web: https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf.

La narrativa disruptiva del Dáesh

La narrativa es la principal arma disruptiva en la gobernanza. Aquellos agentes que logren crear y difundir una narrativa eficaz entre la opinión pública de un determinado país se encontrarán en una posición favorable para implementar su agenda política. Miskimmon, O'Loughlin y Roselle consideran que «debemos tomarnos en serio lo que decimos sobre el mundo y cómo nos ven a nosotros mismos, si queremos explicar los grandes procesos en relaciones internacionales». Estos autores consideran que las narrativas son una parte integral de cómo los actores involucrados en las relaciones internacionales experimentan, comprenden y comunican sus pensamientos.

«Los seres humanos piensan en narrativas y cuentan historias para comprender el mundo que les rodea. Las narrativas fijan los eventos a un pasado, a un presente y a un posible futuro. Las narrativas crean actores y personajes, expectativas sobre su comportamiento y el papel que interpretan, generan significado al contexto y organizan los eventos en un plan que, a su vez, oculta y margina otras formas de entender la realidad. Las narrativas son un aspecto central para entender los procesos de conformación de identidad, el comportamiento de los protagonistas de un sistema internacional, la estructura de un sistema. De igual manera, las narrativas ayudan a entender cómo las ideas, los eventos y las políticas son contestadas por otros agentes»⁸³.

La principal arma disruptiva del grupo terrorista Dáesh en su campaña híbrida ha sido la creación y difusión de una narrativa que ha interpelado y movilizado de manera eficaz a sus audiencias. El éxito de la creación de la narrativa del Dáesh se fundamenta en un doble proceso: comprensión de las principales debilidades y vulnerabilidades de las audiencias y la difusión de las narrativas teniendo en cuenta las resonancias culturales de la audiencia.

Estado Islámico, desde sus comienzos públicos a finales del año 2013, contó con un importante valor añadido respecto a sus rivales y enemigos políticos en Irak y Siria. Esta ventaja consistía en tener la mejor información y análisis político y social de la población suní en estos dos países. Los promotores del califato supieron detectar y entender el creciente malestar que se apoderaba de la población suní en la primera década del siglo xxi.

A pesar del fuerte crecimiento económico que se produjo en Irak entre 2008 y 2012 (7% de crecimiento anual)⁸⁴, las cifras de reducción de la pobreza no mostraron la misma evolución positiva. En las provincias al sur de Kurdistán

⁸³ MISKIMMON, Alister; O'LOUGHLIN, Ben; ROSELLE, Laura. *Strategic Narratives. Communication Power and the New World Order*. Routledge. 2013. P. 176.

⁸⁴ «The Unfulfilled Promise of Oil and Growth. Poverty, Inclusion and Welfare in Irak 2007-2012» [en línea], en *The World Bank Group*. Disponible en web: <http://www.worldbank.org/en/country/irak/publication/unfulfilled-promise-of-oil-and-growth>.

y al norte y alrededor de Bagdad, la pobreza disminuyó sustancialmente, con la única excepción de Nínive, donde la pobreza se disparó. En el año 2012, los niveles de pobreza en Bagdad (de mayoría chií) se mantuvieron estables en torno al 19%. Sin embargo, en la región de Nínive (de mayoría suní) el número de personas pobres se duplicó hasta llegar al 15,7%. Además de eso, en 2007, Nínive, Diyala y Salah El Deen (todas ellas de mayoría suní) juntos sumaron casi el 35% de las personas que vivían en extrema pobreza en Irak⁸⁵.

La marginación económica de la población suní en Irak se ratificó con un informe facilitado por la Oficina de las Naciones Unidas para la Coordinación de Asuntos Humanitarios (UNOCHA, por sus siglas en inglés), donde se corroboraba que las necesidades humanitarias más graves del país se concentran en las partes occidental y septentrional de Irak. Estas áreas coincidían en gran medida con los lugares donde el Dáesh logró concentrar gran parte de su poder sobre el terreno: Nínive, Al Anbar y Salah El Deen⁸⁶.

El Dáesh comprendió que estos datos contribuían de manera decisiva a acelerar la desconexión entre los ciudadanos suníes de áreas como Nínive con el Gobierno central Irakí (gobernado por la mayoría de los chiítas), que se mostraba incapaz de responder a los problemas sociales. El grupo terrorista Dáesh ha utilizado este resentimiento y percepción ciudadana para generar una narrativa que supiera canalizar ese malestar.

El profundo conocimiento que los precursores del califato tuvieron sobre la realidad sociopolítica y económica de Irak demuestra hasta qué punto sus líderes estaban asentados y posicionados dentro de estas comunidades. En este contexto, es especialmente relevante la información y las evidencias que muestran cómo relevantes altos cargos vinculados al partido Baath contribuyeron a la expansión del Dáesh por las áreas sunitas de Irak. Varios documentos secretos confiscados a altos cargos del Estado Islámico muestran que importantes miembros de la inteligencia de Saddam Hussein, como Samir Abd Muhammad al-Khlifawi, desempeñaron un papel decisivo en la creación y conversión del Dáesh en un movimiento social capaz de amenazar la existencia misma del Estado irakí⁸⁷.

El Dáesh comprendió el potencial que tendría elaborar una narrativa que sirviera para, por un lado, desconectar aún más a la población suní de sus instituciones públicas y, al mismo tiempo, promover una narrativa que fomentara un nuevo contrato social que sirviera para poner las bases de un nuevo Estado nación basado en los principios de los Estados modernos: el Estado Islámico.

⁸⁵ Ibídem.

⁸⁶ «Humanitarian Needs Overview» [en línea], en United Nations Office for the Coordination of Humanitarian Affairs. Irak. Noviembre 2015. Disponible en web: http://reliefweb.int/sites/reliefweb.int/files/resources/final_Irak_2016_hno.pdf.

⁸⁷ REUTER, Cristoph. «Secret Files Revel the Structure of th Islamic State» [en línea], en *Spiegel*. 18 abril 2015. Disponible en web: <http://www.spiegel.de/international/world/islamic-state-files-show-structure-of-islamist-terror-group-a-1029274.html>.

Como se ve en la imagen número 1, los mensajes del califato han girado en torno a cuatro grandes temáticas: entrevistas con milicianos, victorias militares, acciones de Gobierno y actos de violencia presentados como espectáculos. Las cuatro grandes temáticas de la narrativa del califato presentan una proporción muy equilibrada (en torno al 25% cada una), lo que sugiere que se trata de una estrategia planeada.

El análisis de las temáticas que guían la narrativa del Dáesh ofrece una interesante conclusión: solo el 15% de los vídeos de este grupo terrorista está únicamente enfocado a mostrar el asesinato de sus enemigos. El 85% del contenido de los 1500 vídeos distribuidos por el califato desde enero de 2014 hasta el 2018 destaca aspectos más relacionados con la gobernanza y la construcción nacional que con la diseminación de terror y caos. En concreto, el 33% de los vídeos del Dáesh muestran entrevistas con jóvenes de todas las partes del mundo en las que explican los aspectos positivos de viajar al califato; el 27% de los vídeos están basados en escenas de batalla en las que el Dáesh se muestra como un ejército propio de un país, capaz de derrotar a sus enemigos en el campo de batalla, y, por último, el 24% de los vídeos muestra la imagen del Dáesh como un Estado nación capaz de proveer servicios públicos a sus ciudadanos y de establecer un nuevo contrato social más justo y eficiente para la población suní de Irak y Siria. Esta última temática entronca de manera directa con el análisis que este grupo terrorista realizó sobre la situación política y socioeconómica de la población suní.

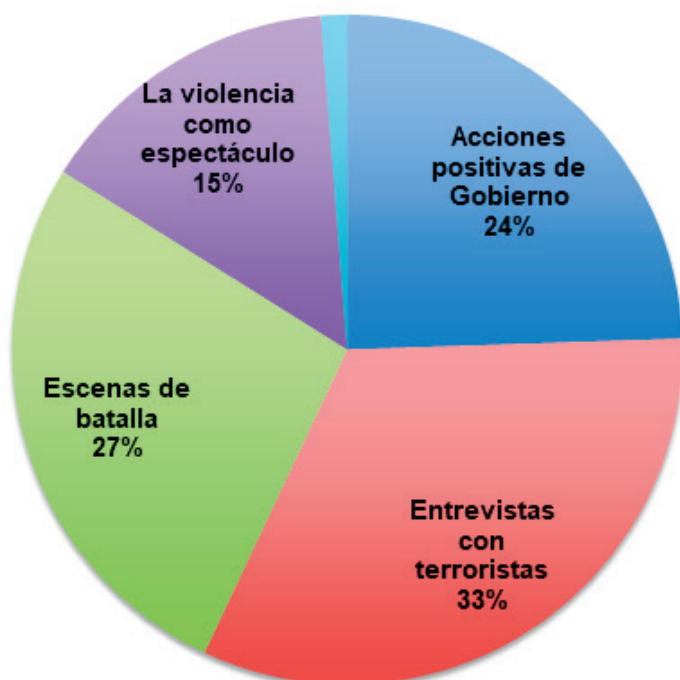


Imagen 1. Principales temáticas de los vídeos distribuidos por el Dáesh entre 2014 y 2018.

Estado Islámico no solo se ha preocupado por crear una narrativa y una temática eficaz para lograr sus logros políticos. El proceso de seducción de sus audiencias potenciales también ha incluido la elaboración y construcción de esas narrativas teniendo en cuenta las características y gustos culturales y estéticos de sus audiencias. Para ello, el Dáesh ha puesto en marcha una sofisticada estrategia transmedia, propia de las industrias del entretenimiento y el espectáculo audiovisual, dando lugar a un nuevo tipo de terrorismo que podría conocerse como *terrorismo transmedia*.

La principal característica del terrorismo transmedia es la elaboración de una narrativa basada en la ausencia de personajes y escenarios principales. O, lo que es lo mismo, una narrativa construida mediante múltiples personajes y diversos escenarios. Al Qaeda asoció su relato a un personaje principal (Bin Laden), que intervenía siempre desde un escenario monótono como una cueva o una sala vacía. El Dáesh rompió desde el principio con esta previsible estrategia comunicativa y aplicó al campo del terrorismo las técnicas más avanzadas de elaboración de guiones de las series de ficción y sagas de películas occidentales como *Juego de Tronos* o *Star Wars*. ¿Quién es el personaje principal de *Juego de Tronos*? ¿Cuál es el principal escenario donde se desarrolla la trama de *Star Wars*? La fuerza del guion de estas historias reside en la interacción de personajes y escenarios. Esa interacción es la verdadera protagonista de la trama. El líder, Abu Bakr al Baghdadi, solo aparece en uno de los mil trescientos vídeos distribuidos por los yihadistas. La fuerza de la narrativa Dáesh, al igual que *Juego de Tronos* o *Star Wars*, reside en la interacción entre múltiples personajes que se relacionan en distintos escenarios, incluso en diferentes plataformas, tal y como se produjo en la estrategia de comunicación del atentado de París del 13 de noviembre de 2015. El grupo yihadista ha ido implementando esta nueva metodología desde mediados de 2014 hasta finales de 2016.

La metodología narrativa empleada por este grupo criminal quedó identificada y definida en la industria del ocio y el entretenimiento en 2003 por Henry Jenkins:

«Según la tradición de Hollywood, una buena historia comienza o bien con un protagonista atractivo o bien con un mundo interesante. De esta afirmación podemos concluir el siguiente argumento: un buen personaje puede sostener múltiples narrativas y, por consiguiente, protagonizar una exitosa saga de películas. Por su parte, un mundo interesante puede sostener múltiples personajes (y sus respectivas historias) y, de esta manera, comenzar con éxito una saga de historias transmedia»⁸⁸.

⁸⁸ Jenkins, Henry. «Transmedia Storytelling» [en línea], en *MIT Technology Review*. Enero 2003. Disponible en web: <https://www.technologyreview.com/s/401760/transmedia-storytelling/>.

Jenkins hacía referencia explícita a exitosas películas y series como *Star Trek*, *Star Wars*, *Tomb Raider*, *Indiana Jones*, *Buffy cazavampiros* o *El Señor de los Anillos*. Once años más tarde, en 2014, las historias transmedia definidas por Jenkins saltaron al mundo del terrorismo mediante la construcción por parte del Dáesh de «un mundo interesante que sostiene múltiples personajes»⁸⁹.

Pero la inspiración cultural occidental del Dáesh no se limita al modelo narrativo transmedia. Con el objetivo de generar la mayor resonancia entre sus potenciales audiencias, Estado Islámico llega incluso a copiar las escenas más populares del imaginario cultural adolescente. Concretamente, el 50% de los vídeos del grupo terrorista en los que se muestra la ejecución de un rehén contiene alguna referencia cultural procedente de productos audiovisuales populares entre las audiencias más jóvenes de los países occidentales.

Un fenómeno similar ocurre en los 345 vídeos publicados, entre enero de 2014 y diciembre de 2016, que incluyen escenas de batalla donde el Dáesh se presenta como un ejército victorioso. Al igual que con los vídeos de asesinatos, más de la mitad de estos productos audiovisuales contienen referencias culturales populares, especialmente del mundo de los videojuegos.

La introducción deliberada de estos elementos culturales propios de la cultura del ocio occidental en los vídeos de los terroristas es un fenómeno que está perfectamente estudiado por los estrategias de la organización terrorista. En verano de 2014 comenzó de manera sistemática y creciente la difusión de grabaciones que contienen las mencionadas referencias culturales. Del total de los mil trescientos vídeos editados y distribuidos hasta diciembre de 2016, un 23,05% contiene alguna referencia cultural explícita a productos culturales previos.

El califato habla el mismo idioma cultural que sus audiencias para que sus mensajes sean más eficaces. Según Entman, los enfoques que empleen elementos que contengan resonancias culturales tienen mayor potencial para influir en la opinión pública: «Cuanto mayor sea la resonancia cultural y la magnitud, más posibilidades existen de que el enfoque de un mensaje logre el apoyo de los pensamientos y las emociones de la audiencia»⁹⁰.

Escenas y planos copiados de películas de acción y de terror populares como *Saw*, *Hostel*, *El francotirador*, *Mad Max*, *Matrix* o *Misión Imposible*; interrogatorios, escenarios y efectos digitales inspirados en series sobre la lucha contra el terrorismo como *Homeland* o *Person of Interest*; efectos digitales, planos subjetivos y dianas interactivas plagiadas de videojuegos como *Call of Duty* o

⁸⁹ LESACA, Javier. *Armas de seducción masiva: la factoría audiovisual de Estado Islámico para fascinar a la generación millennial*. Ediciones Península. 2017.

⁹⁰ ENTMAN, Robert M. *Projections of Power. Framing News, Public Opinion and U.S. Foreign Policy*. Chicago: The University of Chicago Press, 2004.

Grand Theft Auto; vídeoclips con ritmo y estética hip-hop... Los elementos de inspiración cultural que el califato ha introducido en sus producciones audiovisuales han logrado transformar el terror en un producto cultural atractivo y popular y, sobre todo, han difuminado la línea estética que separaba la ficción de la realidad. Las audiencias potenciales perciben sus vídeos como elementos de ficciones fascinantes e imitables.

