CCN-CERT BP/13

Desinformación en el ciberespacio

Febrero 2019

Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Fecha de Edición: febrero de 2019

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL 4
2. INTRODUCCIÓN. 4
3. OBJETIVO DE LA GUÍA 8
4. ¿CUÁL ES EL RIESGO PARA ESPAÑA? 8
5. ¿QUÉ CONSECUENCIAS PUEDE GENERAR UN ATAQUE DE DESINFORMACIÓN? 11
5.1 PÉRDIDA DE CONFIANZA EN LOS MEDIOS DE COMUNICACIÓN TRADICIONALES.11
5.2 PÉRDIDA DE CONFIANZA EN LAS INSTITUCIONES PÚBLICAS 14
5.3 PÉRDIDA DE CONFIANZA EN LA SOBERANÍA DEL CIUDADANO 14
5.4 POLARIZACIÓN SOCIAL.....16
6. LA METODOLOGÍA DE LAS CAMPAÑAS DE DESINFORMACIÓN 17
7. LOS 10 ELEMENTOS CLAVE DE UNA CAMPAÑA DE DESINFORMACIÓN 19
7.1 NOTICIAS FALSAS/*FAKE NEWS* 20
7.1.1 LAS DEEP FAKE NEWS 22
7.2 EL ENFOQUE 23
7.3 LOS NUEVOS MEDIOS.....24
7.4 LOS FOROS SOCIALES 25
7.5 PERFILES DIGITALES MALICIOSOS 25
7.6 CUENTAS AUTOMATIZADAS DE COMPORTAMIENTOS NO HUMANOS.....26
7.7 LAS COBERTURAS DIGITALES O CUENTAS HÍBRIDAS 28
7.8 LAS ESTRELLAS INVITADAS 30
7.9 ALGORITMOS, CÁMARAS DE RESONANCIA Y REDES DE CONFIANZA.....30
7.10 LOS ANUNCIOS PAGADOS 30
8. DECÁLOGO DE RECOMENDACIONES 31

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. INTRODUCCIÓN.

España sufre diariamente tres (3) ciberataques de peligrosidad crítica o muy alta contra el sector público y empresas estratégicas[1]. Algunas de estas acciones ofensivas tienen su origen, principalmente, en otros Estados que tienen entre sus propósitos debilitar y comprometer la capacidad económica, tecnológica y política de España en un mundo cada vez más complejo, competitivo y globalizado.

Las consecuencias de estos ataques pueden ocasionar pérdidas millonarias en empresas privadas y comprometer durante minutos, horas o días el normal funcionamiento de servicios públicos esenciales para los ciudadanos españoles.

En ocasiones los daños producidos por acciones ofensivas digitales se limitan a pérdidas económicas y materiales que en el medio y largo plazo pueden ser subsanables. Tanto las grandes compañías como las instituciones estratégicas del Estado han desarrollado en los últimos años planes y protocolos que les permiten evitar, gestionar y minimizar de manera efectiva las consecuencias de posibles ataques contra sus sistemas e infraestructuras; una parte de estos planes está dedicada a recuperar la operativa de la manera más rápida y eficiente posible: es lo que se conoce como **resiliencia ante ciberataques**.

[1] CCN-CERT. Capacidad de Respuestas a Incidentes del Centro Criptológico Nacional (CCN-CERT)

Sin embargo, cada vez más, se plantean más ataques utilizando el ciberespacio contra los intereses de un país que no consisten en alterar los sistemas informáticos de empresas e instituciones, sino que tienen como objetivo alterar el funcionamiento de unos de los principales elementos del desenvolvimiento de una democracia liberal y de un Estado-Nación moderno: **la opinión pública**.

Pensadores y filósofos, como Jürgen Habermas, defienden que una esfera pública basada en la deliberación racional es la piedra angular sobre la que se asienta una democracia[2]. De esta manera, no pueden pasar desapercibidas las consecuencias que puede tener un ciberataque destinado a erosionar la opinión pública de un Estado y que, de producirse de manera exitosa, sus daños no se limitarían a pérdidas económicas o materiales, sino que podrían erosionar la naturaleza y razón de ser de un sistema de gobierno basado en una democracia liberal, afectando a los factores que proporcionan integridad a un Estado-Nación.

La comunicación utilizada como arma de guerra no es ninguna novedad. Existen referencias a la utilización de guerras comunicativas en contextos bélicos desde hace más de 2.500 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"[3].

Ya en nuestra época, en las facultades de Ciencias de la Información de todo el mundo se estudia la figura de Joseph Goebbles, ministro para la Ilustración Pública y Propaganda del Tercer Reich entre los años 1933 y 1945, como el máximo representante del uso de la propaganda como arma de guerra. Los postulados de Hitler y de su ministro marcaron las pautas de la comunicación y la desinformación, antes incluso del conflicto armado: *"es indispensable desmoralizar a la nación enemiga, prepararla para capitular, constreñirla moralmente a la pasividad, incluso antes de planear cualquier acción militar… No vacilaremos en fomentar revoluciones en tierra enemiga"*[4].

Con el paso del tiempo, las técnicas de propaganda y desinformación se han ido perfeccionando en todos los ámbitos y países. Sin embargo, la revolución tecnológica que se ha producido a nivel global en los últimos diez años ha propiciado un aumento exponencial de estas acciones, tanto en magnitud como en frecuencia y eficacia. Y lo ha hecho, no sólo a través de los métodos tradicionales de desinformación, sino utilizando herramientas automáticas de divulgación, de bajo coste y con una compleja trazabilidad que incrementa de forma considerable su repercusión e impacto.

Los responsables de estos ataques suelen ser gobiernos y grupos subnacionales que tienen como objetivo **erosionar y debilitar la cohesión interna de un Estado o un de grupo de estados** considerados como adversarios y, de esta manera, redefinir su posición geoestratégica. De hecho, algunos países ya reconocen abiertamente que están llevando a cabo y acometiendo este tipo de acciones de manera sistemática. En este sentido, Rusia ha sido uno de los países que más ha desarrollado el concepto de guerra híbrida o, en palabras de la doctrina militar rusa, "guerras no declaradas" y "guerras no lineales"[5].

[2] MACNAMARA, Jim. 2016. Organizational Listening. New York. Peter Lang. P. 10
[3] SUN TZU (s. V a. C. /2013). *El arte de la guerra*. Ed. Medí. S.f
[4] RAUSCHINING, H, 1940. *Hitler me dijo*. Ed. Atlas. Pag.11
[5] Consultar el trabajo "Amenazas Híbridas: nuevas herramientas para viejas aspiraciones". Carlos Galán, PhD. Real Instituto Elcano (2018).

Según el general Valery Gerasimov, jefe del Estado Mayor de las Fuerzas Armadas de la Federación Rusa, un Estado próspero puede *"en cuestión de meses o incluso días, transformarse en una zona de conflicto armado; sufrir una intervención extranjera y hundirse en una red de caos, catástrofes humanitarias y guerra civil"*.

En palabras de este general ruso, impulsor de la denominada **doctrina 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"*[6].

Existen al menos seis (6) factores que contribuyen a impulsar el uso cada vez más recurrente de las acciones hostiles basadas en la distribución de desinformación:

1. **Alto nivel de efectividad.** La revolución tecnológica ha permitido democratizar el acceso a los medios y a la tecnología de producción de mensajes informativos. Actualmente, resulta relativamente barato y fácil producir mensajes multimedia de alta calidad técnica y difundirlos de manera directa y eficaz a las audiencias que se consideren más adecuadas para recibir esos mensajes.

   En cuestión de pocos días, es posible crear páginas webs y plataformas de comunicación multimedia con el mismo aspecto y calidad profesional que medios de comunicación con trayectorias centenarias, o manipular fotografías con programas de edición de fácil acceso y usabilidad.