El análisis de estos elementos refleja que los videojuegos, seguidos por las películas de terror y acción, son las principales fuentes de inspiración de los guionistas del califato⁹¹.

Estrategia de medios y plataformas de difusión propias

El grupo terrorista, al igual que una marca o un producto, utiliza esta combinación de canales, propia del *marketing*, para difundir sus mensajes. El único elemento que los seguidores de Baghdadi no pueden utilizar sistemáticamente es el de medios pagados, puesto que ningún canal de comunicación prestaría sus espacios para que insertaran publicidad de pago.

De esta manera, la estrategia de difusión de los mensajes violentos quedaría principalmente asentada sobre dos patas: medios propios y medios ganados.

La estrategia de medios ganados se mide en función de las veces en las que el grupo terrorista consigue que sus creaciones audiovisuales marquen la agenda y sean reflejadas en los medios de comunicación tradicionales. La cobertura que las televisiones, los periódicos y las páginas web realizaron de la decapitación de James Foley o las informaciones que se publicaron tras la publicación del vídeo con el asesinato del piloto jordano quemado vivo en una jaula representan ejemplos de esta estrategia. Las únicas imágenes disponibles para informar de estos sucesos eran aquellas que proporcionaban los propios extremistas a través de sus propios medios. Los medios de comunicación tradicionales no tenían más remedio que replicar estas imágenes si querían informar del suceso, con lo que, de manera colateral, participaban en la estrategia de comunicación del califato.

La estrategia de medios propios del Estado Islámico resulta de gran relevancia, tanto por su magnitud como por su diversificación. Según explicó el periodista británico John Cantlei en uno de sus reportajes, el objetivo de la estrategia de medios de comunicación de los terroristas es el de «contrarrestar las ideas que provienen de Occidente de tal manera que los ciudadanos de aquí, los que están sobre el terreno, tengan una idea precisa de qué está haciendo el Estado Islámico. No la imagen distorsionada que genera la prensa occidental»⁹².

⁹¹ LESACA, Javier. *Armas de seducción masiva...* Op. cit., p. 218.

⁹² Al Hayat Media Center. From Inside Haleb. 11 febrero 2015.

El Dáesh tiene la vocación de comunicar un gran número de mensajes a sus audiencias y quiere tener el control sobre el enfoque de esos mensajes. Para ello, la organización terrorista ha seguido el ejemplo de consolidación horizontal que se ha producido en los últimos años en el sector de las empresas de comunicación y ocio. La empresa que aglutinó y coordinó la mayor parte de este esfuerzo mediático del grupo violento fue *Al Hayat Media Center*, creada en junio de 2014.

Este proceso de integración de diversas empresas y medios responde, una vez más, a la estrategia transmedia que inspira toda la acción comunicativa del califato. La nueva narrativa creada por este grupo criminal requiere adaptar los procesos de difusión y también la forma en la que se relacionan las empresas que gestionan y difunden esos contenidos. La industria del ocio y del entretenimiento ha adaptado sus estructuras empresariales a esta nueva forma de contar historias, y el Dáesh ha copiado de manera exacta este proceso de consolidación empresarial.

Esta nueva forma de contar las historias y de conectar con las audiencias no solo ha tenido un impacto en la producción de los mensajes, sino en la propia industria de la comunicación y del entretenimiento. Según Jenkins:

«El *storytelling transmedia* es un reflejo de la consolidación económica que se está produciendo en la industria de los medios de comunicación. Un proceso que algunos observadores definen como sinergia. Las empresas modernas de comunicación están viviendo una integración horizontal que les permite mantener intereses a lo largo diversas industrias que antes actuaba [*sic*] de manera independiente. Un conglomerado de medios de comunicación tiene una ventaja para difundir su marca y expandir sus franquicias a lo largo del máximo número de plataformas»⁹³.

El Dáesh es el primer caso documentado de grupo violento y extremista que utiliza y se adapta de manera sistemática a la narrativa transmedia. Sus propias estructuras de comunicación están adaptadas para generar y difundir este tipo de mensajes. Los terroristas crearon en el año 2014 una red de medios propios inspirada en las sinergias de las empresas de comunicación occidentales, una red que incluye revistas en diversos idiomas, agencias de noticias, productoras audiovisuales y cadenas de radio; un conglomerado de medios, integrados horizontalmente, que difunde en diferentes formatos las mismas historias y los mismos encuadres, con el objetivo de que las diferentes audiencias puedan acceder al mensaje desde distintas plataformas.

En un vídeo publicado el 6 de julio de 2016, titulado *La estructura del califato*, el grupo terrorista explica los recursos con los que cuenta su ministerio (*di-*

⁹³ Ibidem.

wan) de comunicación⁹⁴. Los medios de comunicación oficiales propios que el califato reconoce de manera pública son las siguientes:

- a) Dos productoras audiovisuales con una audiencia global (no segmentada): Al Furqan y Al Hayat.
- b) 33 productoras audiovisuales regionales segmentadas en las diferentes regiones del califato.
- c) Una productora musical: Ajnad.
- d) Una emisora de radio: Al Bayan.
- e) Una revista en árabe: Al Nabá.
- f) Esta revista, que nació en el año 2014 como un panfleto que se repartía fotocopiado en aquellos lugares que el Dáesh lograba conquistar, mutó en el año 2015 hacia una revista en formato digital mucho más sofisticada y mejor diseñada.
- g) Cuatro revistas en lenguas extranjeras: Dabiq (inglés); Dar al Islam (francés); Konstantiniyye (turco) e Istok (ruso).
- h) Una agencia de propaganda *offline*: Maktaba Al Hama.
- i) Un departamento de traducción.

Los terroristas reconocen también la existencia de un grupo oficial de «seguidores», aunque no indica qué función específica tienen asignada dentro de la estrategia de comunicación.

Esta relación de medios propios oficiales reconocida por el Dáesh requiere ser matizada y explicada. El análisis científico de las comunicaciones oficiales del califato desde 2014 hasta 2016 refleja un panorama más complejo y sofisticado que incluye también a la productora de comunicación Al Ittissam, la revista Rumiya, una agencia de noticias e infografías y, sobre todo, a la agencia de noticias oficiosa de Estado Islámico, Al Amaaq⁹⁵.

Distribución automatizada de las campañas

¿Dónde almacena el Dáesh sus vídeos? ¿Qué cuentas se encargan de difundir los contenidos de la estrategia de comunicación y *marketing* diseñada por los terroristas?

Los principales aliados del califato para almacenar y distribuir sus campañas de comunicación son las plataformas comerciales más populares de almacenamiento e intercambio de archivos. La estrategia de comunicación pública de los seguidores de Al Baghdadi consiste en no esconderse; al con-

⁹⁴ AL FURQAN. *The structure of the Caliphate*. 6 julio 2016.

⁹⁵ LESACA, Javier. *Armas de seducción masiva... Op. cit.*, p. 218.

trario, se esfuerzan para que sus mensajes sean lo más públicos y abiertos posible. Un equipo de especialistas del Dáesh se encarga periódicamente de mantener activos y de reponer en plataformas digitales de uso abierto todos los vídeos creados por sus 37 productoras.

Hay que reconocer que las empresas tecnológicas que dan servicio a páginas como Youtube, Dropbox, Archive.org, Sendvid, Dailymotion, GoogleDrive, Microsoft OneDrive o Wetransfer están cada vez más sensibilizadas ante este fenómeno y se esfuerzan a diario por borrar y eliminar los contenidos subidos por la organización terrorista. El 6 de diciembre de 2016, las principales compañías tecnológicas anunciaron un pacto para crear una base de datos común que permitiera eliminar el contenido extremista y violento que se difundía en sus plataformas⁹⁶. Sin embargo, también es cierto que en enero de 2017 costaba muy pocos segundos encontrar y descargar en páginas abiertas de Internet el vídeo del asesinato del piloto jordano o la decapitación del periodista James Foley, entre otros.

La difusión a la opinión pública de estos contenidos audiovisuales de carácter violento y extremista también se desarrolla de manera abierta a través de las redes sociales más populares. Un estudio detallado de la distribución de estos mensajes en la red social Twitter demuestra que los seguidores del califato distribuyen en cada campaña una media de 746 mensajes escritos por 337 cuentas creadas *ad hoc* el mismo día de la difusión de la campaña.

Esta investigación, desarrollada con la tecnología de la empresa de análisis de *big data* Alto Data Analytics, ha permitido radiografiar y dibujar la evolución de diecisiete campañas de distribución de vídeos del Dáesh en mayo de 2016. Los datos muestran cómo la media de difusión de cada campaña es de unas cinco horas y que la media de impactos directos es de una audiencia de más de 110.000 personas. La organización terrorista es consciente de que las compañías tecnológicas tardan una media de dos y cuatro horas en detectar y eliminar los mensajes de sus plataformas. Ese es el espacio que utilizan para difundir sus campañas a la opinión pública. La investigación también ha detectado que en cada campaña los comunicadores del califato utilizan una media de nueve robots para difundir el contenido de manera automática y masiva⁹⁷.

Conclusión

Las ofensivas comunicacionales en el contexto de las guerras híbridas no son una amenaza para el futuro de España, sino para su presente. Naciones Estado y grupos violentos de carácter subnacional interesados en debilitar

⁹⁶ EUROPA PRESS. «Los gigantes de Internet crearán base de datos común para combatir el contenido extremista» [en línea]. 6 diciembre 2016. Disponible en web: <http://www.europapress.es/internacional/noticia-gigantes-internet-crearan-base-datos-comun-combatir-contenido-extremista-20161206091427.html>.

⁹⁷ LESACA, Javier. *Armas de seducción masiva... Op. cit.*, s.p.

la cohesión social del Estado español tienen la capacidad y la voluntad para emprender acciones ofensivas destinadas a influenciar de manera artificial la opinión pública, socavar la confianza de los ciudadanos con las instituciones públicas y dañar el contrato social entre ciudadanos y agentes públicos.

La metodología disruptiva utilizada por estos potenciales enemigos está claramente definida y sigue un patrón constante:

- a) Detección de las vulnerabilidades y puntos de fricción en la opinión pública de una sociedad.
- b) Creación de una narrativa disruptiva que potencie los puntos de fricción de una sociedad, debilite la cohesión social y aumente las vulnerabilidades de una nación Estado.
- c) Implementación de una red de medios propios que permita la comunicación directa con los ciudadanos sin tener que pasar por el papel mediador de los medios de comunicación tradicionales.
- d) Utilización tramposa y automatizada de las plataformas sociales con el fin de distribuir de manera masiva y segmentada las narrativas disruptivas.

España y los organismos multilaterales aliados deben protegerse ante este tipo de amenaza de manera eficaz y rápida. Las democracias liberales son instituciones especialmente vulnerables a este tipo de ataques. El Estado tiene limitaciones a la hora de emprender políticas encaminadas a condicionar o interferir en la opinión pública de un país y en la libertad de pensamiento y de expresión de los ciudadanos. Sin embargo, de igual manera que es preciso preservar los principios básicos y fundamentales que definen un Estado de derecho y una democracia liberal, también es recomendable construir mecanismos de defensa ante hipotéticas injerencias y disrupciones comunicativas destinadas a socavar el propio Estado de derecho.

Las herramientas de escucha activa y de análisis de *big data* en redes sociales permiten determinar con precisión y objetividad las acciones comunicativas disruptivas que utilizan herramientas artificiales para desestabilizar la opinión pública de un determinado Estado. La monitorización constante, el análisis riguroso y la denuncia pública de estas acciones deben incluirse como una capacidad de defensa prioritaria en las instituciones públicas, destinadas a velar por la defensa y seguridad de los ciudadanos.

Al mismo tiempo, los Gobiernos deben adoptar un papel proactivo y constituir una plataforma de diálogo para el diálogo de políticas con el sector privado (empresas de tecnología, plataformas de distribución de contenido, productoras audiovisuales), con los medios de comunicación tradicionales, con la Academia y con agentes relevantes de la sociedad civil. El objetivo de esta plataforma de diálogo es el de consensuar acciones que garanticen el acceso de los ciudadanos a información veraz y contrastada y a un entorno comunicativo que fomente la libertad, el debate, la pluralidad y la transparencia.

Capítulo quinto

El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato

Manuel R. Torres Soriano

Resumen

El propósito de este capítulo es analizar cómo el hacktivismo ha sido empleado por individuos y organizaciones como una eficaz estrategia de comunicación. Se presta una especial atención a dos manifestaciones particulares: el hacktivismo yihadista y el antisistema. El propósito de ambos estudios de caso es analizar las dinámicas organizativas de estos movimientos. Se parte de la tesis de que el principal reto al que tiene que enfrentarse el hacktivismo (particularmente el de carácter delictivo) no es tanto la viabilidad de sus operaciones sino cómo conciliar su vertiente colectiva con la individualidad de sus miembros.

Palabras clave

Internet, ciberseguridad, medios de comunicación, privacidad, propaganda.

Abstract

The purpose of this chapter is to analyze how hacktivism has been used by individuals and organizations as an effective communication strategy. Particular attention is paid to two particular manifestations: Jihadist and anti-system hacktivism. The purpose of both case studies is to analyze the organizational

dynamics of these movements. The starting point is the thesis that the main challenge facing hacktivism (particularly that of a criminal nature) is not so much the viability of its operations, but how to reconcile its collective side with the individuality of its members.

Keywords

Internet, cybersecurity, media, privacy, propaganda.

Introducción

A comienzos de 2010, la secretaria de Estado norteamericana Hillary Clinton presentó la *Internet Freedom*¹ como uno de los ejes de la política exterior de su país. En un entusiasta discurso atribuyó a las nuevas tecnologías de la información la capacidad de reescribir las reglas del activismo político y empujar a la humanidad hacia un proceso irreversible de liberalización política y democratización. Esta visión era consecuente con una tradición previa de utopismo tecnológico² que atribuía a esta herramienta una naturaleza intrínsecamente beneficiosa. Según esto, las nuevas tecnologías fomentan la circulación de la información y la participación de los ciudadanos en las cuestiones políticas, los cuales gozan de un poderoso instrumento para obtener una mayor transparencia y responsabilidad en la actuación de sus gobernantes. Siguiendo esta lógica, algunos autores llegaron a sugerir que los creadores de la red social Twitter deberían recibir el Premio Nobel de la Paz por haber hecho posible el instrumento que galvanizó las protestas de 2009 en Irán contra el fraude electoral³.

Esta visión sobre Internet como una fuerza en pro del conocimiento y la libertad recibió un nuevo respaldo durante los primeros compases de las llamadas Primaveras Árabes. Internet era el elemento diferencial que había hecho posible en ese momento histórico el proceso de transformación política en el mundo árabe y musulmán. El futuro estaría protagonizado por una masa de ciudadanos empoderados por las nuevas tecnologías, frente a unas autócratas que habían perdido el monopolio sobre los flujos de información.

Este optimismo se vio pronto afectado por el insatisfactorio (y en algunos casos, trágico) desenlace de los distintos escenarios donde se produjeron las protestas. Empezó así a ganar fuerza una visión antagónica sobre la naturaleza de Internet, una perspectiva que atribuía efectos deterministas a un instrumento que era capaz de erosionar la libertad y privacidad de los ciudadanos en los países democráticos, al tiempo que cimentaba el autoritarismo político en el resto del mundo, potenciando hasta límites insospechados los aparatos de control y represión. Esta visión pesimista se vio reforzada por el desembarco en el territorio virtual de todo tipo de depravados, criminales y grupos terroristas. Una presencia inquietante que alimentaba los miedos y fobias de una sociedad que contemplaba con desconcierto cómo

¹ CLINTON, Hillary. «Remarks on Internet Freedom» [en línea], en *The Newseum*. Washington DC. 21 enero 2010. Disponible en web: <https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm>

² TORRES, Manuel R. «Internet como motor del cambio político: ciberoptimistas y ciberpesimistas» [en línea], en *Revista del Instituto Español de Estudios Estratégicos*, n.º 1. 2013. pp. 127- 148. Disponible en web: <http://revista.ieee.es/index.php/ieee/article/view/40/36>.

³ ADAY, Sean et al. «Blogs and Bullets. New Media in Contentious Politics» [en línea], en *United States Institute of Peace*. Washington DC. 2010. Disponible en web: <https://www.usip.org/publications/2010/09/blogs-and-bullets-new-media-contentious-politics>.

la herramienta que presuntamente iba a universalizar el conocimiento y la libertad, otorgaba una visibilidad inédita a la superstición, la intolerancia y el fanatismo.

Más allá de las lecturas maniqueas que ignoran la naturaleza neutra de esta herramienta, existe un terreno intermedio donde se ha producido la eclosión de un nuevo tipo de activismo político que no solo emplea Internet como una plataforma para promover sus objetivos, sino que también emplea esta tecnología para llevar a cabo, desde un punto de vista instrumental, actividades ilícitas o delictivas que contribuyen a aumentar la resonancia de su ideario. Es el llamado *hacktivismo*, un término que apunta hacia la confluencia entre el activismo político y el uso de técnicas de *hacking*. Se trata de un fenómeno de gran interés que se mueve en una incómoda intersección entre el crimen y el activismo político. Supone, al mismo tiempo, la confirmación de las dos visiones deterministas sobre la naturaleza de Internet: aquella que lo contemplaba como un proceso de empoderamiento de los individuos, y aquella otra que lo contempla como una ventana abierta a los aspectos más sórdidos de la naturaleza humana. Esta naturaleza ambivalente ha generado que no exista unanimidad sobre su conceptualización y elementos definitorios. Las aproximaciones a este fenómeno oscilan entre aquellas visiones que lo entienden como una nueva forma de participación política no convencional, que aprovecha las potenciales que ofrece el ciberespacio, a aquellas otras que lo entienden como una táctica delictiva para avanzar en los objetivos de grupos de carácter ilegítimo.

El propósito de este capítulo es analizar cómo el hacktivismo ha sido empleado por individuos y organizaciones como una eficaz estrategia de comunicación. Todo lo relacionado con el ciberespacio se encuentra rodeado de una aureola de misterio y sofisticación que lo convierte en irresistible ante la perspectiva de los medios de comunicación. Esta atracción es aún más intensa cuando ese ámbito se fusiona con otro tipo de factores de alto impacto informativo como el escándalo político y social, el crimen o el terrorismo. El hacktivismo es contemplado por algunos actores como una carta ganadora que proporciona una visibilidad que difícilmente podrían alcanzar con otro tipo de tácticas.

El universo del hacktivismo es muy heterogéneo, y en él podemos encontrar actores que, a pesar de su praxis delictiva, gozan de una amplia legitimidad por el tipo de objetivos que persiguen o por el antagonismo que originan las víctimas de sus acciones. Este trabajo va a centrar su atención en dos manifestaciones particulares, cuyos objetivos son rechazados por una gran mayoría social: el hacktivismo yihadista y el antisistema. El propósito de ambos estudios de caso es analizar las dinámicas grupales e individuales en las cuales se basan estos movimientos, así como las ventajas y debilidades que posee este tipo de activismo como estrategia de comunicación.

Una breve historia del hacktivismo

Hactivismo es un término cuyo origen suele atribuirse a un grupo de *hackers* estadounidense que en 1984 adoptaron el nombre de La Secta de la Vaca Muerta, en referencia al matadero texano donde el grupo realiza sus reuniones. Entre su ideario se encontraba la proclama de que el acceso a la información online era un derecho humano universal, lo que les llevó a poner en marcha un proyecto llamado *hacktivismo*, destinado a luchar contra la censura de Internet y a la prestación de apoyo técnico a los internautas que vivían bajo Gobiernos opresivos. Sus acciones características incluían toda una serie de prácticas exclusivamente virtuales, las cuales, a pesar de su carácter no violento, planteaban problemas en cuanto a su legalidad.

A principios de la década de los noventa, cuando los primeros grupos de hacktivismo hicieron su aparición, fue frecuente que desde el ámbito académico se interpretara el fenómeno como una expresión natural del activismo político protagonizado por redes de ciudadanos. Según esta visión, el fenómeno era el resultado de la intersección entre la disponibilidad del ciberespacio, las sociedades de la información y los modernos movimientos sociales de protesta y resistencia. Para algunos observadores, constituían el vínculo entre Internet y la globalización de la democracia participativa⁴.

Aquellos que contemplaban con simpatía estos nuevos actores establecían una clara distinción entre este uso poco ortodoxo del activismo político a través del ciberespacio y aquellas otras actividades catalogadas como *cracking*, las cuales no dejaban de ser usos meramente delictivos de las nuevas herramientas informáticas.

El contexto sociopolítico que desencadenó el movimiento antiglobalización de mediados de la década de los noventa⁵ sirvió también como germen de los primeros grupos hacktivistas. Puede apreciarse una confluencia entre ambos fenómenos (malestar antiglobalización y nuevas tecnologías de la información) en el protagonismo mundial que alcanzaría el movimiento zapatista de Chiapas (México)⁶.

Al amparo de esta nueva ventana tecnológica se congregaron un tipo de activistas políticos revestidos de tres cualidades propias⁷: a) La apuesta por acciones simples, pero de gran impacto social y mediático; b) Una elevada

⁴ JORDAN, Tim. *Activism! Direct Action, Hacktivism and the Future of Society*. London: Reaktion Books, 2002; HILL, Kevin & HUGHES, John E. *Cyberpolitics: Citizen Activism in the Age of the Internet*. Lanham (Md): Rowman & Littlefield, 1998.

⁵ AUTY, Caroline. «Political hacktivism: tool of the underdog or scourge of cyberspace?», *Aslib Proceedings*, vol. 56, n.º 4, 2004, pp. 212-221.

⁶ HARVEY, Neil. *The Chiapas Rebellion: The Struggle for Land and Democracy*. London: Duke University Press, 1998.

⁷ JORDAN, Tim; TAYLOR, Paul A. *Hacktivism and cyberwars: Rebels with a cause?* London: Routledge, 2004.

cualificación técnica que les permitía dominar las nuevas tecnologías de la información, y c) Su desprecio hacia las normas establecidas.

A pesar de que las primeras aproximaciones académicas al fenómeno partían de una valoración positiva sobre los integrantes y objetivos de estos grupos, los medios de comunicación de masas tardaron poco tiempo en enfatizar aquellas otras características que más suspicacia generaban entre la ciudadanía. El carácter anónimo de sus acciones sirvió de base para el tratamiento sensacionalista de la información procedente sobre estos grupos. La predilección que sus miembros mostraron por adoptar nombres inquietantes como The Legion of Doom, Bad Ass Mother Fuckers, Toxic Shock, etc., tampoco ayudó a mejorar este enfoque.

Esta tendencia se vio reforzada por el clima de inseguridad generado por los atentados del 11 de septiembre de 2001 en Washington y Nueva York. La figura del *hacker* empezó a identificarse con la de criminal, y por extensión con la del ciberterrorista⁸. Empezaron a ganar peso los análisis que lo identifican básicamente como una nueva forma de participación política ilegítima, centrada básicamente en el recurso a los ciberataques, sabotajes y robo de información en el ciberespacio como instrumento de presión e influencia.

La trayectoria de grupos de hacktivismo como Anonymous fue interpretada como una premonición del preocupante poder que podía alcanzar una nueva generación de actores virtuales motivados únicamente por el nihilismo. A la altura de 2011, tan solo tres años después de sus primeras acciones, el grupo ya era percibido como una ciberamenaza de primer nivel debido a la magnitud y frecuencia de sus operaciones de hackeo.

Entre lo individual y lo colectivo

A la hora de entender las causas que han provocado la eclosión del activismo político a través del *hacking* ha sido habitual centrar la atención en su utilidad instrumental. Suele incidirse⁹ en factores como:

- a) Su accesibilidad, incluso para gente que carece de conocimientos técnicos.
- b) El reducido riesgo personal de este tipo de activismo si lo ponemos en relación con otro tipo de prácticas como las protestas o sabotajes callejeros.

⁸ VEGH, Sandor. «The media's portrayal of hacking, hackers, and hacktivism before and after September 11» [en línea], en *First Monday*. 2005. Disponible en web: <http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126>.

⁹ DENNING, Dorothy. «The Rise of Hacktivism» [en línea], en *Georgetown Journal of International Affairs*. 2015. Disponible en web: <https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism>.

- c) Permite sumarse de manera efectiva a todo tipo de causas, sin importar la distancia o las diferencias culturales o idiomáticas.
- d) Sus acciones tienen un alto impacto en la opinión pública y los medios de comunicación.

Los patrones organizativos en este tipo de movimientos varían en términos de formalización y apertura, pero todos ellos normalmente comparten estas características:

- e) Suelen constituirse entre grupos de iguales y rechazan jerarquías y mecanismos de representación, aunque es posible encontrar algún tipo de estructuras basadas en un reparto consensuado de tareas para garantizar su sostenibilidad.
- f) La confianza y la lealtad suelen ser los principales mecanismos de reclutamiento, lo que produce organizaciones de tamaño reducido, pero también movimientos más amplios que se basan en la existencia de pequeños clústeres de individuos comprometidos con un objetivo específico.
- g) La división de trabajo se realiza en base a la reputación individual y a la existencia de un alto grado de motivación de sus miembros.
- h) El proceso de toma de decisiones suele producir tensiones entre lo colectivo y lo individual. Mientras que el hacktivismo es un proceso predominante grupal, gran parte de su éxito depende de las habilidades individuales de unos pocos de sus miembros, lo que puede producir conflictos entre sus participantes más valiosos y aquellos que desean disipar las individuales dentro de una personalidad colectiva.

Para entender las dinámicas de gestión de la identidad de los miembros de estos grupos, resulta útil realizar un paralelismo con el mundo de la criminalidad común en Internet. Puede observarse, por ejemplo, que para los ciberdelinquentes el anonimato es tanto un beneficio como un problema: es útil porque los hace menos detectables para las agencias policiales y para otros competidores que desean atacarlos, pero es una limitación porque sin reputación es muy complicado hacer negocios o establecer relaciones de cooperación con otros delinquentes. Sin alguna forma de verificar la identidad, no se puede establecer la confianza. El objetivo es por tanto conjugar objetivos que *a priori* parecen incompatibles: anonimato y reputación.

Existen diferentes procedimientos que permiten establecer relaciones de confianza en un entorno hostil¹⁰. Así, por ejemplo, los ciberdelinquentes recurren a múltiples indicadores para establecer si un posible colaborador es un agente del orden público, un impostor sin credenciales reales o un mero

¹⁰ LUSTHAUS, Jonathan. «Trust in the world of cybercrime», en *Global crime*, vol. 13, n.º 2, 2012, pp. 71-94.

espectador «en el lugar equivocado, en el momento equivocado». Como en cualquier otra subcultura, los criminales cibernéticos exhiben sus propios patrones de comportamiento y lenguaje. Estos pueden ser una mezcla de elementos idiomáticos, los temas de los que hablan, actitud, conocimiento y capacidad. La participación permanente en este tipo de subculturas virtuales proporciona un tipo de conocimiento intuitivo muy similar al que se desarrolla en las interacciones cara a cara dentro de los entornos delincuenciales, el cual constituye un importante patrón para establecer la confianza hacia un desconocido. No obstante, este sistema de identificación no es perfecto y necesita ser complementado con otra serie de procedimientos, como la creación de espacios virtuales excluyentes, en los cuales es muy difícil que se produzca un encuentro accidental con alguien que no tiene una voluntad clara de frecuentar esos espacios. Así, por ejemplo, uno de los elementos clave que discrimina un ciberdelincuente genuino de otro tipo de internauta es el conocimiento de dónde se hallan los diversos canales y foros *online* donde localizar a este tipo de individuos. De esa forma, si en el mundo «físico» es plausible que un no criminal pueda acceder de manera accidental a un bar con conexiones criminales, es muy improbable que un internauta común pueda acceder a un foro de venta de narcóticos oculto dentro del anonimato de la *dark web*. Este tipo de espacios no solo están excluidos de manera deliberada de los motores de búsqueda e indexación, sino que su ubicación está en continua migración para eludir el bloqueo de las empresas prestadoras de servicios. Sin una considerable inversión de tiempo para mantener actualizados los contactos y el conocimiento de los lugares de encuentro, resulta muy difícil acceder a estos espacios y contar con la reputación suficiente para poder interactuar con sus miembros.

No suele prestarse tanta atención¹¹ a los incentivos psicológicos que aporta este tipo de activismo. Se trata de un aspecto que ayuda a entender cómo el hacktivismo no es solo un instrumento útil para el logro de un objetivo político, sino que, para algunos, puede ser un fin en sí mismo debido a su capacidad de aportar una experiencia gratificante.

Algunos de los principales movimientos hacktivistas han tenido su origen en comunidades virtuales cuyo principal nexo de unión era el deseo de sus miembros de transgredir las convenciones sociales desde una perspectiva lúdica. Así, por ejemplo, las raíces de Anonymous pueden detectarse en un foro japonés denominado 2chan dedicado a compartir todo tipo de contenidos aberrantes relacionados con el anime, el porno y las bromas pesadas¹². En 2003 se crea el equivalente en lengua inglesa de esta página,

¹¹ CHENG, Justin; DANESCU-NICULESCU-MIZIL, Cristian; LESKOVEC, Jure. «Antisocial Behavior in Online Discussion Communities» [en línea], en *Proceedings of the Ninth International AAAI Conference on Web and Social Media*. 2015. pp. 61-70. Disponible en web: <https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/viewFile/10469/10489>.

¹² BARTLETT, Jamie. *The dark net: Inside the digital underworld*. London: Melville House, 2015.