   De igual manera, con recursos limitados, incluso con un dispositivo móvil, es posible transmitir contenidos en directo, de forma masiva, o generar vídeos con imágenes artificialmente retocadas, que serán posteriormente difundidos en Internet y redes sociales.

2. **Dificultad para establecer una atribución directa.** Una de las principales características de las campañas de desinformación es generar confusión, tanto a través de los mensajes, como de las fuentes.

   Las plataformas digitales y la propia naturaleza de la red propician el surgimiento de actores anónimos que influyen de manera maliciosa en la conformación de la opinión pública. Los perfiles digitales anónimos, los programas para automatizar la distribución de mensajes, el software de ocultación de direcciones IP, la tecnología para crear nuevos medios que mimetizan el aspecto de empresas de comunicación consolidadas…

[6] 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.

Cualquier usuario de Internet tiene hoy día al alcance de su mano la tecnología necesaria para crear redes de comunicación, potencialmente influyentes, que hacen muy compleja la trazabilidad de la información y su fuente de origen.

Por ello, resulta **laborioso y complejo sustanciar en evidencia una acusación directa** o presentar cargos legales o emprender acciones coercitivas contra un país o un grupo subnacional al que se le acusa de iniciar una guerra de comunicación.

3. **Compleja regulación.** A diferencia de otras acciones ofensivas, como la guerra abierta en un campo de batalla, las acciones terroristas o el hackeo digital, **las acciones de desinformación y de manipulación de opinión pública no son fáciles de combatir** desde la perspectiva legal propia de las democracias liberales.

   La libertad de expresión y de opinión son principios fundamentales en un Estado-Nación democrático y suele ser inviable, por principio democrático, limitar estos derechos, tanto a ciudadanos nacionales, como extranjeros.

   Crear un medio de comunicación que difunde información no contrastada no es un delito, como tampoco lo es gestionar multitud de cuentas anónimas en redes sociales, o crear filiales o medios asociados con grupos vinculados a gobiernos extranjeros. Los actores, tanto estatales como no estatales, que actualmente realizan este tipo de operaciones son conscientes y sacan provecho de las limitaciones y contradicciones que plantean las precitadas regulaciones.

4. **Limitación para establecer una relación de causalidad.** Las actuales metodologías técnicas permiten detectar intentos de desinformación y atribuirlos, con mayor o menor grado de certeza, a determinados agentes nacionales o subnacionales con intenciones de condicionar de manera maliciosa el debate público en un Estado.

   Sin embargo, todavía es **muy difícil poder probar una relación de causalidad** entre los intentos por alterar la opinión pública y los cambios en el comportamiento de los ciudadanos.

5. **Aprovechamiento de vulnerabilidades sociales ya existentes.** Los agentes responsables de emprender acciones de desinformación contra un Estado no inician sus acciones desde cero. Primero, detectan vulnerabilidades sociales y políticas reales y espontáneas que se están produciendo en el debate público de un Estado para después centrarse en **aumentar y polarizar ese debate**.

   De esta manera, resulta complejo acusar a estos agentes de provocar crisis políticas o sociales, puesto que en verdad su papel consiste en distorsionar, incitando al alza o a la baja en intensidad conflictos preexistentes o introduciendo nuevos factores para modificar su rumbo.

6. **Infiltración de la desinformación ilegítima en los métodos de la comunicación social y política legítima**. La proliferación de acciones de desinformación ilegítima por parte de actores interesados en influir en la audiencia ciudadana de los países se da, en sí misma, en el marco de la utilización legítima que actores políticos y sociales hacen de las nuevas

plataformas tecnológicas de difusión masiva de información para distribuir sus propios mensajes y contenidos.

En ese escenario de conversaciones con miles de actores en redes sociales y conversaciones cruzadas sobre temas social o políticamente polémicos, el reto para evaluar y reaccionar apropiadamente ante las campañas de desinformación, anulándolas o contrarrestándolas, es **separar el "grano de la paja"**: discernir qué opiniones e informaciones de las distribuidas masivamente en plataformas digitales forman parte del legítimo intento de influencia por parte de actores sociales, económicos o políticos; y qué otras utilizan técnicas de influencia y las nuevas posibilidades de las redes sociales con propósitos de injerencia maliciosa.

Por ejemplo, el proyecto de *Propaganda Computacional* del Instituto de Internet de la Universidad de Oxford[7] en Reino Unido estudia "cómo los *bots*, los algoritmos y otras formas de automatización son utilizados por actores políticos en países alrededor del mundo", partiendo de la base de que las tecnologías de la automatización ya forman parte de las conversaciones políticas también en las democracias y, por tanto, que la desinformación con propósitos de injerencia maliciosa se intercalará en esa realidad.

3. OBJETIVO DE LA GUÍA

Actualmente, la manera más efectiva de desarrollar una resiliencia efectiva ante las acciones de desinformación es protegiendo el principal objetivo de estos ataques: los ciudadanos. Es necesario que los habitantes de un Estado tengan los recursos y desarrollen las **habilidades necesarias para identificar productos y plataformas de comunicación propias de las herramientas de desinformación**.

Estas estrategias de desinformación serán exitosas en la medida en la que sus mensajes logren ser hegemónicos, asumidos y compartidos por usuarios finales que, en la mayoría de los casos, desconocen el verdadero origen y motivación de las fuentes de información que consumen y comparten.

El objetivo de esta guía de buenas prácticas es precisamente explicar las principales características y metodología de las actuales acciones de desinformación, con el objetivo de que los ciudadanos y los usuarios finales de medios de comunicación digital dispongan de las herramientas que les permitan consumir y compartir información de manera crítica y evitar ser cómplices involuntarios de acciones ofensivas contra los intereses del Estado.

4. ¿CUÁL ES EL RIESGO PARA ESPAÑA?

Más de 20 millones de ciudadanos españoles, en riesgo de ser víctimas de la desinformación

Países como España ya han reconocido oficialmente la amenaza para la seguridad que supone este nuevo tipo de acciones. La **Estrategia de Seguridad Nacional**[8]**,** elaborada por el Gobierno

[7] https://www.oii.ox.ac.uk/research/projects/computational-propaganda/
[8] GOBIERNO DE ESPAÑA. Departamento de Seguridad Nacional. http://www.dsn.gob.es/sites/dsn/files/Estrategia_de_Seguridad_Nacional_ESN%20Final.pdf

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[9].

La Estrategia de Seguridad Nacional de España sitúa el origen de estas nuevas amenazas en el complejo contexto sociopolítico y económico y 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"[10].

En España existen actualmente 27,6 millones usuarios de Internet, de los cuales 25,5 millones utilizan diariamente las redes sociales. Las fuentes consultadas indican que el 92 por ciento de la población española entre 16 y 65 años se informa diariamente a través de Internet y que el 85 por ciento lo hace a través de las redes sociales, según datos del Observatorio Nacional de las Telecomunicaciones y la Sociedad de la Información (ONTSI) del año 2017[11].

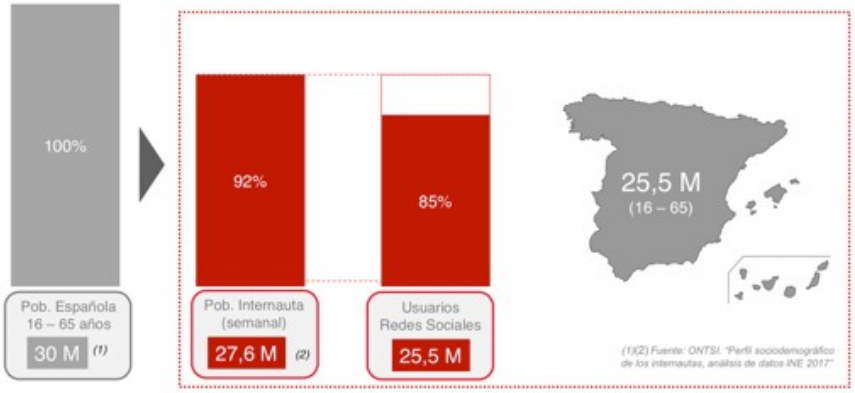

Ilustración 1.- Gráfico elaborado por la Asociación de la Publicidad, el Marketing y la Comunicación digital en España (IAB Spain). Estudio Anual de Redes Sociales 2018.