4chan, el cual copió con éxito este modelo y fue capaz de congregarse a una amplia comunidad dedicada al «lulz» (una corrupción del acrónimo en inglés LOL: *laugh out loud*; reír a carcajadas). Este germen prepolítico originó las primeras tensiones internas en este colectivo cuando algunos de sus usuarios propusieron enfocar sus actividades hacia causas más trascendentes, como la lucha contra la censura en Internet. Algunos usuarios se opusieron a esta reorientación, que contemplaban como una amenaza existencial al único propósito del foro: divertirse sin importar las consecuencias. A pesar de ello, un buen número entendió como conciliables ambos propósitos, y no renunció a la vertiente lúdica del logro de objetivos «morales».

Para entender esta predisposición a la transgresión de las normas sociales resulta útil recurrir a la psicología social. Alguna de sus aportaciones permite entender el atractivo de algunos comportamientos que rompen con lo que se considera socialmente aceptable, pero también cómo este tipo de actitudes pueden verse reforzadas y ampliadas cuando se producen en el ámbito de Internet.

Una de las contribuciones más populares a este ámbito de estudio ha sido la de John Suler, el cual desarrolló el concepto de *efecto de desinhibición online*¹³, según el cual los individuos tienen una mayor propensión a romper las normas sociales cuando se encuentran en un entorno *online* que en uno *offline*. Esto se produce como consecuencia de que algunos sujetos «disocian» su realidad física de su realidad virtual. En esta última puede proyectar una identidad ficticia que no tiene por qué atenerse a las restricciones sociales o a la idea de asumir las consecuencias de su comportamiento. La percepción de anonimato (tanto propio como ajeno) y la sensación de irrealidad les lleva a entender que sus infracciones son impunes al carecer de consecuencias en el mundo «real». El sentido de pertenencia a un colectivo que aprueba y alienta este tipo de actitudes difumina en la responsabilidad grupal determinadas prácticas que serían más difíciles de racionalizar desde un punto de vista individual. Así, por ejemplo, uno de los eslóganes más desafiantes de Anonymous era precisamente: «porque ninguno de nosotros es tan cruel como todos nosotros»¹⁴.

Este tipo de percepciones se ven reforzadas en espacios como, por ejemplo, 4chan, donde el anonimato constituye un principio organizativo¹⁵. Ante

¹³ SULER, John. «The online disinhibition effect», en *Cyberpsychology & Behavior*, vol. 7, n.º 3, 2004, pp. 321-326.

¹⁴ MITCHELL, Liam. «Because none of us are as cruel as all of us: Anonymity and Subjectivation» [en línea], en *Theory Beyond the Codes*. 2013. Disponible en web: http://ctheory.net/ctheory_wp/because-none-of-us-are-as-cruel-as-all-of-us-anonymity-and-subjection/.

¹⁵ BERNSTEIN, Michael S., et al. «4chan and/b: An Analysis of Anonymity and Ephemerality in a Large Online Community» [en línea], en *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*. 2011. pp. 50-57. Disponible en web: <http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/download/2873/4398/>.

la ausencia de un sistema que permita verificar la identidad y credibilidad de sus participantes, estas comunidades adoptan otro tipo de estrategias de identificación como el uso compartido de determinadas imágenes, una jerga propia o determinadas pautas de comportamiento que distinguen a los miembros del grupo del resto de internautas. En el caso de la comunidad que dio origen a Anonymous, se optó por cualquier manifestación transgresora: la misoginia, el racismo, la burla contra las minusvalías, las extravagancias sexuales, etc.

Otro factor que facilita las dinámicas que hacen posible el hacktivismo es lo que se ha denominado *sindicación online*¹⁶, la cual hace referencia a cómo Internet ha permitido agregar a individuos que comparten determinadas conductas o intereses, que son minoritarios y habitualmente rechazables por el conjunto de la sociedad. En un contexto previo a Internet, era el azar y la cercanía física lo que determinaba las oportunidades de que estos sujetos pudiesen socializar, normalizar y promover sus intereses comunes. Así, por ejemplo, la probabilidad de que alguien interesado en una parafilia sexual minoritaria pudiese entrar en contacto con otras personas que compartan sus mismas aficiones era muy reducida si este residía en una pequeña localidad alejada de los grandes núcleos urbanos. Sin embargo, Internet crea los espacios de encuentro necesarios para conectar y promover desde un punto de vista colectivo actitudes que antaño habían sido relegadas por la improbabilidad de que se produjese esta conexión física.

La eclosión del hacktivismo antisistema: Anonymous¹⁷

La marca Anonymous y el hacktivismo se han convertido en sinónimos como consecuencia del enorme éxito mediático alcanzado por este movimiento de base virtual. El nombre de Anonymous empezó a ser una palabra familiar en los informativos y en las declaraciones de políticos y responsables de las agencias de seguridad e inteligencia de medio mundo. Su estructura sin liderazgo y su lógica de funcionamiento basada en la espontaneidad y el voluntarismo de sus miembros parecían una combinación invencible frente a la cual poco podían hacer las estructuras de poder clásicas¹⁸. Sin embargo, en un corto espacio de tiempo, tuvo lugar una sucesión de operaciones policia-

¹⁶ AIKEN, Mary. *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*. New York: Random House Publishing Group, 2017.

¹⁷ Este epígrafe se basa de manera extensa en un artículo previo del autor: TORRES, Manuel R. «Lecciones aprendidas de la lucha contra el yihadismo en Internet» [en línea], en *IEEE Documento de Opinión*. Abril 2017. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEE004-2017_Lucha_Yihadismo_Internet_MRTorres.pdf.

¹⁸ OLSON, Parmy. «5 Things Every Organization Can Learn From Anonymous» [en línea], en *Forbes*. 6 mayo 2012. Disponible en web: <http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/>.

les contra sus miembros más destacados, lo que provocó una rápida decadencia operativa del movimiento y la pérdida de su protagonismo mediático.

La breve historia de Anonymous es de gran interés para entender algunas dinámicas de poder y movilización social en plena era de la información. El principal activo de Anonymous es precisamente su atractivo como marca. Su nombre y una estética propia de los comics de superhéroes funcionaron como reclamo para que miles de internautas se sintiesen atraídos por una identidad alternativa que prometía misterio, secretismo y la oportunidad de cambiar el mundo desde la comodidad de un ordenador.

Una de las realidades más sorprendentes de este «éxito comercial» es que su origen no es el sesudo trabajo de un equipo de expertos en *marketing* y comunicación, sino el resultado del azar y la creatividad espontánea de la subcultura de Internet. Como se ha mencionado con anterioridad, el germen de Anonymous es un foro de Internet llamado 4chan, creado originariamente como un lugar para el intercambio de archivos de imagen entre los aficionados al anime japonés. Desde su aparición en 2003 fue evolucionando dando cabida a otro tipo de contenidos, los cuales siempre tuvieron como rasgo común el uso de un lenguaje deliberadamente ofensivo y una finalidad lúdica. La plataforma estaba compuesta por varios directorios temáticos, dentro de los cuales destacaba el llamado */b/ board*, el más inclasificable de todos. La búsqueda de diversión a toda costa, sin importar sus consecuencias, dio lugar a bromas que traspasaran el ámbito virtual como, por ejemplo, el envío masivo de pizzas o pornografía a personas, grupos o instituciones elegidas únicamente por la expectativa de que sintiesen especialmente molestas u ofendidas.

El foro 4chan, a diferencia de otras plataformas de Internet, no exigía un registro previo para participar o acceder a sus contenidos. Aquellos que optaban por ingresar sin nombre de usuario, eran etiquetados automáticamente por el foro como usuario anónimo. En el caso del directorio */b/ board*, el lugar más activo y proclive a los excesos verbales, el porcentaje de usuarios que decidían no hacerlo alcanzaba el 90%, lo que les llevó a conocerse entre sí como los *anonymous*.

Entre los habituales del foro empezó a ganar fuerza un sector al que los usuarios bautizaron como *moralfags*, los cuales querían añadir algún sentido trascendente o utilidad a las bromas pesadas que periódicamente se organizaban desde esta plataforma. Su propuesta era dirigir estas acciones hacia objetivos a los que consideraban perniciosos para la libertad en Internet o para la propia sociedad.

A principios de 2008 tuvo lugar un acontecimiento que supuso la consolidación de Anonymous como movimiento de hacktivismo. En enero se filtró en Internet un vídeo protagonizado por el actor Tom Cruise donde reflexionaba sobre su experiencia como adepto a la scienciológia. Se trataba de una producción de consumo interno, donde el intérprete estadounidense no salía

especialmente bien parado. El vídeo fue motivo de todo tipo de bromas y sátiras dentro de la comunidad de internautas. Tras la difusión no autorizada de esta grabación, la Iglesia de la Cienciología, como ya había sido habitual en el pasado, empezó a demandar judicialmente a cualquier web o servicio que alojase en sus páginas este vídeo o aprovecharse su difusión para realizar comentarios críticos contra este grupo.

Los «anons» partidarios de conjugar la diversión y cierta conciencia política se organizaron fuera del foro y dirigieron su primera gran ofensiva coordinada (Project Chanology) contra la Iglesia de la Cienciología, a la cual consideraban una peligrosa secta dedicada al lavado de cerebro de sus miembros¹⁹. Además de sabotear algunas de sus webs oficiales, alentaron un boicot global que se trasladó al ámbito físico. Algunos miembros empezaron a protestar en frente de las dependencias de esta Iglesia, pero al hacerlo decidieron ocultar sus rostros para no ser identificados y demandados por los cienciólogos. Acordaron utilizar la máscara de Guy Fawkes, un conspirador inglés del siglo xvi, el cual sirvió de inspiración para un comic y una película con un claro mensaje antisistema llamada *V de Vendetta*. De ese modo nació una estética que se convertiría en el núcleo central de la identidad de Anonymous por encima de cualquier elemento ideológico u objetivo común.

Uno de los más poderosos potenciadores de la actividad de Anonymous fue precisamente la reacción de sus víctimas. Cuando la Iglesia de la Cienciología empezó a ser hostigada, respondió de manera desproporcionada declarando públicamente que eran víctimas de «un grupo de ciber-terroristas[sic] [...] perpetrando crímenes de odio religioso»²⁰. Estas declaraciones divirtieron profundamente a los atacantes, animándoles a seguir por el mismo camino e incitando a otros unirse a esta ofensiva contra lo que consideraban eran una secta detestable que empezaba a perder los nervios.

Uno de los eslóganes más célebres de Anonymous es «Somos legión», una expresión que pretende trasladar a la opinión pública la idea de que sus miembros son innumerables. El propio grupo se encargó de afirmar que no había líderes detrás del movimiento y, por tanto, la detención de algunos de sus activistas no podía neutralizarles. La realidad era bien distinta. En la génesis del grupo y su evolución posterior encontramos apenas cinco *hackers* sobre los cuales orbitó no solo la actividad comunicativa de la organización, sino la ejecución de sus ataques más destacados a lo largo de 2011. El arresto de este núcleo duro supuso el inicio de un periodo de decadencia operativa y de irrelevancia mediática. Aunque son miles los internautas que

¹⁹ ANDERSON, Nate. «Who Was That Masked Man?» [en línea], en *Foreign Policy*. 31 enero 2012. Disponible en web: http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man.

²⁰ SMITH, Stevie. «Scientologists accuse protestors of cyber terrorism» [en línea], en *The Tech Herald*. 11 febrero 2008. Disponible en web: <http://www.thetechherald.com/articles/Scientologists-accuse-protestors-of-cyber-terrorism>.

han frecuentado los chats, foros y redes sociales administradas o inspiradas por Anonymous, la realidad es que solo un pequeño grupo de ellos han sido verdaderos *hackers* con las habilidades necesarias para implementar ciberataques²¹.

La gran mayoría han sido simpatizantes que han consumido y retroalimentado el discurso del grupo a través de Internet, siendo muy heterogéneo su grado de identificación, compromiso e implicación. Algunos frecuentaron estos espacios por curiosidad; otros buscaban una vía de «bajo coste» en términos de esfuerzo y riesgo para dar salida a su frustración o voluntad de transformar la realidad, mientras que tampoco escaseaban los que identificaron una oportunidad para sentirse miembros de un proyecto colectivo, sin importar excesivamente su contenido. Sin embargo, en todos esos casos, la importancia de sus contribuciones fue totalmente secundaria para el éxito de las «operaciones» de Anonymous. No obstante, algunos de los ciberataques más exitosos fueron presentados como el resultado del esfuerzo colaborativo de decenas de miles de internautas que ponían a disposición de las «operaciones» sus habilidades y potencial informático. Para ello, habrían recurrido a herramientas descargadas de los foros del movimiento y ejecutadas de manera coordinada en sus equipos para «tumbear» las webs atacadas. La realidad es que esta participación masiva solo era útil contra objetivos modestos, siendo totalmente ineficaz contra las páginas de grandes compañías concienciadas sobre la necesidad de proteger sus redes. A pesar de ello, este tipo de llamamientos al hackeo colectivo se mantuvo no por necesidades logísticas, sino como un instrumento para lograr la implicación de los seguidores y como recurso propagandístico.

La imagen de sofisticación técnica proyectada por Anonymous no se corresponde necesariamente con las habilidades de sus miembros. Muchos de sus ataques se implementaron llevando a cabo herramientas genéricas de hackeo disponibles en manera abierta en Internet. Las operaciones destinadas al robo de información, aparentemente más complejas, también fueron llevadas a cabo a través de procedimientos simples como las llamadas *inyecciones SQL*, las cuales pueden ser ejecutadas a través de aplicaciones automatizadas gratuitas²².

El verdadero poder de Anonymous residió en la falta de diligencia de sus víctimas, las cuales no habían mantenido medidas de ciberseguridad básicas para evitar ser víctimas de estos sabotajes y robos de datos. Esta deficiente protección era común incluso en grandes empresas cuya principal línea de negocio tenía una base tecnológica. Así, por ejemplo, la compañía japonesa Sony

²¹ OLSON, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. London: Little, Brown and Company, 2012.

²² OLSON, Parmy. "Now Anyone Can Hack a Website Thanks To Clever, Free Programs", *Forbes* (25.04.2012), disponible en: <http://www.forbes.com/sites/parmyolson/2012/04/25/now-anyone-can-hack-a-website-thanks-to-clever-free-programs>.

no nombró a un responsable de ciberseguridad hasta haber sufrido a manos de Anonymous el robo de los datos de los 77 millones de clientes que accedían a su red de juegos *online*, algo que obligó a la firma japonesa a suspender el servicio durante semanas. La deficiente ciberseguridad de algunas de estas empresas no era un dato de acceso público, algo que permitió a Anonymous seguir cultivando una imagen de supremacía técnica. Sin embargo, sus miembros, lejos de dedicarse a desarrollar procedimientos creativos e individualizados para sobrepasar las defensas de sus objetivos, se limitaron a la búsqueda indiscriminada de víctimas que pudiesen ser vulnerables al *software* de hackeo disponible en la red.

A pesar de sus proclamas, los «anons» tampoco eran indetectables ni impunes. El núcleo duro del movimiento fue identificado y detenido en un corto espacio de tiempo a través de medios de investigación convencionales, los cuales se vieron facilitados por la traición de uno de sus miembros más importantes: Hector Xavier Monsegur, alias *Sabu*, el cual actuó como «agente provocador» para el FBI²³. Desde diciembre de 2010 hasta abril de 2012 fueron identificadas, interrogadas o detenidas más de doscientas diez personas relacionadas con Anonymous en doce países distintos²⁴.

Esta realidad llevó a algunos analistas a matizar las valoraciones más alarmistas sobre el peligro que suponía este colectivo. Sus miembros no dejaban de ser unos «grafiteros de Internet»²⁵ cuyas acciones generaban mucho «ruido», pero escasas consecuencias.

Anonymous pasó, en un corto espacio de tiempo, de ser un pequeño grupúsculo de *hackers* con inquietudes políticas a un verdadero movimiento con miles de seguidores repartidos por toda la geografía del planeta. Sin embargo, el atractivo de lo que algunos catalogaron como «el primer movimiento de conciencia *online*» no residía en un relato ideológico persuasivo o en un plan de acción coherente. Más allá de sus poses antisistema que le llevaron a denunciar la manipulación y el sometimiento ciudadano ejercido por parte de Gobiernos y grandes empresas, el ideario de Anonymous era imposible de concretar en propuestas específicas sobre cómo debía organizarse la política, la sociedad o la economía.

²³ ALANDETE, David. «Hacker, líder, insurgente y... topo del FBI» [en línea], en *El País*. 10 marzo 2012. Disponible en web: http://internacional.elpais.com/internacional/2012/03/10/actualidad/1331404002_864490.html; FISHMAN, Steve. «Hello, I Am Sabu...» [en línea], en *New York Magazine*. 3 junio 2012. Disponible en web: <http://nymag.com/news/features/lulzsec-sabu-2012-6/>.

²⁴ PAGET, François. «Hacktivism. Cyberspace has become the new medium for political voices» [en línea], en *White Paper – McAfee Labs*. 2012. Disponible en web: <http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf>.

²⁵ GOLDMAN, David. «Hacker group Anonymous is a nuisance, not a threat» [en línea], en *CNN Money*. 20 enero 2012. Disponible en web: http://money.cnn.com/2012/01/20/technology/anonymous_hack/.

Algunos autores²⁶ han creído detectar en su ideario múltiples matices que coexisten al mismo tiempo y que podrían ser calificados de libertarismo, colectivismo, idealismo, nihilismo, utopismo, distopismo, etc. Sin embargo, por encima de la existencia de una compleja producción doctrinal que requiere interpretación, la realidad es que los diferentes activistas que ejercieron de portavoces o redactaron sus escritos plasmaban sus propios planteamientos y fobias personales, haciendo que el discurso de Anonymous fuese oscilando en función de quién se decidiese a hablar en cada momento en nombre del grupo.

Ni siquiera su lema más importante («Somos legión. No olvidamos. No perdonamos. Espéranos») permitía intuir algo diferente a que eran muchos los que tenían ganas de venganza, pero ni una palabra sobre la razón de esa ira. No existía una estrategia elaborada sobre cuáles eran las prioridades o cómo sus acciones contribuirían al logro de sus fines. Esta confusión les llevó a dirigir sus ataques contra objetivos tan heterogéneos e inconexos como el grupo mexicano de narcos Los Zetas²⁷, los pedófilos de Internet²⁸, las asociaciones de gestión de derechos de autor²⁹, el Gobierno de Israel³⁰ o el Opus Dei.

El ejemplo de Anonymous nos muestra cómo en plena era de la información una iconografía atrayente, aunque carezca de un respaldo ideológico, puede ser un elemento suficiente para lograr una movilización masiva. Muchos de los que se sumaron a los planes de los «anons» lo hicieron atraídos por la estética de un grupo que se identifica con la mitología heroica propia de un cómic: la oportunidad de formar parte de un grupo invisible, omnipotente y omnipresente. Los comunicados en vídeo de los portavoces del grupo ataviados con la máscara de Guy Fawkes y una voz distorsionada a través de ordenador era una imagen perturbadora, pero a la vez fascinante.

Su estructura caótica permitió proyectar una imagen de ubicuidad; sin embargo, esta ausencia de control sobre aquellos que reivindicaban la pertenencia al movimiento también provocó el solapamiento de múltiples grupos

²⁶ GOODE, Luke. «Anonymous and the political ethos of hacktivism», en *Popular Communication*, vol. 13, n.º 1, 2015, pp. 74-86.

²⁷ REXTON KAN, Paul. «Cyber War in the Underworld: Anonymous vs Los Zetas in Mexico» [en línea], en *Yale Journal of International Affairs*. 2013. pp. 40-51. Disponible en web: <http://yalejournal.org/wp-content/uploads/2013/03/Kan.pdf>.

²⁸ STEADMAN, Ian. «Anonymous launches #OpPedoChat, targets paedophiles» [en línea], en *Wired*. 10 julio 2012. Disponible en web: <http://www.wired.co.uk/news/archive/2012-07/10/anonymous-targets-paedophiles>.

²⁹ ROMERO, Pablo. «Así actuó la Policía para identificar a los supuestos 'líderes' de Anonymous» [en línea], en *El Mundo*. 27 junio 2011. Disponible en web: <http://www.elmundo.es/elmundo/2011/06/24/navegante/1308937468.html>.

³⁰ ASSOCIATED PRESS. «'Anonymous' hackers launch cyberattack on Israeli sites» [en línea], en *Fox News*. 7 abril 2013. Disponible en web: <http://www.foxnews.com/tech/2013/04/07/anonymous-hackers-launch-cyberattack-on-israeli-sites/>.

e individuos con agendas contradictorias. Bajo la bandera de Anonymous se congregaron personas que sinceramente creían que debían apoyar los procesos de democratización en cualquier lugar del planeta; otros cuya única inspiración era una destrucción nihilista del mundo tal y como lo conocían. Algunos grupos de ciberdelinquentes sacaron partido de esta ausencia de control para apropiarse de la marca Anonymous y llevar a cabo acciones de chantaje contra empresas. De manera paralela, otros utilizaban de manera ilimitada este nombre para lanzar una serie de amenazas que no se veían respaldadas por ninguna acción y terminaban erosionando la credibilidad del colectivo.

Anonymous ha sido definido de varias formas: como la quintaesencia de una marca «antimarcas»³¹ o como la «marca de acceso abierto»³² que cualquiera podía adoptar y abandonar cuando estimase conveniente. Esta ausencia de responsabilidad sobre su reputación ha generado la contradicción de que algunos miembros deban unir el nombre de Anonymous a algo tan escasamente anónimo como sus respectivos pseudónimos en la red, los cuales sí tienen un historial previo y una posible verificación.

La falta de una mínima estructura organizativa capaz de coordinar el potencial y el trabajo de sus miembros también ha supuesto al movimiento una limitación a la hora de llevar a cabo acciones distintas a las del sabotaje a través de Internet. Cuando Anonymous robó los archivos digitales de la empresa de análisis geopolítico Stratfor³³ no tenía capacidad para sacar partido al contenido de 2,7 millones de correos electrónicos que habían conseguido extraer de sus servidores. Para llevar a cabo la lectura, interpretación y explotación mediática de los escándalos que supuestamente encerraban los intercambios de esta empresa con Gobiernos y empresas de todo el mundo, Anonymous recurrió a los servicios del portal de filtraciones Wikileaks, que bautizó esta colaboración como *Global Intelligence Files*. Sin embargo, la plataforma dirigida por Julian Assange, en buena medida, adolecía de las mismas limitaciones organizacionales y tuvo a su vez que externalizar la labor de análisis con veinticinco medios de comunicación tradicionales. La experiencia no fue demasiado satisfactoria para Anonymous, ya que poco tiempo después anunció públicamente que rompía su acuerdo de colaboración con Wikileaks afirmando: «no podemos

³¹ COLEMAN, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso Books, 2014.

³² PAGET, Francois. «The Future of Hacktivism and Anonymous» [en línea], en *McAfee Blog Central*. 18 enero 2013. Disponible en web: <http://blogs.mcafee.com/mcafee-labs/the-future-of-hacktivism-and-anonymous>.

³³ DURDEN, Tyler. «Intelligence Service Stratfor Suffered a Devastating Hacking Attack Last Night» [en línea], en *Business Insider*. 25 noviembre 2011. Disponible en web: <http://www.businessinsider.com/stratfor-hacked-anonymous-2011-12>.

apoyar más en lo que se ha convertido Wikileaks: en el espectáculo de un solo hombre, Julian Assange»³⁴.

Frustrados por la decreciente atención pública de sus acciones, en 2012 algunos miembros del colectivo pusieron en marcha una iniciativa llamada Par:AnoIA (Potentially Alarming Research: Anonymous Intelligence Agency)³⁵. Se trataba de su propio portal de filtraciones que trataba de cubrir el hueco que había dejado su ruptura con Wikileaks. La plataforma pretendía ampliar el impacto de sus publicaciones masivas de datos, las cuales tenían un impacto mediático fugaz debido a la incapacidad de los medios de comunicación convencionales para explotar un elevado volumen de información. Los creadores de esta iniciativa pretendían explotar el potencial de la *inteligencia colectiva* que reside en el ciberespacio, ofreciendo a los internautas una plataforma para trabajar de manera desestructurada en el análisis de estas filtraciones. Sin embargo, este experimento de *crowdsourcing* no funcionó. La comunidad de internautas que respaldaba las acciones de Anonymous no se mostró muy dispuesta a implicarse en el tedioso trabajo de análisis de los datos, los cuales, en muchos casos, requerían de una elevada cualificación y experiencia para hacer inteligibles dichos documentos. Otro problema añadido era la necesidad de contar con estructuras permanentes de coordinación que fuesen capaces de explotar un conocimiento multidisciplinar que se encontraba disperso. Se trataba, por tanto, de un tipo de organización que chocaba con la propia filosofía antijerarquías del movimiento y que ponía en peligro el anonimato de sus miembros.

Bajo la estela de Anonymous

El principal legado de Anonymous ha sido el haber convertido al hacktivismo en una práctica popular que trasciende el ámbito *hacker*. El *expertise* técnico fue perdiendo relevancia en este tipo de movimientos³⁶ a medida que hizo su aparición un tipo de *software* que permitía llevar a cabo acciones disruptivas sin necesidad de conocer lenguaje de programación.

Por otro lado, la información volvió a situarse en el centro de la estrategia hacktivista: mientras que el sabotaje de las redes y sistemas de sus objetivos eran acciones de gran visibilidad, no dejaban de ser meras contingencias.

³⁴ ASSOCIATED PRESS. «Anonymous rompe relaciones con Assange y WikiLeaks» [en línea], en *La Voz*. 12 octubre 2012. Disponible en web: <http://www.lavoz.com.ar/noticias/tecnologia/anonymous-rompe-relaciones-con-assange-wikileaks>.

³⁵ NORTON, Quinn. «Par:AnoIA: Anonymous Launches WikiLeaks-esque Site for Data Dumps» [en línea], en *Wired*. 3 julio 2012. Disponible en web: <https://www.wired.com/2012/07/paranoia-anonymous/>.

³⁶ HOLT, Thomas J.; FREILICH, Joshua D.; CHERMAK, Steven M. «Exploring the subculture of ideologically motivated cyber-attackers», en *Journal of Contemporary Criminal Justice*, vol. 33, n.º 3, pp. 212-233.

cias temporales. En cambio, la difusión pública de sus datos confidenciales (el contenido de sus correos electrónicos, listas de clientes, contraseñas, datos financieros, etc.) podía erosionar gravemente la reputación de su víctima. Para algunas incluso suponía una amenaza existencial debido a los graves perjuicios económicos o personales que estas filtraciones podían causarle por la pérdida de contratos o posibles demandas judiciales por parte de los afectados.

Anonymous puso en evidencia alguna de las contradicciones de la actual sociedad de la información, donde la sobreabundancia informativa y las demandas de transparencia pública, no han anulado la necesidad que tienen las organizaciones de custodiar y mantener alejados del conocimiento público sus datos más sensibles. La acción de un grupo poco sofisticado demostró lo frágil que puede ser la posición de fuerza que ocupan algunas grandes corporaciones e instituciones públicas. La pérdida de control sobre su propia información, bien por filtraciones originadas desde dentro o por incursiones externas, puede destruir de manera instantánea las expectativas de algunos de los actores más poderosos, e incluso provocar un cambio en las reglas del juego.

Esta es una de las principales aportaciones del polémico legado de Anonymous que han sido replicadas por otros grupos hacktivistas: la apropiación ilícita y divulgación de información sensible puede convertirse en una vía principal de activismo político.

Durante los últimos años, uno de los principales exponentes de este modelo de hacktivismo antisistema ha sido un actor que opera aparentemente a título individual y que ha ganado un elevado prestigio dentro de la subcultura antisistema debido a su pericia técnica y la cuidada selección de sus víctimas.

Es el caso de Phineas Fisher, el cual adquiriría fama internacional tras el filtrado masivo de los datos privados de dos controvertidas compañías: Gamma Group³⁷ y Hacking Team³⁸. Con esta acción pretendía desvelar los oscuros negocios de unas empresas de *software* que proporcionaban herramientas de monitorización de las comunicaciones a todo tipo de clientes, incluyendo regímenes dictatoriales que emplean estos recursos para reprimir a disidentes y periodistas críticos. Phineas, que se definía asimismo como «un anarquista revolucionario» que vivía de la ciberdelincuencia porque no tenía «demasiadas opciones para vivir con dignidad dentro del

³⁷ Cox, Joseph. «A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher» [en línea], en *Motherboard*. 7 agosto 2014. Disponible en web: https://motherboard.vice.com/en_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher.

³⁸ FRANCESCHI-BICCHIERAI, Lorenzo. «The Vigilante Who Hacked Hacking Team Explains How He Did It» [en línea], en *Motherboard*. 15 abril 2016. Disponible en web: https://motherboard.vice.com/en_us/article/3dad3n/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it.

sistema»³⁹, optó por un modelo más selectivo a la hora de orientar sus ataques. Sus objetivos no solo debían tener un elevado perfil mediático, sino también debían ser fácilmente culpabilizados desde la óptica de este movimiento. Esto le llevó también a publicar trescientos mil correos electrónicos del partido político AKP del presidente de Turquía Tayyip Erdogan,⁴⁰ en represalia por los ataques del Gobierno turco a algunas organizaciones kurdas de ideología anticapitalista. También filtraría la identidad de 5540 miembros de la policía autonómica catalana alojados en los servidores del sindicato policial SME como una forma de represalia contra los supuestos abusos policiales y la represión del cuerpo de Mossos d'Escuadra contra el movimiento antisistema en Cataluña⁴¹.

Desde el comienzo de sus actividades, mantuvo una notable actividad comunicativa a través de la administración de perfiles propios en redes sociales, la publicación de un vídeo reivindicativo donde registra de manera didáctica cómo había logrado vulnerar la seguridad de sus objetivos y la concesión de entrevistas a periodistas. Sin embargo, su principal contribución a la promoción del hacktivismo antisistema fue la publicación de dos manuales⁴² con instrucciones detalladas para que cualquier activista pudiese imitar sus acciones de hackeo contra otros objetivos.