Según datos de la Asociación para la Investigación de Medios de Comunicación (AIMC), el principal uso que los ciudadanos españoles hacen de Internet es para la lectura de noticias de actualidad, así lo manifestó el 84,6 por ciento de las personas encuestadas entre octubre y diciembre de 2017[12].

Estos estudios sobre el uso de Internet y los hábitos de consumo de información digital sugieren que cerca del **90 por ciento de la población española entre 16 y 65 años puede ser potencialmente víctima de un ataque de desinformación**. Otras investigaciones recientes han evidenciado que, a pesar del extendido uso de Internet y de las redes sociales entre los ciudadanos españoles, existe aún un importante porcentaje de usuarios que desconoce cómo funciona la distribución de noticias en plataformas digitales.

[9] GOBIERNO DE ESPAÑA. *Op. cit.*, p. 16.
[10] GOBIERNO DE ESPAÑA. *Op. cit.*, p. 32
[11] OBSERVATORIO NACIONAL DE LAS TELECOMUNICACIONES Y DE LA SI. 2018. Perfil sociodemográfico de los internautas. Análisis de datos INE 2017. https://www.ontsi.red.es/ontsi/sites/ontsi/files/Perfil%20sociodemogr%C3%A1fico%20de%20los%20internautas%202017.pdf

[12] ASOCIACIÓN PARA LA INVESTIGACIÓN DE MEDIOS DE COMUNICACIÓN (AIMC). 2018. 20º Edición Navegantes en la red. Encuesta AIMC a usuarios de Internet. (octubre-diciembre 2017). https://www.aimc.es/otros-estudios-trabajos/navegantes-la-red/infografia-resumen-20o-navegantes-la-red/

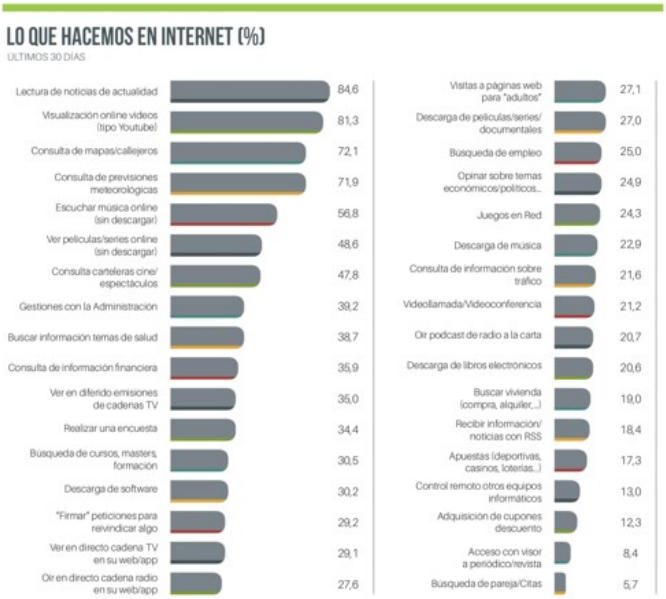

Ilustración 2.- Gráfico elaborado por la Asociación para la Investigación de Medios de Comunicación (AIMC[13]).

El informe "Digital News Report", realizado en el año 2018 por la Universidad de Oxford y la Universidad de Navarra, reconoce por ejemplo que apenas tres de cada diez usuarios digitales en España son conscientes de que las noticias que leen en la red social Facebook dependen de un algoritmo[14] . **Esta falta de concomimiento sobre el entorno informativo digital constituye una vulnerabilidad de la opinión pública española**.

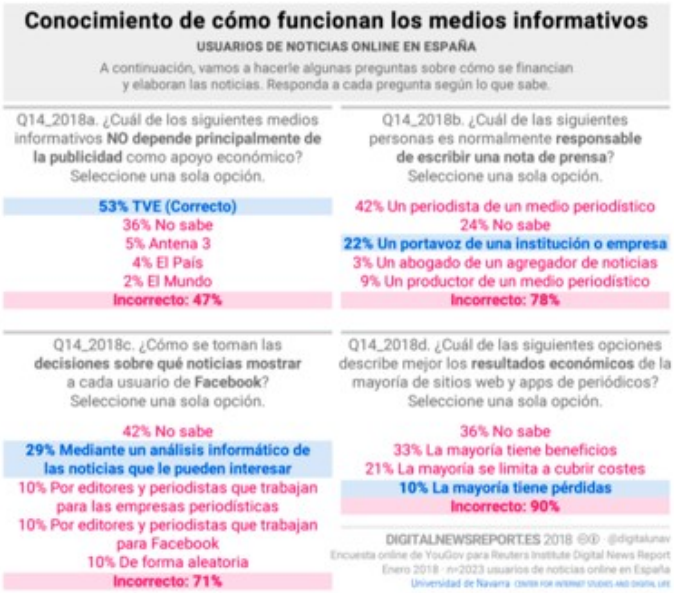

Ilustración 3.- Digital News Report. ES 2018. Universidad de Navarra. Oxford University[15].

[13] Disponible en https://www.aimc.es/otros-estudios-trabajos/navegantes-la-red/infografia-resumen-20o-navegantes-la-red/

[14] UNIVERSIDAD DE NAVARRA/OXFORD UNIVERSITY. 2018. Digital News Report.ES 2018. Una audiencia diversa y preocupada por la desinformación. Coordinado por Avelino Amoedo, Alfonso Vara-Miguel y Samuel Negredo. Center for Intenet Studies and Digital Life School of Communication and Reuters Institute for the Study of Journalism. https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8lZ_D/view

[15] Disponible en: https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8lZ_D/view

5. ¿QUÉ CONSECUENCIAS PUEDE GENERAR UN ATAQUE DE DESINFORMACIÓN?

El principal objetivo de una campaña de desinformación es suministrar en el proceso de formación de la opinión pública de un país noticias falsas, medias verdades, información altamente subjetiva presentada como objetiva (**confusión deliberada entre opinión e información**) e información diseñada para producir un efecto emocional en el receptor, minimizando la probabilidad de que la procese aplicando juicio crítico.

Esta información se distribuye desde plataformas y perfiles que aparentan ser creíbles, pero que ocultan su verdadero origen y dificultan su trazabilidad. La distribución maliciosa y sistemática de informaciones de escasa calidad en el debate público pretende quebrar la confianza entre los ciudadanos de un país y dos (2) de los principales actores responsables de mantener la cohesión social: instituciones y medios de comunicación.

El Estado-Nación moderno está sustentado en un **contrato social basado en la confianza que los ciudadanos depositan en su administración y sus instituciones**. La quiebra de esta relación de confianza puede comprometer la solidez del tejido democrático de un Estado. En este sentido, las consecuencias de una campaña sistemática y maliciosa de desinformación entre la opinión pública pueden derivar en peligrosas consecuencias para una democracia liberal.

5.1 PÉRDIDA DE CONFIANZA EN LOS MEDIOS DE COMUNICACIÓN TRADICIONALES

Los ciudadanos europeos y, especialmente, los españoles, confían cada vez menos en los medios de comunicación, así lo refleja una encuesta realizada en 2018 por el "Eldman Trust Barometer", que concluía que solo mantienen su confianza en ellos el 44 por ciento de los ciudadanos españoles[16].

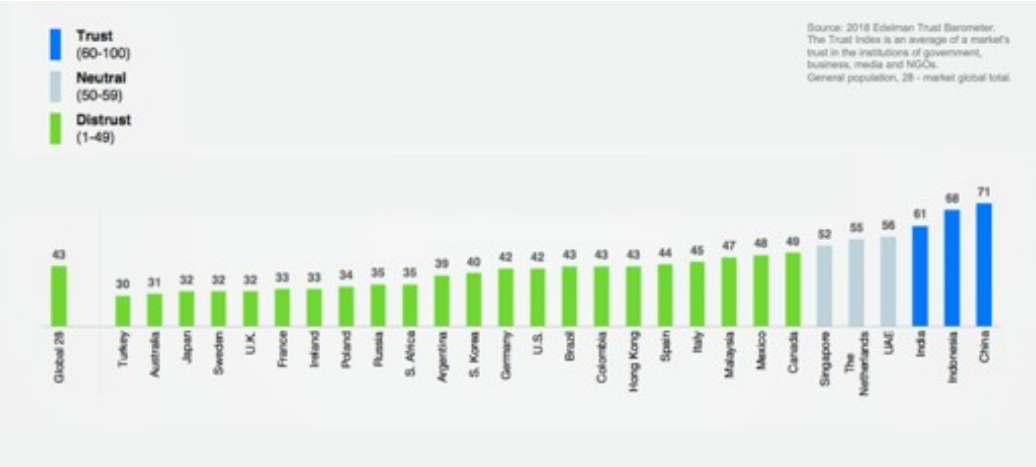

Ilustración 4.- Gráfico elaborado por Edelman Trust Barometer[17].

[16] EDELMAN. 2018. "2018 Edelman Trust Barometer. Global Report".
https://www.edelman.com/sites/g/files/aatuss191/files/201810/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
[17] Disponible en: https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

Hasta finales del siglo XX, los medios de comunicación tradicionales ejercían el papel de mediadores en el proceso de conformación de la opinión pública. Se trataba de agentes identificados y creíbles que creaban y transmitían mensajes que marcaban la agenda y modelaban el debate público y, en consecuencia, la cohesión social de un Estado.

Este dato coincide con los datos del precitado estudio conjunto de la Universidad de Navarra y la Universidad de Oxford, que también señalaba que sólo el 44 por ciento de los usuarios de Internet en España confían en las noticias que leen en los medios[18].

Ilustración 5.- Digital News Report.ES 2018. Universidad de Navarra. Oxford University. [19]

El descenso de confianza de los ciudadanos hacia los medios de comunicación se explica por mecanismos causales históricos en donde entran en juego numerosos factores estructurales ligados a la evolución de las sociedades, de la política, de la tecnología, de la generación y transmisión de información, y de la revolución que afronta la propia práctica periodística.

Este escenario de **cambio de la opinión pública hacia la credibilidad de los medios** es aprovechado por las estrategias ofensivas de desinformación para multiplicarse y generar inestabilidad en las opiniones públicas.

Según el mencionado informe de la Universidad de Navarra y la Universidad de Oxford, España es uno de los países del mundo donde los usuarios de Internet se muestran más preocupados por ser víctimas de campañas de desinformación digital. En concreto, **un 69 por ciento de los internautas reconoce su preocupación por no saber diferenciar entre lo que es cierto y es falso en Internet**[20]. El informe de Edelman, por su parte, también coincide en destacar a España como uno de los países del mundo con mayor número de usuarios de Internet preocupados por las noticias falsas en la red[21].

[18] UNIVERSIDAD DE NAVARRA/OXFORD UNIVERSITY. 2018. Digital News Report.ES 2018. Una audiencia diversa y preocupada por la desinformación. Coordinado por Avelino Amoedo, Alfonso Vara-Miguel y Samuel Negredo. Center for Intenet Studies and Digital Life School of Communication and Reuters Institute for the Study of Journalism. https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8IZ_D/view

[19] Disponible en: https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8IZ_D/view

[20] Ibid.

[21] EDELMAN. 2018. "2018 Edelman Trust Barometer. Global Report". https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

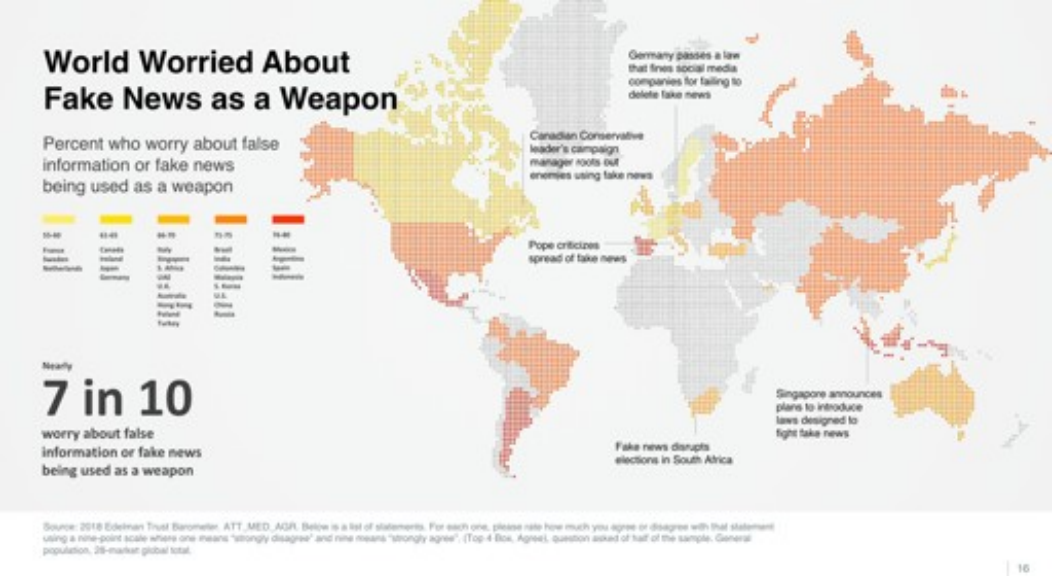

Ilustración 6.- Gráfico elaborado por Edelman Trust Barometer[22].

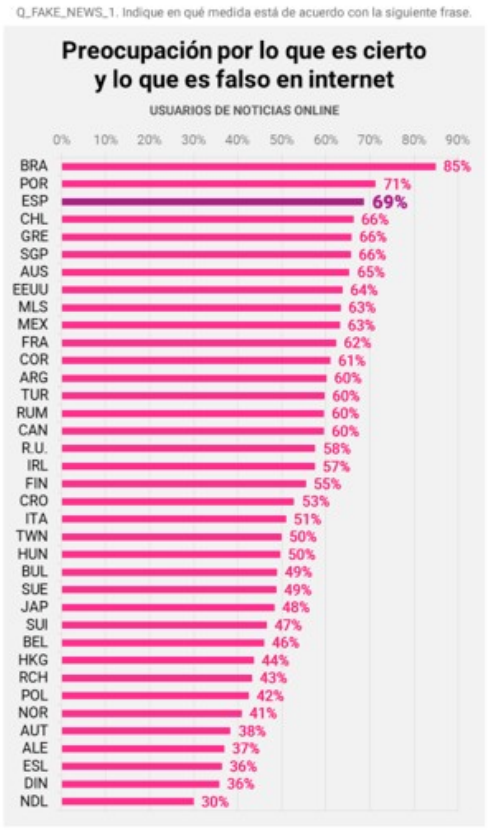

Ilustración 7.- Digital News Report. ES2018. Universidad de Navarra. Oxford University[23].

[22] Disponible en: https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
[23] Disponible en: https://drive.google.com/file/d/1_MqxpbPvMQM1lpvjsGm4QOKxlMC8IZ_D/view

Finalmente, el Eurobarómetro de la Unión Europea, en diciembre de 2018, recogía que el 83 por ciento de los ciudadanos europeos consideran que las noticias falsas son una amenaza real para la democracia, mientras que el 73 por ciento se muestran preocupados sobre las campañas de desinformación digital en periodos pre electorales[24].