El carácter quirúrgico de sus acciones, junto a una mayor sofisticación ideológica y seriedad sobre las causas de su activismo⁴³, le otorgaron una autoridad entre la subcultura *hacker* mucho más elevada que la que fue capaz de cosechar Anonymous.

Sin embargo, la aparición de Phineas en el universo hacktivista fue tan repentina como su desaparición. A comienzos de 2017 tuvo lugar una operación policial en España contra tres individuos a los que se atribuía la respon-

³⁹ FRANCESCHI-BICCHIERAI, Lorenzo. «Hacking Team Hacker Phineas Fisher Is Taking a Break Because of Stress» [en línea], en *Motherboard*. 9 febrero 2017. Disponible en web: https://motherboard.vice.com/en_us/article/xy5enw/hacking-teams-phineas-fisher-will-return-but-only-after-a-break-at-the-beach.

⁴⁰ FRANCESCHI-BICCHIERAI, Lorenzo. «Notorious Hacker 'Phineas Fisher' Says He Hacked The Turkish Government» [en línea], en *Motherboard*. 21 julio 2016. Disponible en web: https://motherboard.vice.com/en_us/article/yp3n55/phineas-fisher-turkish-government-hack.

⁴¹ Cox, Joseph. «A Notorious Hacker Just Released a How-To Video Targeting Police» [en línea], en *Motherboard*. 19 julio 2016. Disponible en web: https://motherboard.vice.com/en_us/article/vv77y9/phineas-fisher-sme.

⁴² «Hack Back! A DIY Guide». Disponible en web: <https://pastebin.com/0SNSvyjJ>; «A DIY Guide for those without the patience to wait for whistleblowers». Disponible en web: <https://pastebin.com/BMb543G9>.

⁴³ FRANCESCHI-BICCHIERAI, Lorenzo. «A Notorious Hacker Is Trying to Start a 'Hack Back' Political Movement» [en línea], en *Motherboard*. 23 mayo 2016. Disponible en web: https://motherboard.vice.com/en_us/article/qkjjnb/notorious-hacker-phineas-fishers-is-trying-to-start-a-hack-back-political-movement.

sabilidad de la filtración de los afiliados al sindicato de Mossos⁴⁴. Aunque se especuló con la posibilidad de que entre los detenidos se encontrase el misterioso Phineas Fisher, este reaparecería en Internet para negar que hubiese sido apresado. A pesar de ello, eliminaría repentinamente sus perfiles en redes sociales e interrumpiría su actividad de hackeo para tomarse un «descanso», como declararía a un periodista. Según esto, su elevado perfil público y, por motivos de seguridad, la necesidad de mantener una doble vida, le habían causado algún tipo de depresión/estrés de la cual esperaba recuperarse. Ante la pregunta del periodista sobre si podía considerarse que Phineas Fisher había muerto, el respondió: «No. Las palabras viven para siempre. Mientras que alguien lea los manuales y se sienta inspirado, seguirá vivo»⁴⁵.

Hactivismo yihadista

Entre el heterogéneo catálogo de usos que el terrorismo yihadista hace de Internet también podemos encontrar el recurso del hactivismo. Un amplio elenco de siglas y actores individuales han recurrido al *hacking* para apoyar los objetivos y tácticas de estas organizaciones.

Este ha sido el principal fruto de su llamamiento para que sus seguidores saquen partido a las potencialidades del ciberespacio en beneficio de la yihad. Así, por ejemplo, en un vídeo de 2011 elaborado por Al Qaeda con el título *No confíes en otros, toma la responsabilidad por ti mismo*⁴⁶, se incitaba a que cualquier musulmán con conocimientos especializados llevase a cabo «en armonía con el plan general de los muyahidín [...] ataques contra los *websites* y las redes electrónicas de las grandes empresas y las administraciones públicas de los países que atacan a musulmanes [...]».

Los foros yihadistas de Internet han sido el principal espacio donde los partidarios de estos grupos han depositado sus esperanzas en que el ciberespacio se convirtiese en el arma definitiva que les permitiría alterar la balanza de fuerzas y vencer así a enemigos mucho más poderosos. Alguno de estos internautas llegó incluso a especular con la posibilidad de que un cibersa-

⁴⁴ BORRÀS, Enric. «Els Mossos arresten tres persones per la filtració de dades personals 5.540 policies» [en línea], en ARA. 1 febrero 2017. Disponible en web: https://www.ara.cat/societat/Arresten-persona-filtracio-mossos-desquadra_0_1733826703.html.

⁴⁵ FRANCESCHI-BICCHIERAI, Lorenzo. «Hacking Team Hacker Phineas Fisher Is Taking a Break Because of Stress» [en línea], en *Motherboard*. 9 febrero 2017. Disponible en web: https://motherboard.vice.com/en_us/article/xy5enw/hacking-teams-phineas-fisher-will-return-but-only-after-a-break-at-the-beach.

⁴⁶ JIHADOLOGY. «As-Sahāb Media presents a new vídeo message from al-Qā'idah: "For Incitement and Publishing: You Are Held Responsible Only for Yourself, Parts 1 and 2"» [en línea], 3 junio 2011. Disponible en web: <http://jihadology.net/2011/06/03/as-sa%E1%B8%A5ab-presents-a-new-v%C3%ADeo-message-from-al-qa%E2%80%99idah-thou-are-held-responsible-only-for-yourself-parts-1-2/>.

botaje contra Estados Unidos diese como resultado el lanzamiento remoto de alguna de sus armas nucleares contra China o Rusia, y que esto fuese el inicio de una guerra que terminaría exterminando a los «enemigos del islam»⁴⁷. A pesar de esas reflexiones en «voz alta», lo cierto es que estos llamamientos no han logrado que ningún partidario con las capacidades necesarias atendiese esta llamada y protagonizase algún acto de ciberterrorismo en sentido estricto. Sí que se ha producido, por el contrario, la activación de ese otro activismo que, aun siendo muy modesto desde el punto de vista técnico, ha generado unos cuantiosos resultados en términos de publicidad y generación de miedo entre sus víctimas.

Es muy significativo que el primer registro existente sobre el uso de Internet desde una perspectiva ofensiva por parte de un yihadista se pueda catalogar como un acto de hacktivismo. Este es el caso del juicio en Estados Unidos contra el mauritano Mohamedou Ould Slahi⁴⁸, un reclutador de Al Qaeda, con experiencia profesional como administrador de sistemas. Según relataría, la organización de Bin Laden llevó a cabo una serie de ciberataques contra redes informáticas gubernamentales en el año 2001. Sin embargo, dichas operaciones se limitaron al sabotaje temporal de páginas web públicas (como la del primer ministro israelí) a través de los llamados *ataques de denegación de servicio*.

A pesar de la existencia a lo largo del tiempo de numerosos incidentes de hacktivismo yihadista, el fenómeno no alcanza su eclosión hasta fechas más recientes. Se trata de un fenómeno tardío que obedece a dos factores principales: su inspiración en el exitoso modelo Anonymous, el cual sería el detonante de un considerable movimiento de hacktivismo pro-alestino en países de mayoría musulmana, y la capacidad del grupo terrorista Estado Islámico para conectar con una nueva generación de partidarios que se desenvuelven con mayor comodidad en el activismo virtual.

Algunos internautas que simpatizaban con el ideario y métodos del terrorismo yihadista extrajeron de la experiencia de Anonymous unas valiosas lecciones sobre cómo alcanzar una elevada notoriedad en los medios de comunicación, pero también cómo era posible importar ese modelo de compromiso de «baja intensidad» con una causa, lo que permitía extender el abanico de contribuciones a la yihad al ámbito del *hacking*.

Este tipo de conexiones entre la subcultura antisistema y la yihadista no solo se han producido en el plano del aprendizaje vicario, sino que también es

⁴⁷ TORRES, Manuel R. «Cómo contener a un califato virtual» [en línea], en JORDÁN, Javier. (coord.) *Estrategias para derrotar al Dáesh y la reestabilización regional*. Madrid: Ministerio de Defensa, 2016. Disponible en web: http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2016/Cuaderno_180.html.

⁴⁸ THE NEW YORK TIMES. «Mohamedou Ould Slahi» [en línea], en *The Guantánamo Docket*. Disponible en web: <https://www.nytimes.com/interactive/projects/guantanamo/detainees/760-mohamedou-ould-slahi>.

posible detectarlas en el perfil biográfico de algunos de sus protagonistas. El caso más destacado es el del británico de origen pakistaní Junaid Hussain. Siendo un adolescente creó junto a un amigo un grupo denominado Team Poison que tendría una clara orientación propalestina. A través de su apodo *Trick* se movería en la órbita de Anonymous, un colectivo con el cual compartiría varias ofensivas de *hacking* como Operation Free Palestine⁴⁹, que apuntó hacia el sistema financiero de Israel en 2011. Team Poison reivindicaría un buen número de acciones de un considerable impacto mediático, como la filtración de datos provenientes de políticos e instituciones gubernamentales. En 2012 sería condenado a seis meses de prisión por el hackeo de la agenda de contactos del asistente del primer ministro británico Tony Blair, así como por realizar más de cien bromas pesadas en la línea de teléfono habilitada por el Gobierno para recibir denuncias contra individuos relacionados con actividades terroristas.

Su paso por prisión intensificó la agresividad contra los que consideraba los responsables de un sistema opresivo que se cebaba especialmente contra los musulmanes. El 2014 reaparecería en los territorios dominados por Estado Islámico en Siria. Junaid había decidido sumarse a la causa de este grupo terrorista y marcó un punto de inflexión en su vida. Alteró su perfil en Twitter para adoptar un nuevo nombre de guerra, Abu Hussain al-Britani, y sustituyó una imagen donde podía verse un niño cubierto con una bandera palestina por una foto personal donde mostraba medio rostro cubierto por un pañuelo mientras apuntaba con un rifle a la cámara. Junaid puso a disposición del grupo sus conocimientos para formar a otros activistas y apoyar las actividades propagandísticas de la organización. Se convertiría asimismo en el operativo más reconocible del grupo más importante del hacktivismo yihadista, el Cibercalifato, el cual protagonizaría varias operaciones de gran resonancia como el hackeo del perfil en Twitter del Comando Central del Ejército de los Estados Unidos (CENTCOM). En paralelo, también lideró otra nueva denominación del hacktivismo yihadista bajo el nombre de Islamic State Hacking Division (ISHD)⁵⁰.

Junaid trató de potenciar las actividades de su nuevo grupo rentabilizando su antigua red de contactos entre el hacktivismo antisistema. Uno de los pocos activistas que aceptó su oferta fue el kosovar Ardit Ferizi⁵¹, líder de un

⁴⁹ ANONYMOUS. «A message from Anonymous to the Israeli government and the Zionist establishment» [en línea]. Disponible en web: <https://www.anonymous-france.eu/anonymous-operation-free-palestine.html>.

⁵⁰ FRANCESCHI-BICCHIERAI, Lorenzo. «How a Teenage Hacker Became the Target of a US Drone Strike» [en línea], en *Motherboard*. 28 agosto 2015. Disponible en web: https://motherboard.vice.com/en_us/article/jp5wed/junaid-hussain-isis-hacker-drone.

⁵¹ VARANDANI, Suman. «Who Is Ardit Ferizi? Malaysia Arrests Kosovo National For Hacking US Security Data For ISIS» [en línea], en *International Business Times*. 16 octubre 2015. Disponible en web: <http://www.ibtimes.com/who-ardit-ferizi-malaysia-arrests-kosovo-national-hacking-us-security-data-isis-2143489>.

grupúsculo denominado Kosova Hacker's Security. El yihadista le encargó la obtención de un listado con información personal de militares y funcionarios estadounidenses. El kosovar le facilitaría más de mil datos de contacto, los cuales fueron difundidos en Internet por Cyber Caliphate junto a un llamamiento público para que fuesen asesinados. La pobre diligencia técnica⁵² de Ferizi facilitaría su detención poco tiempo después.

Abu Hussain al-Britani no solo sería conocido por su faceta virtual, sino que también protagonizaría una intensa actividad destinada a alentar la realización de atentados en Occidente por parte de musulmanes radicalizados con los que había entrado en contacto a través de Internet⁵³.

El 24 de agosto de 2015, el disparo de un dron militar de los Estados Unidos acabaría con su vida en la ciudad siria de Raqqa. Tras su muerte, varios colectivos de *hacker* opuestos a Estado Islámico (entre los que se encontraban antiguos camaradas de Junaid) se disputaron la responsabilidad de haber desvelado la localización del más famoso ciberactivista de Estado Islámico, haciendo así posible su muerte.

Su desaparición supone una nueva evidencia de la importancia del factor individual en los movimientos hacktivistas. Tras su muerte, Cyber Caliphate cambió su nombre por Islamic Cyber Army; sin embargo, en esta nueva fase se podía apreciar fácilmente una pérdida de capacidades en cuanto a sus procedimientos y selección de objetivos⁵⁴.

A pesar de ello, el yihadismo continúa siendo uno de los principales motores del hacktivismo. El elemento diferenciador se halla en su vinculación ideológica con los grupos e individuos que emplean la violencia terrorista, lo que otorga un nuevo sentido a muchas de sus actividades. Así, por ejemplo, el robo y difusión de información personal (o *doxxing*) no tiene como finalidad exclusiva atacar la intimidad de la víctima, sino el emplear esa información para crear *kill lists* donde se facilita la localización de personas a las que se presenta como candidatos propicios a ser asesinados. Este tipo de amenazas les otorga una enorme relevancia pública, teniendo en cuenta que se producen en un contexto de elevada ansiedad por la incidencia del terrorismo en todo el planeta. A pesar de que la gran mayoría de las siglas proyihadistas que han emergido en los últimos años carecen de vinculación

⁵² UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA. «Criminal Complaint United States of America v. Ardit Ferizi» [en línea]. Disponible en web: <https://www.justice.gov/opa/file/784501/download>.

⁵³ NEWSWEEK. «Junaid Hussain: How a Boy From Birmingham Became ISIS's Leading Hacker» [en línea], en *Newsweek*. 27 agosto 2015. Disponible en web: <http://www.newsweek.com/junaid-hussain-isis-us-syriabritainisis-cybercyber-caliphateisis-hackermiddle-601034>.

⁵⁴ MURPHY, Lorraine. «The Curious Case of the Jihadist Who Started Out as a Hacktivist» [en línea], en *Vanity Fair*. 15 diciembre 2015. Disponible en web: <https://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain>.

efectiva con los grupos que emplean la violencia⁵⁵, su adhesión ideológica les ha permitido disfrutar de un acceso a la opinión pública que difícilmente se hubiese dado en otras causas que no estén respaldadas por las armas.