5.2 PÉRDIDA DE CONFIANZA EN LAS INSTITUCIONES PÚBLICAS

Por lo dicho, existen evidencias para sospechar que las campañas de desinformación están aprovechando la crisis social de confianza en los medios de comunicación para implantarse y extenderse con mayor facilidad. Sin embargo, resulta aún más preocupante comprobar cómo la confianza de los ciudadanos en las instituciones públicas de sus países también está cayendo a mínimos históricos.

En el caso de España, sólo el 24 por ciento de ciudadanos confía en sus instituciones de gobierno, según el informe de Endelman[25]. Uno de los principales objetivos de las campañas de desinformación es, precisamente, **detectar los puntos de vulnerabilidad en el contrato social de un país y potenciarlos** con el objetivo de aumentar la desconfianza entre ciudadanos e instituciones públicas.

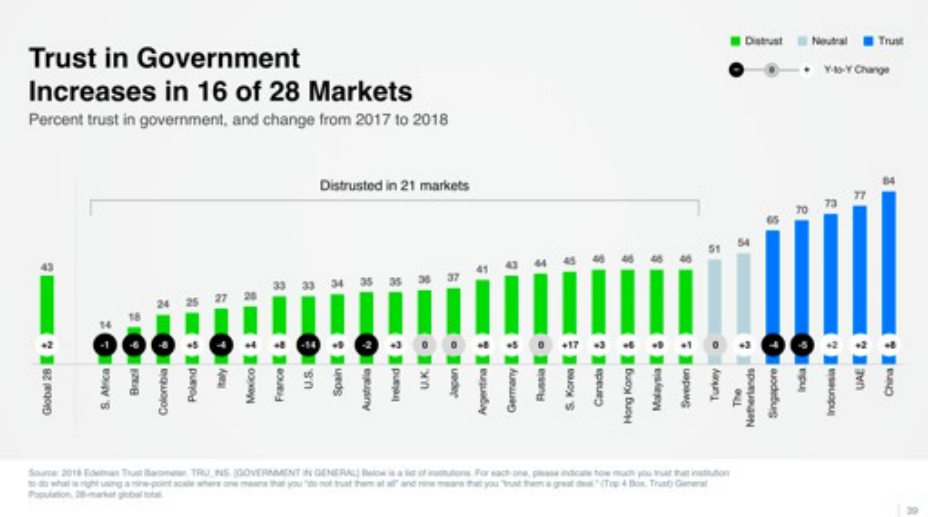

Ilustración 8.- Gráfico elaborado por Edelman Trust Barometer[26].

5.3 PÉRDIDA DE CONFIANZA EN LA SOBERANÍA DEL CIUDADANO

En relación tanto con la crisis de confianza en los medios de prensa tradicionales como con la erosión de la confianza en las instituciones públicas democráticas, algunas estrategias de desinformación pueden buscar desestabilizar la propia base de ambas: **la confianza de las**

[24] COMISIÓN EUROPEA. 2018. Action Plan Against Desinformation. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=55907
[25] EDELMAN. 2018. "2018 Edelman Trust Barometer. Global Report". https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf
[26] Disponible en: https://www.edelman.com/sites/g/files/aatuss191/files/2018-10/2018_Edelman_Trust_Barometer_Global_Report_FEB.pdf

democracias en que el ciudadano mejor informado será capaz de tomar las mejores decisiones para su gobernanza.

Esta línea de acción desinformativa persigue **quebrar la confianza del ciudadano en la esencia de la información como elemento de decisión democrática**. Por un lado, si se consigue sembrar y hacer germinar la sensación de que los medios de prensa tradicionales no son creíbles y que, por otro lado, a través de las redes sociales sólo circula información basura o de baja calidad (que es utilizada además por países extranjeros para influir en el sentido del voto en elecciones democráticas) se estará intentando instalar en el ciudadano la sensación de que no hay forma de obtener información de calidad para establecerse un juicio de valor para tomar sus decisiones de voto y, por tanto, de gobernanza.

En el análisis de las campañas de desinformación, principalmente en aquellas que se atribuyen a países extranjeros con intereses geoeconómicos o geopolíticos, es una **buena práctica tener en cuenta hasta qué punto se está intentando minar la confianza del ciudadano en los medios informativos** (medios de prensa, redes sociales, plataformas digitales), más que el hecho de que la intención sea polarizar la conversación de temas sociales o políticos hacia direcciones espurias.

Por ejemplo, si un Estado con intenciones maliciosas logra acaparar titulares de prensa y análisis académicos por todo el mundo que le atribuyen la capacidad de manipular a la ciudadanía e influir en procesos democráticos en buena parte de los escenarios electorales de países en cualquiera de los continentes, uno de los efectos que se genera es que se atribuye a ese Estado malicioso el poder y las capacidades para ejercer esa influencia.

A partir de ahí, el ciudadano puede inferir que tiene menos posibilidades de informarse legítimamente para decidir sobre su democracia, puesto que hay un Estado extranjero que manipula las redes sociales en un escenario donde la confianza en la prensa y en las instituciones también ha decrecido.

De este modo, el reto para **contrarrestar y anular las campañas de desinformación** es, al menos, quíntuple:

1. Detectar y atajar los intentos de influencia ilegítima en asuntos concretos de polarización social y política.
2. Analizar adecuadamente esos intentos ilegítimos para distinguirlos de procesos de influencia política y social por actores legítimos.
3. Contextualizar adecuadamente las atribuciones sobre intenciones y capacidades de actores con objetivos de desinformación, para enmarcar correctamente la dimensión pequeña o grande de esos actores en el conjunto global de la comunicación masiva y transmedia que se está dando ya en cualquier proceso democrático.
4. Arbitrar campañas de información al ciudadano sobre la desinformación, sus intenciones y sus alcances, así sobre los intentos de algunos actores de hacer parecer ante la opinión pública que pueden ejercer sobre ella una “total manipulación”, cuando ni tienen los recursos ni muchas veces esas intenciones tan ambiciosas.

5. Introducir buenas prácticas en análisis académicos o por medios de prensa para, describiendo intentos de campañas de desinformativas en redes sociales, dimensionar adecuadamente el alcance que esas campañas pueden tener y cómo esas campañas maliciosas comparten espacio con otro volumen de información legítima que, en la mayoría de los casos, es la que en mayor cantidad y calidad está llegando al ciudadano.

5.4 POLARIZACIÓN SOCIAL

La propia naturaleza de las plataformas digitales de información, que utilizan algoritmos para seleccionar de manera personalizada noticias que consideran del gusto del usuario, contribuye a la creación de conversaciones digitales altamente polarizadas. Las campañas de desinformación buscan, precisamente, aumentar esta polarización.

En primer lugar, detectando aquellas conversaciones digitales que resultan más polémicas o causan mayor confrontación en el debate público y, de una manera maliciosa, fomentando y ampliando estos debates con el fin de enfrentar a los ciudadanos de un país en torno a determinados temas políticos o sociales.

Un estudio del Laboratorio Social Machines del MIT sobre la conversación digital (chats) en la campaña electoral estadounidense en 2016 detectó altos índices de polarización, en torno a dos comunidades políticas: una, en favor de Donald Trump y otra, favorable a Hillary Clinton[27]. El debate entre estas dos comunidades en el entorno digital fue prácticamente nulo y la conversación sólo contribuyó a radicalizar las posturas de los miembros de cada una de estas comunidades.

Actualmente, las autoridades judiciales y el propio Congreso de los Estados Unidos están analizando si países extranjeros utilizaron esta polarización para aumentar la crispación social y erosionar la cohesión interna del país de manera maliciosa.

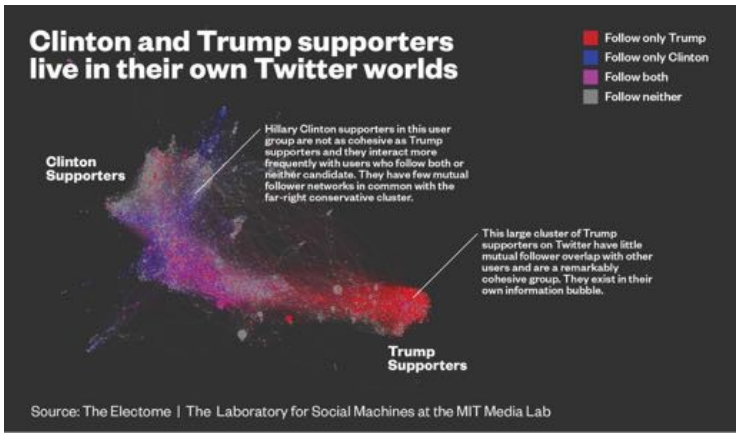

Ilustración 9.- Grafico realizado por Vice News. 8 diciembre de 2016 con datos del Social Machines del MIT Media Lab[28].

[27] VICE NEWS. 2016. Parallel narratives. Clilnton and Trump supporters really don´t listen to each other on Twitter. Alex Thompson. 8 diciembre 2016. https://news.vice.com/en_us/article/d3xamx/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows

[28] Diposnible en: https://news.vice.com/en_us/article/d3xamx/journalists-and-trump-voters-live-in-separate-online-bubbles-mit-analysis-shows

De igual manera, un estudio realizado por la empresa española Alto Analytics demostró que el debate digital sobre la inmigración en la precampaña electoral italiana en el año 2017 también mostraba que la sociedad de este país estaba altamente polarizada en torno a dos comunidades y que apenas interrelacionaban entre ellas.

Este mismo estudio aportó indicios de que medios de comunicación extranjeros y otros agentes no identificados pudieron contribuir a aumentar esta división en la sociedad italiana mediante campañas sistemáticas de desinformación[29].

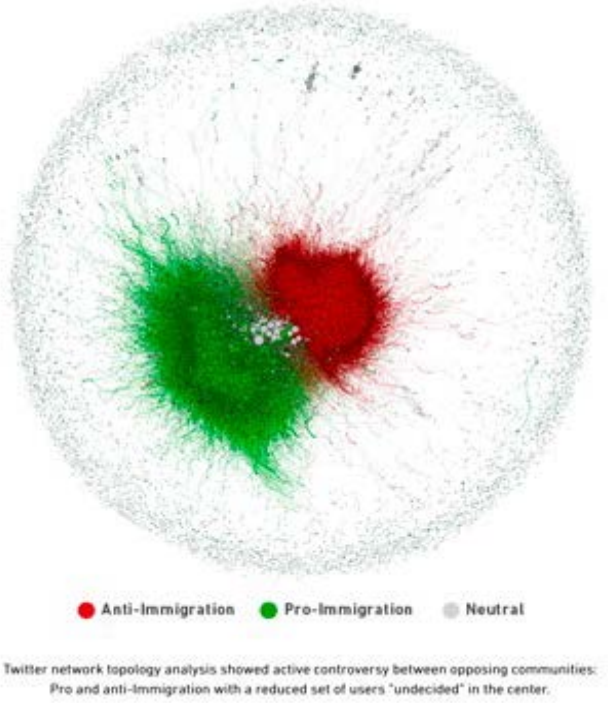

Ilustración 10.- Gráfico elaborado por Alto Analytics[30].

6. LA METODOLOGÍA DE LAS CAMPAÑAS DE DESINFORMACIÓN

Las acciones de *hackeo,* manipulación o perturbación de la opinión pública mediante acciones de desinformación siguen un patrón constante, tanto en acciones ofensivas por parte de Estados-nación como por parte de grupos subnacionales. Esta metodología está asentada en una combinación de diversas disciplinas, tales como la sociología, la política, la literatura, el periodismo o la tecnología.

Los cuatro (4) pasos que se requieren para implementar una exitosa campaña de disrupción digital y comunicativa para desestabilizar la opinión pública de un estado son los siguientes:

[29] ALTO ANALYTICS. 2017. The Construction of Anti-immigration electoral messages in Italy. The role of foreign media in the anti-immigration debate one year before the 2018 election. https://www.alto-analytics.com/en_US/the- construction-of-anti-immigration-messages-in-italy/

[30] Disponible en: https://www.alto-analytics.com/en_US/the-construction-of-anti-immigration-messages-in-italy/

1. **Análisis y detección de vulnerabilidades sociales y políticas de un país.**

   Las acciones de desinformación están basadas en explotar el caldo de cultivo de los asuntos que en la dinámica interna de un país ya generan confrontaciones en la opinión pública.

   La alteración de la opinión pública no consiste en crear nuevas confrontaciones en la política interna del país considerado como adversario. Por el contrario, la estrategia está enfocada en alimentar debates y confrontaciones políticas ya instaladas y que polarizan una sociedad.

   En el caso de Estados Unidos, la presunta disrupción comunicativa generada, supuestamente por Rusia, alimentó debates políticos y sociales ya existentes. Por su parte, el DAESH 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.

2. **Creación de narrativas "transmedia".**

   Una vez detectados en un país los espacios donde se producen escenarios de confrontación social o política, los responsables de una acción disruptiva de desinformación 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 personajes, formatos y plataformas de comunicación, adaptándose a las particularidades culturales y estéticas de los colectivos a los que van dirigidos.

3. **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 (3) elementos es la base para la difusión eficaz de los contenidos de una campaña de marketing.

   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 que la marca inserta en canales de comunicación ajenos a cambio de una contraprestación económica, y los medios ganados hacen referencia a las informaciones, comentarios o comunicaciones no pagadas que usuarios y agentes influyentes realizan sobre la marca.

   Las narrativas construidas para canalizar y retroalimentar los conflictos socioeconómicos y políticos de un Estado son introducidas en el debate digital a través de una red de medios propios controlados jerárquicamente por los responsables de un mecanismo de disrupción con fines de desinformación.

4. **Creación de canales de distribución automatizados.**

   El último paso de la disrupción es la distribución directa, automatizada y segmentada de las narrativas, dirigida 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 estatales[31], así como de actores no estatales[32].

7. LOS 10 ELEMENTOS CLAVE DE UNA CAMPAÑA DE DESINFORMACIÓN

La Comisión Europea identifica el fenómeno de la desinformación con las noticias falsas. Según esta institución, *"la desinformación o noticias falsas consiste en información demostrablemente falsa o incorrecta que es elaborada, presentada y difundida para obtener una ganancia económica, para engañar de manera maliciosa al pública o para causar un daño"*[33].

Esta definición recoge de manera muy clara la naturaleza de las acciones ofensivas de comunicación. Sin embargo, también es demostrable que las noticias falsas, o *fake news,* en inglés, son sólo una herramienta más de la compleja maquinaria que está detrás de una campaña de desinformación.

Las acciones ofensivas de comunicación son fenómenos complejos que utilizan diferentes herramientas y procedimientos (no sólo *fake news*) para hacer llegar a los ciudadanos mensajes que causen el caos y la confusión en la opinión pública de un país considerado adversario.

A continuación, se van a identificar algunas de las herramientas más utilizadas en campañas de desinformación. Las dos (2) primeras técnicas están relacionadas con la creación de contenidos o narrativas y las ocho (8) siguientes tienen que ver con el proceso de distribución de contenidos (a través de medios, redes sociales o algoritmos).

[31] , Javier. «Why did Russian social media swarn 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.

[32] 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.