Un análisis detallado de estas «listas»⁵⁶ evidencia no solo la existencia de datos «fabricados», sino que en las que son genuinas también se aprecia un pobre bagaje técnico, así como un muy cuestionable criterio de selección de los objetivos. En unos casos, el acceso a este tipo de datos personales se ha logrado a través de simples métodos de ingeniería social a través de la impostación de identidades. En los casos más elaborados, se ha hecho uso de herramientas fácilmente accesibles como Havij u otro tipo de plataformas que automatizan las llamadas *inyecciones SQL*, las cuales permiten capturar los datos de acceso restringido de las webs que presentan graves deficiencias de seguridad⁵⁷. Por otro lado, si en las primeras *kill list* se podía deducir cierta lógica en la culpabilización y en la selección de las víctimas (personal militar, policial, personal gubernamental, etc.), en aportaciones posteriores se incluyó de manera indiscriminada a residentes de cualquier ciudad occidental, por la única razón de que sus datos estaban disponibles de manera semipública en listines telefónicos a los que había tenido acceso estos grupos.

A pesar de este carácter *amateur*, las distintas organizaciones yihadistas no han estado especialmente interesadas en resolver la ambigüedad existente sobre sus posibles vínculos con los grupos de *hackers*. Estos grupos son conscientes de su capacidad para amplificar el terror entre sus enemigos, de ahí que, en vez de aclarar de manera explícita que estos actores no forman parte de su estructura organizativa, han preferido hacerlo de manera más sutil. Así, por ejemplo, Estado Islámico ha hecho varios llamamientos a sus seguidores para que solo atribuyan al grupo la información proveniente de fuentes oficiales y, acto seguido, han informado de cuáles eran esos canales oficiales, entre los cuales no se haya ninguno de los utilizados por estos grupos para divulgar sus mensajes.

El hacktivismo yihadista se mueve en los mismos parámetros culturales que otros grupos de ciberactivismo que recurren a técnicas delictivas, lo que le permite que se produzcan sinergias sorprendentes⁵⁸. Así, por ejemplo,

⁵⁵ KING, Meg; GRAYSON, Clary. «Confronting Terror-affiliated Hacktivists» [en línea], en *Wilson Briefs*. 28 mayo 2015. Disponible en web: <https://www.wilsoncenter.org/publication/confronting-terror-affiliated-hacktivists>.

⁵⁶ SITE INTELLIGENCE GROUP. «Kill Lists from Pro-ISIS Hacking Groups» [en línea], en *SITE*, 7 junio 2016. Disponible en web: http://sitemultimedia.org/docs/SITE_Analysis_of-Islamic_State_Kill_Lists.pdf.

⁵⁷ BERNARD, Rose. «These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State», en *Journal of Cyber Policy*, vol. 2, n.º 2, 2017, pp. 255-265.

⁵⁸ STALINSKY, Steven; SOSNOW, R. «Hacking In The Name Of The Islamic State (ISIS)» [en línea], en *MEMRI Inquiry & Analysis Series n.º 1183*. 21 agosto 2015. Disponible en web: https://www.memri.org/reports/hacking-name-islamic-state-isis#_ednref7.

encontramos grupos que iniciaron su andanza como movimientos antiautoritarios o antisemitas en países de mayoría musulmana, que no poseían ningún objetivo de carácter religioso y que terminaron derivando hacia el hacktivismo yihadista. La estela del «caballo ganador» puede ser un movilizador mucho más importante, que la identificación ideológica o religiosa, especialmente cuando se comparte un mismo conjunto de odios y fobias hacia los que se consideran enemigos. En otros casos, encontramos actores que identifican el yihadismo (y particularmente el Estado Islámico) como una poderosa marca que garantiza impacto mediático y cierta respetabilidad y prestigio a sus acciones individuales de *hacking*. Esto explica, por ejemplo, cómo algunos individuos y grupúsculos de la escena *hacker* en América Latina terminasen orbitando hacia el hacktivismo proyihadista⁵⁹.

A pesar de la grandiosidad con la que describen sus capacidades técnicas y objetivos⁶⁰, el grueso de sus acciones se ha ceñido a simples ataques en fuerza contra algunas páginas web escasamente protegidas. En ocasiones, sus sabotajes contra aquellos contenidos virtuales que consideran ofensivos desde una perspectiva islámica se han implementado a través de procedimientos carentes de cualquier componente técnico, como la obtención de las contraseñas atacadas a través de ingeniería social o incluso el envío de mensajes amenazantes a las empresas que prestan servicios de alojamiento virtual, para forzarlas a descolgar estos contenidos del ciberespacio. En otros casos, se han limitado a escanear de manera automatizada vulnerabilidades en páginas web que les permitan tomar el control sobre ellas y llevar a cabo acciones de *defacement*, a través de las cuales publicitar las consignas de las diferentes organizaciones yihadistas. Sin embargo, que el principal criterio de selección de la víctima sea su accesibilidad ha llevado a muchos de estos actores a sabotear webs cuyo contenido difícilmente guarda alguna relación con esa supuesta pugna entre el Islam y sus enemigos. Así, por ejemplo, algunas de las víctimas de esta ofensiva han sido restaurantes, gimnasios, colegios o incluso asociaciones de taxistas⁶¹.

Esta selección arbitraria de objetivos ha erosionado el poder coactivo de estos actores, así como su capacidad de concitar la atención de los medios de comunicación de masas. Si bien las primeras acciones obtuvieron un elevado eco mediático, el hacktivismo yihadista terminó agotando rápidamente

⁵⁹ CCN-CERT. «Hacktivismo y Ciberyihadismo Informe Resumen 2016», en *Informe de Amenazas CCN-CERT IA-04/17*. Marzo de 2017.

⁶⁰ Véase, por ejemplo: <https://ia801309.us.archive.org/9/items/MessageToAmerica-MessageFromTheVirtualWorldandEuropeAustralia/Message%20to%20America%20Message%20From%20The%20Virtual%20World%20%28and%20Europe%2c%20Australia%29.mp4>.

⁶¹ CEMBRERO, Ignacio. «Un ciberataque yihadista tumba las webs de tres liceos franceses en España» [en línea], en *El Confidencial*. 11 enero 2017. Disponible en web: https://www.elconfidencial.com/espana/2017-01-11/ciberataque-yihadista-liceos-webs-paginas_1314725/.

ese crédito cuando dejaron patente el carácter arbitrario y sin respaldo real de sus amenazas.

Otro elemento que ha minado el crédito de este tipo de actores ha sido su escasa coherencia doctrinal e incluso estética. Su discurso y la simbología están plagados de elementos que entran en contradicción con los planteamientos doctrinales de los grupos a los que pretenden apoyar con sus acciones. En la subcultura del hacktivismo yihadista pesa mucho más la estética que terminaría popularizando Anonymous que el rigorismo de Estado Islámico, el cual cataloga gran parte de esas manifestaciones como influencias pecaminosas ajenas al verdadero islam. Es el caso, por ejemplo, del grupo tunecino denominado Al Fallaga Team, el cual, a pesar de estar alineado con los objetivos del Dáesh, siguió conservando en su emblema la bandera de Túnez. Este símbolo choca frontalmente con el rechazo del salafismo yihadista a la existencia de comunidades nacionales, a las cuales considera una creación de Occidente para dividir y enfrentar a los musulmanes, los cuales forman una única comunidad que debe ser regida bajo la forma del califato.

En las representaciones visuales de estos grupúsculos⁶² e individuos no solo es recurrente la máscara del Guy Fawkes, sino otra serie de imágenes aún más problemáticas que la del *merchandising* moderno de este conspirador católico del siglo xvi: podemos encontrar, por ejemplo, calaveras, fantasmas e incluso demonios. Al mismo tiempo, se obvia la pugna existente entre las organizaciones de Al Qaeda y Estado Islámico, cuyos nombres y símbolos han aparecido de manera indistinta en algunas de estas acciones de sabotaje de páginas web⁶³.

Otro elemento que ha restado eficacia a la acción comunicativa del hacktivismo yihadista es su carácter disperso: a pesar de compartir objetivos y metodología, los activistas de la yihad cibernética se han empeñado en agruparse en multitud de siglas y alianzas efímeras que dificultan en extremo el acto de catalogar y comprender a sus protagonistas. Para añadir más complejidad, algunos de estos grupos han utilizado de manera indistinta varias combinaciones de un mismo nombre; es el caso de Caliphate Cyber Army (CCA), que también se hacía llamar Islamic Cyber Army o Cyber Caliphate. Han creado nuevas marcas que supuestamente fusionaban grupos preexistentes, lo cual no implicaba que sus componentes no siguiesen existiendo y actuando a título individual. Es el caso de United Cyber Caliphate (UCC), presentado públicamente en abril de 2016 como la unión de tres grupos: Kalachnikov E-security Team, Sons Caliphate Army y Ghost Caliphate Section. Cuando se han agregado o escindido a título individual algunos de estos grupos, nunca ha quedado claro cuáles son los factores que motivaban estos

⁶² Véase, por ejemplo: ICT Cyber-Desk. «Cyber-Terrorism Activities Report No. 15» [en línea]. 2015. Disponible en web: <https://www.ict.org.il/UserFiles/ICT-Cyber-Review-15.pdf>.

⁶³ Es el caso, por ejemplo, de un grupo autodenominado Al Qaeda Electronic Base, el cual empleaba como símbolo la bandera de Estado Islámico. Véase: https://justpaste.it/qe_b2.

continuos movimientos de refundación, unión o separación. Desde la óptica de un observador externo, era inevitable percibir el hacktivismo yihadista como un ámbito dominado por las rivalidades individuales, la incapacidad de cooperar y la inmadurez de sus protagonistas.

Conclusiones

En el ámbito de la ciberseguridad estamos viviendo un momento de «cierre de etapa». Gran parte de las acciones de *hacking* que se han producido en los últimos años ha sido posible no tanto por la sofisticación técnica de sus autores, sino por la falta de preparación y las inadecuadas defensas de sus víctimas. Dicha ventana de oportunidad ha sido explotada con escasa discreción por parte de actores públicos y privados, lo que ha terminado generando entre sus víctimas una respuesta de adaptación que está limitando su efectividad. A medida que Internet se vaya «endureciendo» como objetivo, los grupos que recurren al hacktivismo tendrán que innovar en sus procedimientos para seguir obteniendo relevancia mediática.

Sin embargo, este cambio no supondrá el fin de las grandes filtraciones de datos ni de los sabotajes virtuales. Aunque estos resultados resulten más difíciles de alcanzar desde un punto de vista técnico, es previsible que se produzca una mayor implicación en términos de esfuerzo por parte de los protagonistas, sobre todo en la medida en que el activismo político convencional parezca cada vez más ineficaz frente a otras modalidades transgresoras que obtiene un impacto mediático mucho más elevado.

El futuro del hacktivismo está intimamente vinculado al cambio tecnológico y a su recepción por parte de la sociedad. Si por un lado una mayor concienciación pública sobre la necesidad de la ciberseguridad hará obsoletos algunos de los procedimientos tradicionales, debe contemplarse la posibilidad de que la irrupción de nuevas tecnologías abra nuevas ventanas de oportunidad. Ese es el escenario que podría plantearse como consecuencia de la popularización de aplicaciones basadas en inteligencia artificial, las cuales pueden hacer viables determinados objetivos y procedimientos que hasta ahora no han sido asumibles por su elevado coste en términos de movilización de recursos humanos o por la necesidad de conocimiento especializado⁶⁴.

Es el caso, por ejemplo, de los engaños individualizados a través de la suplantación de identidad (*spear phishing attacks*) con el propósito de acceder a información confidencial. El éxito de estos ataques depende de una considerable inversión de tiempo y esfuerzo para poder identificar así el objetivo,

⁶⁴ BRUNDAGE, Miles et al. «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» [en línea], en *Future of Humanity Institute- Oxford University*. Febrero 2018. Disponible en web: <https://maliciousaireport.com/>.

su red social y el contexto en el cual la víctima daría credibilidad y estaría dispuesta a aceptar una petición que la sitúa en una situación de vulnerabilidad. La considerable inversión en tiempo y esfuerzo que debe realizarse para hacer viable este tipo de engaños explica que hasta el momento se haya reservado a objetivos de alto valor. Sin embargo, la inteligencia artificial puede hacer posible que las tareas de investigación del objetivo puedan ser automatizadas, lo que reducirá drásticamente el coste de este tipo de prácticas. Como resultado, se podrá lanzar de manera indiscriminada este tipo de ataques sin que por ello resulten menos eficaces.

Sin embargo, el principal reto al que tiene que enfrentarse el hacktivismo no es tanto la viabilidad de sus operaciones de hackeo, sino cómo conciliar su vertiente colectiva con la individualidad de sus miembros.

Uno de los principales activos propagandísticos de estos actores es el hecho de que sean percibidos por la sociedad como movimientos capaces de movilizar a un elevado número de activistas. Su discurso alcanza una resonancia distinta cuando su público interpreta que tras las palabras se encuentra una masa amorfa de entusiastas expertos informáticos a los que resulta imposible descabezar. Sin embargo, esta imagen no hace justicia a la realidad del hacktivismo, donde los números no solo son mucho más reducidos, sino donde las individualidades dificultan la capacidad de estos movimientos de actuar como un actor homogéneo. Muchos de los miembros que se suman a estas formaciones lo hacen desde una trayectoria previa, portando consigo una reputación individual de dominio técnico, osadía o compriso. Se trata de un patrimonio inmaterial del cual muchos no quieren desprenderse, sobre todo, si entiende que su militancia en estos proyectos es solo temporal. De ahí que cuando estos grupos reivindicar sus acciones sea frecuente que, junto con el nombre del grupo, aparezcan también mencionados los seudónimos de sus activistas que han llevado a cabo la acción, los cuales no están dispuestos a perder la oportunidad de incrementar su reputación. Esto no solo es una contradicción en los términos para movimientos que, como Anonymous, hacen bandera de cómo sus integrantes conforman una mentalidad colectiva, sino también para el hacktivismo yihadista, el cual tiene dificultades para presentarse como la vanguardia tecnológica de los muyahidín, sobre todo si el ego y el deseo de visibilidad de sus integrantes eclipsa al propio grupo.

En definitiva, la viabilidad futura del hacktivismo dependerá no tanto de su eficacia mediática, la cual ha quedado demostrada a lo largo de los últimos años, sino de la capacidad de sus protagonistas para superar los considerables desafíos organizativos. En la medida en que movimientos de hacktivismo actuales y futuros consigan coordinar y dar coherencia a este heterogéneo colectivo, hablaremos de actores con capacidad real de influencia o de meras erupciones temporales sin impacto en la realidad.