[33] COMISIÓN EUROPEA. 2018. "Fake News and Online Disinformation". https://ec.europa.eu/digital-single-market/en/fake-news-disinformation

7.1 NOTICIAS FALSAS/*FAKE NEWS*

Las noticias falsas son mensajes informativos que se difunden a la opinión pública y que no se corresponden con ningún hecho verdadero o demostrable científica o históricamente. A pesar de su nula relación con la verdad, las noticias falsas pueden ser aceptadas como creíbles o verosímiles por un amplio número de ciudadanos y provocar graves crisis políticas y de seguridad en un Estado.

La aceptación como verdad de este tipo de noticias se debe a las siguientes características:

- **Están basadas en algunos elementos verdaderos**. Estas noticias se basan en algún personaje, lugar o fenómeno de actualidad, reales.
- **Resultan sorprendentes**. Estas noticias son presentadas al lector de una manera muy atractiva y sensacionalista, que normalmente incluyen títulos provocadores o sorprendentes, que invitan a su lectura.
- **Provienen de medios de reciente creación o de escasa trazabilidad**. Las noticias falsas se difunden originariamente en medios de comunicación desconocidos, bien porque son de reciente creación (creados ad-hoc para iniciar acciones de este tipo) o porque tienen su origen en países extranjeros donde es difícil investigar el origen y la trazabilidad del medio.
- **Ausencia de fuentes**. Las noticias falsas son relatadas en textos donde no se identifican o se mencionan fuentes fiables o reconocidas. En el caso de que se presente alguna fuente, sólo es para dar voz a aquellas que reafirman la teoría de la noticia y no se da ninguna oportunidad de expresión a voces o pensamientos que pongan en duda la tesis mantenida en la información.
- **Confían en el largo plazo**. Las noticias falsas pueden tener un impacto a corto plazo, pero también pueden desarrollar su capacidad ofensiva en el largo plazo. En algunas ocasiones, la noticia falsa se publica en algún medio desconocido de un país extranjero, a la espera de que con el tiempo entre en la cadena de distribución de noticias de medios más fiables y adquiera aspecto de credibilidad.

  Igualmente, estas noticias publicadas en medios desconocidos pueden acabar siendo citadas en investigaciones académicas o en páginas web de referencia de uso masivo (como Wikipedia) y, de esta manera, adquirir al cabo de meses o años apariencia de credibilidad y contaminar el proceso de conformación de la opinión pública.

Una de las operaciones de desinformación más exitosas utilizando las noticias falsas fue la llamada "Operation Infektion"[34]. Esta campaña fue puesta en marcha por el gobierno ruso a comienzos de los años ochenta con el objetivo de difundir que el virus del sida lo había creado el gobierno de los Estados Unidos para eliminar a su población afroamericana y homosexual. Esta noticia se publicó por primera vez en julio de 1983 en un desconocido periódico local de la India y pasó casi desapercibida.

[34] NEW YORK TIMES. 2018. "Operation Infektion. Russian Disinformation: from Cold War to Kanye", by Adam B. Ellick and Adam Westbrook. https://www.nytimes.com/2018/11/12/opinion/russia-meddling-disinformation-fake-news-elections.html

Sin embargo, con el paso del tiempo, la noticia fue citada y mencionada por medios de otros países, hasta que, el 30 de marzo de 1987, la cadena estadounidense CBS se hizo eco de la información en un programa de máxima audiencia y convirtió una noticia falsa, creada cuatro años antes por los servicios de inteligencia soviéticos en la India, en un tema de debate público y político en los Estados Unidos.

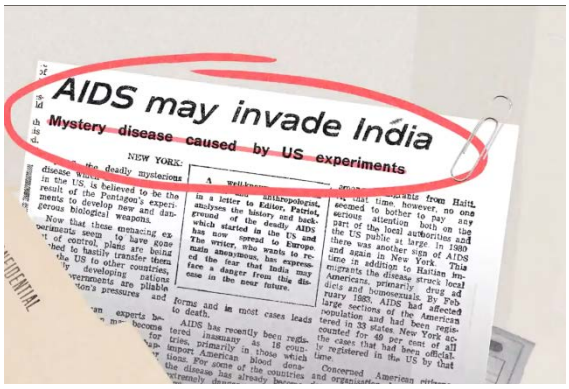

Ilustración 11.- Artículo original publicado en la India en julio de 1983 en el que se informaba de que el sida había sido creado por el gobierno de Estados Unidos.

Una historia de éxito más reciente, a finales de octubre de 2016, en la que **cuentas anónimas en Facebook y medios de comunicación de escasa credibilidad** comenzaron a difundir la noticia de que la candidata demócrata a la presidencia de Estados Unidos, Hillary Clinton, formaba parte de una red de explotación sexual de menores que tenía su sede en una conocida pizzería de Washington D.C.

Estas informaciones se difundieron a gran velocidad y miles de ciudadanos le dieron credibilidad. De hecho, apenas un mes después de la publicación de esta noticia, un ciudadano estadounidense entró armado al restaurante y comenzó a disparar con la intención de liberar a los presuntos niños explotados sexualmente[35].

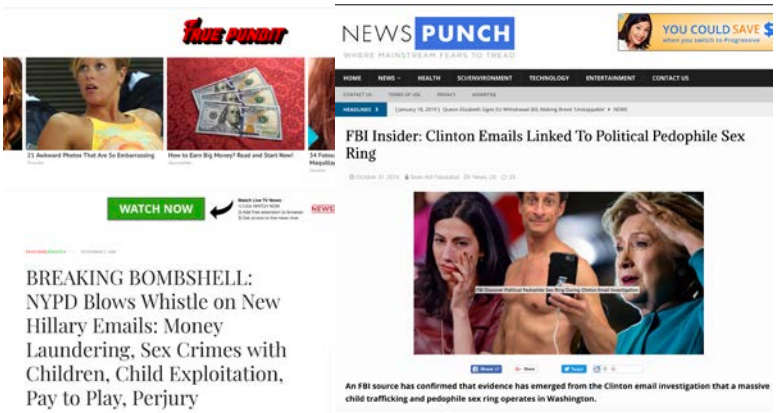

Ilustración 12.- Capturas de pantalla de algunos de los medios que difundieron a finales de octubre de 2016 la falsa noticia sobre la relación de Hillary Clinton con una presunta red de explotación sexual de menores.[36]

[35] ROLLING STONE. 2017. "Anatomy of a Fake News Scandal", by Amanda Robb. https://www.rollingstone.com/politics/politics-news/anatomy-of-a-fake-news-scandal-125877/

[36] Las noticias siguen disponibles en internet en los siguientes enlaces: https://newspunch.com/fbi-clinton-email-pedophile-ring/ https://truepundit.com/breaking-bombshell-nypd-blows-whistle-on-new-hillary-emails-money-laundering-sex-crimes-with-children-child-exploitation-pay-to-play-perjury/

Otro ejemplo de noticias falsas, en este caso relativas a la actualidad española, se produjo el 28 de octubre de 2017, cuando el medio de comunicación de origen ruso RT News publicó un titular en el que anunciaba la presencia de tanques en las calles de Barcelona (la noticia fue compartida en Facebook por 11.800 usuarios).

Ilustración 13.- Captura de pantalla de la información publicada por RT News donde se sugería la presencia de tanques en las calles de Barcelona en octubre de 2017[37].

Ilustración 14.- Captura de pantalla de dos perfiles digitales desinformativos en Twitter que aseguran que milicianos extranjeros están "asesinando inocentes" en las calles de Francia durante la crisis de los chalecos amarillos.

7.1.1 LAS DEEP FAKE NEWS

Dentro del fenómeno de las noticias falsas es importante destacar la evolución y popularización de las llamadas noticias falsas profundas, o *deep fake news*. Se trata de una tecnología que puede añadir aún más complejidad y capacidad ofensiva a esta técnica y consiste en la utilización

[37] Disponible en: https://actualidad.rt.com/actualidad/253812-espana-cataluna-violencia-conflicto

de software para crear imágenes de video reales de autoridades y políticos pero que tienen el audio y el movimiento de la boca modificado.