Composición del grupo de trabajo

Coordinador de la obra:

D. Leandro Esteban Villamor

Adjunto civil al director del Centro Superior de Estudios de la Defensa Nacional (CESEDEN)

Vocal y secretario:

D. Federico Aznar Fernández-Montesinos

Capitan de Fragata de la Armada

Analista principal del Instituto Español de Estudios Estratégicos (IEEE)

Vocales:

D. Alfonso Merlos

Periodista

D^a. Eva Moya Losada

Analista de Inteligencia OSINT. Especialización en redes sociales para seguridad y defensa

D. Javier Lesaca Esquiroz

Consultor e investigador visitante de la Universidad George Washington

D. Manuel Ricardo Torres Soriano

Profesor de la Universidad Pablo de Olavide

Cuadernos de Estrategia

- 01 La industria alimentaria civil como administradora de las FAS y su capacidad de defensa estratégica
- 02 La ingeniería militar de España ante el reto de la investigación y el desarrollo en la defensa nacional
- 03 La industria española de interés para la defensa ante la entrada en vigor del Acta Única
- 04 Túnez: su realidad y su influencia en el entorno internacional
- 05 La Unión Europea Occidental (UEO) (1955-1988)
- 06 Estrategia regional en el Mediterráneo Occidental
- 07 Los transportes en la raya de Portugal
- 08 Estado actual y evaluación económica del triángulo España-Portugal-Marruecos
- 09 Perestroika y nacionalismos periféricos en la Unión Soviética
- 10 El escenario espacial en la batalla del año 2000 (I)
- 11 La gestión de los programas de tecnologías avanzadas
- 12 El escenario espacial en la batalla del año 2000 (II)
- 13 Cobertura de la demanda tecnológica derivada de las necesidades de la defensa nacional

- 14 Ideas y tendencias en la economía internacional y española
- 15 Identidad y solidaridad nacional
- 16 Implicaciones económicas del Acta Única 1992
- 17 Investigación de fenómenos belígenos: método analítico factorial
- 18 Las telecomunicaciones en Europa, en la década de los años 90
- 19 La profesión militar desde la perspectiva social y ética
- 20 El equilibrio de fuerzas en el espacio sur europeo y mediterráneo
- 21 Efectos económicos de la unificación alemana y sus implicaciones estratégicas
- 22 La política española de armamento ante la nueva situación internacional
- 23 Estrategia finisecular española: México y Centroamérica
- 24 La Ley Reguladora del Régimen del Personal Militar Profesional (cuatro cuestiones concretas)
- 25 Consecuencias de la reducción de los arsenales militares negociados en Viena, 1989. Amenaza no compartida
- 26 Estrategia en el área iberoamericana del Atlántico Sur
- 27 El Espacio Económico Europeo. Fin de la Guerra Fría
- 28 Sistemas ofensivos y defensivos del espacio (I)
- 29 Sugerencias a la Ley de Ordenación de las Telecomunicaciones (LOT)
- 30 La configuración de Europa en el umbral del siglo XXI
- 31 Estudio de «inteligencia operacional»
- 32 Cambios y evolución de los hábitos alimenticios de la población española
- 33 Repercusiones en la estrategia naval española de aceptarse las propuestas del Este en la CSBM, dentro del proceso de la CSCE
- 34 La energía y el medio ambiente
- 35 Influencia de las economías de los países mediterráneos del norte de África en sus respectivas políticas defensa
- 36 La evolución de la seguridad europea en la década de los 90
- 37 Análisis crítico de una bibliografía básica de sociología militar en España. 1980-1990
- 38 Recensiones de diversos libros de autores españoles, editados entre 1980-1990, relacionados con temas de las Fuerzas Armadas
- 39 Las fronteras del mundo hispánico
- 40 Los transportes y la barrera pirenaica

- 41 Estructura tecnológica e industrial de defensa, ante la evolución estratégica del fin del siglo XX
- 42 Las expectativas de la I+D de defensa en el nuevo marco estratégico
- 43 Costes de un ejército profesional de reclutamiento voluntario. Estudio sobre el Ejército profesional del Reino Unido y (III)
- 44 Sistemas ofensivos y defensivos del espacio (II)
- 45 Desequilibrios militares en el Mediterráneo Occidental
- 46 Seguimiento comparativo del presupuesto de gastos en la década 1982-1991 y su relación con el de Defensa
- 47 Factores de riesgo en el área mediterránea
- 48 Las Fuerzas Armadas en los procesos iberoamericanos de cambio democrático (1980-1990)
- 49 Factores de la estructura de seguridad europea
- 50 Algunos aspectos del régimen jurídico-económico de las FAS
- 51 Los transportes combinados
- 52 Presente y futuro de la conciencia nacional
- 53 Las corrientes fundamentalistas en el Magreb y su influencia en la política de defensa
- 54 Evolución y cambio del este europeo
- 55 Iberoamérica desde su propio sur. (La extensión del Acuerdo de Libre Comercio a Sudamérica)
- 56 La función de las Fuerzas Armadas ante el panorama internacional de conflictos
- 57 Simulación en las Fuerzas Armadas españolas, presente y futuro
- 58 La sociedad y la defensa civil
- 59 Aportación de España en las cumbres iberoamericanas: Guadalajara 1991-Madrid 1992
- 60 Presente y futuro de la política de armamentos y la I+D en España
- 61 El Consejo de Seguridad y la crisis de los países del Este
- 62 La economía de la defensa ante las vicisitudes actuales de las economías autonómicas
- 63 Los grandes maestros de la estrategia nuclear y espacial
- 64 Gasto militar y crecimiento económico. Aproximación al caso español
- 65 El futuro de la Comunidad Iberoamericana después del V Centenario
- 66 Los estudios estratégicos en España
- 67 Tecnologías de doble uso en la industria de la defensa

- 68 Aportación sociológica de la sociedad española a la defensa nacional
- 69 Análisis factorial de las causas que originan conflictos bélicos
- 70 Las conversaciones internacionales Norte-Sur sobre los problemas del Mediterráneo Occidental
- 71 Integración de la red ferroviaria de la península ibérica en el resto de la red europea
- 72 El equilibrio aeronaval en el área mediterránea. Zonas de irradiación de poder
- 73 Evolución del conflicto de Bosnia (1992-1993)
- 74 El entorno internacional de la Comunidad Iberoamericana
- 75 Gasto militar e industrialización
- 76 Obtención de los medios de defensa ante el entorno cambiante
- 77 La Política Exterior y de Seguridad Común (PESC) de la Unión Europea (UE)
- 78 La red de carreteras en la península ibérica, conexión con el resto de Europa mediante un sistema integrado de transportes
- 79 El derecho de intervención en los conflictos
- 80 Dependencias y vulnerabilidades de la economía española: su relación con la defensa nacional
- 81 La cooperación europea en las empresas de interés de la defensa
- 82 Los cascos azules en el conflicto de la ex-Yugoslavia
- 83 El sistema nacional de transportes en el escenario europeo al inicio del siglo XXI
- 84 El embargo y el bloqueo como formas de actuación de la comunidad internacional en los conflictos
- 85 La Política Exterior y de Seguridad Común (PESC) para Europa en el marco del Tratado de no Proliferación de Armas Nucleares (TNP)
- 86 Estrategia y futuro: la paz y seguridad en la Comunidad Iberoamericana
- 87 Sistema de información para la gestión de los transportes
- 88 El mar en la defensa económica de España
- 89 Fuerzas Armadas y sociedad civil. Conflicto de valores
- 90 Participación española en las fuerzas multinacionales
- 91 Ceuta y Melilla en las relaciones de España y Marruecos
- 92 Balance de las primeras cumbres iberoamericanas
- 93 La cooperación hispano-franco-italiana en el marco de la PESC

- 94 Consideraciones sobre los estatutos de las Fuerzas Armadas en actividades internacionales
- 95 La unión económica y monetaria: sus implicaciones
- 96 Panorama estratégico 1997/98
- 97 Las nuevas Españas del 98
- 98 Profesionalización de las Fuerzas Armadas: los problemas sociales
- 99 Las ideas estratégicas para el inicio del tercer milenio
- 100 Panorama estratégico 1998/99
- 100-B 1998/99 Strategic Panorama
- 101 La seguridad europea y Rusia
- 102 La recuperación de la memoria histórica: el nuevo modelo de democracia en Iberoamérica y España al cabo del siglo XX
- 103 La economía de los países del norte de África: potencialidades y debilidades en el momento actual
- 104 La profesionalización de las Fuerzas Armadas
- 105 Claves del pensamiento para la construcción de Europa
- 106 Magreb: percepción española de la estabilidad en el Mediterráneo, perspectiva hacia el 2010
- 106-B Maghreb: perception espagnole de la stabilité en Méditerranée, prospective en vue de L'année 2010
- 107 Panorama estratégico 1999/2000
- 107-B 1999/2000 Strategic Panorama
- 108 Hacia un nuevo orden de seguridad en Europa
- 109 Iberoamérica, análisis prospectivo de las políticas de defensa en curso
- 110 El concepto estratégico de la OTAN: un punto de vista español
- 111 Ideas sobre prevención de conflictos
- 112 Panorama Estratégico 2000/2001
- 112-B Strategic Panorama 2000/2001
- 113 Diálogo mediterráneo. Percepción española
- 113-B Le dialogue Méditerranéen. Une perception espagnole
- 114 Aportaciones a la relación sociedad - Fuerzas Armadas en Iberoamérica
- 115 La paz, un orden de seguridad, de libertad y de justicia
- 116 El marco jurídico de las misiones de las Fuerzas Armadas en tiempo de paz
- 117 Panorama Estratégico 2001/2002

- 117-B 2001/2002 Strategic Panorama
- 118 Análisis, estrategia y prospectiva de la Comunidad Iberoamericana
- 119 Seguridad y defensa en los medios de comunicación social
- 120 Nuevos riesgos para la sociedad del futuro
- 121 La industria europea de defensa: presente y futuro
- 122 La energía en el espacio euromediterráneo
- 122-B L'énergie sur la scène euroméditerranéenne
- 123 Presente y futuro de las relaciones cívico-militares en Hispanoamérica
- 124 Nihilismo y terrorismo
- 125 El Mediterráneo en el nuevo entorno estratégico
- 125-B The Mediterranean in the New Strategic Environment
- 126 Valores, principios y seguridad en la comunidad iberoamericana de naciones
- 127 Estudios sobre inteligencia: fundamentos para la seguridad internacional
- 128 Comentarios de estrategia y política militar
- 129 La seguridad y la defensa de la Unión Europea: retos y oportunidades
- 130 El papel de la inteligencia ante los retos de la seguridad y defensa internacional
- 131 Crisis locales y seguridad internacional: El caso haitiano
- 132 Turquía a las puertas de Europa
- 133 Lucha contra el terrorismo y derecho internacional
- 134 Seguridad y defensa en Europa. Implicaciones estratégicas
- 135 La seguridad de la Unión Europea: nuevos factores de crisis
- 136 Iberoamérica: nuevas coordenadas, nuevas oportunidades, grandes desafíos
- 137 Irán, potencia emergente en Oriente Medio. Implicaciones en la estabilidad del Mediterráneo
- 138 La reforma del sector de seguridad: el nexo entre la seguridad, el desarrollo y el buen gobierno
- 139 Security Sector Reform: the Connection between Security, Development and Good Governance
- 140 Impacto de los riesgos emergentes en la seguridad marítima
- 141 La inteligencia, factor clave frente al terrorismo internacional
- 142 Del desencuentro entre culturas a la Alianza de Civilizaciones. Nuevas aportaciones para la seguridad en el Mediterráneo

- 143 El auge de Asia: implicaciones estratégicas
- 144 La cooperación multilateral en el Mediterráneo: un enfoque integral de la seguridad
- 145 La Política Europea de Seguridad y Defensa (PESD) tras la entrada en vigor del Tratado de Lisboa
- 145-B The European Security and Defense Policy (ESDP) after the entry into Force of the Lisbon Treaty
- 146 Respuesta europea y africana a los problemas de seguridad en África
- 146-B European and African Response to Security Problems in Africa
- 147 Los actores no estatales y la seguridad internacional: su papel en la resolución de conflictos y crisis
- 148 Conflictos, opinión pública y medios de comunicación. Análisis de una compleja interacción
- 149 Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio
- 150 Seguridad, modelo energético y cambio climático
- 151 Las potencias emergentes hoy: hacia un nuevo orden mundial
- 152 Actores armados no estables: retos a la seguridad
- 153 Proliferación de ADM y de tecnología avanzada
- 154 La defensa del futuro: innovación, tecnología e industria
- 154-B The Defence of the Future: Innovation, Technology and Industry
- 155 La Cultura de Seguridad y Defensa. Un proyecto en marcha
- 156 El gran Cáucaso
- 157 El papel de la mujer y el género en los conflictos
- 157-B The role of woman and gender in conflicts
- 158 Los desafíos de la seguridad en Iberoamérica
- 159 Los potenciadores del riesgo
- 160 La respuesta del derecho internacional a los problemas actuales de la seguridad global
- 161 Seguridad alimentaria y seguridad global
- 161-B Food security and global security
- 162 La inteligencia económica en un mundo globalizado
- 162-B Economic intelligence in global world
- 163 Islamismo en (r)evolución: movilización social y cambio político
- 164 Afganistán después de la ISAF
- 165 España ante las emergencias y catástrofes. Las Fuerzas Armadas en colaboración con las autoridades civiles

- 166 Energía y Geoestrategia 2014
- 166-B Energy and Geostrategy 2014
- 167 Perspectivas de evolución futura de la política de seguridad y defensa de la UE. Escenarios de crisis
- 167-B Prospects for the future evolution of the EU's security and defence policy. Crisis scenarios
- 168 Evolución del mundo árabe: tendencias
- 169 Desarme y control de armamento en el siglo xxi: limitaciones al comercio y a las transferencias de tecnología
- 170 El sector espacial en España. Evolución y perspectivas
- 171 Cooperación con Iberoamérica en materia de defensa
- 172 Cuadernos de Estrategia 172 Cultura de Seguridad y Defensa: fundamentos y perspectivas de mejora
- 173 La internacional yihadista
- 174 Economía y geopolítica en un mundo globalizado
- 175 Industria Española de Defensa. Riqueza, tecnología y seguridad
- 176 Shael 2015, origen de desafíos y oportunidades
- 177 UE-EE.UU.: Una relación indispensable para la paz y la estabilidad mundiales
- 178 Rusia bajo el liderazgo de Putin. La nueva estrategia rusa a la búsqueda de su liderazgo regional y el reforzamiento como actor global.
- 179 Análisis comparativo de las capacidades militares españolas con las de los países de su entorno
- 180 Estrategias para derrotar al Dáesh y la reestabilización regional
- 181 América Latina: nuevos retos en seguridad y defensa
- 182 La colaboración tecnológica entre la universidad y las Fuerzas Armadas
- 183 Política y violencia: comprensión teórica y dearrollo en la acción colectiva
- 184 Una estrategia global de la Unión Europea para tiempos difíciles
- 185 Ciberseguridad: lal cooperación público-privada
- 186 El agua: ¿fuente de conflicto o cooperación?
- 187 Geoeconomías del siglo xxi
- 188 Seguridad global y derechos fundamentales
- 189 El posconflicto colombiano: una perspectiva transversal
- 190 La evolución de la demografía y su incidencia en la defensa y seguridad nacional
- 190-B The evolution of demography and its impact on defense and national security

191	OTAN: presente y futuro
192	Hacia una estrategia de seguridad aeroespacial
193	El cambio climático y su repercusión en la Defensa
194	La gestión del conocimiento en la gestión de programas de defensa
195	El rol de las Fuerzas Armadas en operaciones posconflicto
196	Oriente medio tras el califato



SECRETARÍA
GENERAL
TÉCNICA

SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL

ISBN-13: 978-84-9091-368-0



9 788490 913680