De esta manera, se pueden difundir discursos o declaraciones de autoridades públicas con apariencia real, pero cuyo mensaje está totalmente o parcialmente adulterado.

7.2 EL ENFOQUE

Las campañas de desinformación no sólo están basadas en contenidos falsos. En otras ocasiones, las informaciones difundidas con ánimo malicioso están basadas en un hecho real, pero se presentan ante la opinión pública con un enfoque elaborado y construido de tal manera que el usuario final interpreta ese hecho de una manera que no coincide con la realidad.

Los enfoques manipulan las percepciones que pueden generar los titulares y las fotografías de la información, lo que se conoce como el "primer nivel de lectura" de una noticia. Este primer nivel de lectura no sólo atrae la primera atención del usuario, sino que, con los actuales hábitos de consumo informativo en dispositivos móviles, constituye, en muchas ocasiones, la única información que se recibe de una noticia.

Un ejemplo de esta modalidad de desinformación es la noticia publicada, el 1 de octubre de 2017, en el canal de información de origen ruso RT News en su versión en español. La noticia que tenía el siguiente titular: "Fuertes videos: la brutal represión de la Policía contra los votantes del referéndum catalán" es un ejemplo de esta modalidad de desinformación.

Ilustración 15.- Noticia publicada por RT News el 1 de octubre de 2017[38].

El titular está acompañado de una fotografía en la que una persona yace tendida en el suelo con los ojos cerrados y con una herida sangrante en la frente que aparece *pixelada*. El texto en

[38] Disponible en: https://actualidad.rt.com/actualidad/251682-represion-brutal-policia-espa%C3%B1ola-referendum-catalan

ningún momento miente de manera explícita con la información, con lo cual no se podría presentar como un caso de noticia falsa o *fake news*. No se dice que hay personas fallecidas, la fotografía es real y muestra una persona herida en un enfrentamiento con la policía durante la celebración del referéndum de independencia ilegal en Cataluña.

Sin embargo, el primer nivel de lectura, compuesto por el titular ("fuertes videos, brutal represión") y la fotografía (una persona tumbada con los ojos cerrados y con una herida sangrante en la frente) puede llevar al lector a la conclusión de que hubo personas fallecidas durante el 1 de octubre de 2017 en Cataluña (la noticia ha sido compartida hasta enero de 2018 por 22.800 personas en Facebook).

7.3 LOS NUEVOS MEDIOS

El fenómeno de las noticias falsas se ha popularizado e incrementado de manera exponencial a comienzos del siglo XXI debido a la facilidad y efectividad con la que actores con intereses propios, agentes políticos encubiertos o países extranjeros pueden crear medios y plataformas de comunicación de aspecto profesional y creíble, y en diversos idiomas.

Estos nuevos medios sirven como plataformas para la publicación inicial de información maliciosa y, en cuestión de días o meses, pueden competir en influencia con medios de comunicación asentados durante décadas en la opinión pública de una sociedad.

Suelen compartir algunas de las siguientes características:

- Reciente creación y ausencia de trayectoria profesional reconocida.
- Ausencia de firma en las noticias.
- Falta de información sobre los responsables editoriales de los contenidos y sobre los responsables financieros o accionistas.
- Falta de información sobre la sede física de la empresa.
- Vinculados a gobiernos extranjeros, que ocultan su relación gubernamental e incluso se intentan mimetizar con medios locales o nacionales para generar confusión.

Los medios de comunicación de calidad están implementando medidas para diferenciarse de las nuevas plataformas digitales destinadas a difundir campañas de desinformación. Uno de estos proyectos es el denominado *Trust Project* al cual se han adherido diversos medios de comunicación de todo el mundo, así como diversas instituciones académicas.

Este proyecto establece ocho (8) indicadores de confianza que garantizan que el proceso de producción y difusión de sus noticias se rige por criterios de calidad y confianza[39]:

- **Mejores prácticas.** ¿Cuáles son los principios del medio? ¿Quién lo financia? ¿Cuál es su misión? Implica, además, la inclusión del código ético, el compromiso por la diversidad, el rigor, las correcciones y otros estándares**.**

[39] https://elpais.com/estaticos/que-es-the-trust-project/

- **Experiencia del periodista:** ¿Quién escribió este artículo? Información sobre el autor, incluyendo su trayectoria y los artículos publicados.
- **Tipo de trabajo:** ¿A qué género periodístico pertenece el artículo? Etiquetas que distinguen los textos de opinión, de análisis o publicitarios de las noticias.
- **Citas y referencias:** ¿Cuál es la fuente? Para historias de investigación o en profundidad, acceso a las fuentes detrás de los hechos y las afirmaciones.
- **Métodos de trabajo:** ¿Cómo se construyó? También para historias en profundidad, información sobre porqué los reporteros decidieron seguir una historia y cómo abordaron el proceso.
- **¿De origen local?:** Identificar cuando la historia surgió en un lugar sobre el que el medio cuenta con un profundo conocimiento sobre el contexto local o de la comunidad a la que se dirige.
- **Diversidad:** ¿Cuál es el compromiso de la redacción por aportar perspectivas diversas?
- **Comentarios de los lectores:** Facilitar espacios para fomentar la participación de los lectores y que den su opinión.

7.4 LOS FOROS SOCIALES

Los foros de discusión *online* (tanto abiertos, en plataformas públicas, o cerrados, en páginas de la Internet profunda) son también utilizados de manera recurrente para la difusión de mensajes propios de campañas de desinformación.

El éxito de estos foros radica precisamente en que los usuarios pueden comentar cualquier asunto de la actualidad de manera completamente anónima y no existe ningún control ni censura sobre la veracidad de los mensajes compartidos.

Los responsables de las campañas de desinformación difunden los mensajes maliciosos con la **esperanza de que otros usuarios den credibilidad a la información y difundan los contenidos** en otras plataformas digitales abiertas, así como en las redes sociales personales.

7.5 PERFILES DIGITALES MALICIOSOS

La difusión de noticias falsas o maliciosas no sólo se produce a través de nuevos medios de comunicación de escasa credibilidad. También lo hacen a través de la **manipulación o falsificación de perfiles digitales en redes sociales** de personajes o instituciones reales con el objetivo de hacer creer a la opinión pública que han realizado unas declaraciones que, en realidad, nunca llegaron a hacer.

La manipulación de estos perfiles digitales puede adoptar diferentes aspectos o modalidades:

- **Simulación maliciosa de cuentas y perfiles reales.** El método más efectivo de suplantar el perfil digital de una persona o institución es mediante la utilización de software o sitios web que permiten recrear el aspecto de la cuenta de una red social real, pero añadiendo contenido inventado.

Una vez hecha la recreación, se realiza una fotografía o una captura de pantalla (*screenshot*) de la publicación y se comparte a través de redes sociales como WhatsApp entre contactos cercanos, hasta que se *viraliza* el mensaje falso.

- **Creación de perfiles digitales falsos o parodias.** Otra manera de difundir informaciones maliciosas a través de redes sociales es mediante la creación de un perfil digital de una persona o institución sin contar con su consentimiento y suplantando su identidad.

  Para evitar este tipo de situaciones, algunas plataformas digitales ofrecen la posibilidad de verificar y autentificar que el perfil digital de un individuo coincide con su verdadera identidad.

- **Hackeo de perfiles digitales.** Una forma más sofisticada es mediante el *hackeo* o el robo de las contraseñas del usuario de un perfil digital para controlarlo de manera maliciosa durante un periodo de tiempo. Algunas de estas acciones han llegado a causar pérdidas y daños no sólo en la reputación de empresas, sino en la economía global.

  Una de las acciones más perjudiciales que se llevaron a cabo utilizando esta metodología ocurrió el 23 de abril de 2013, cuando el grupo autodenominado "Ejército Electrónico Sirio" se hizo con el control de la cuenta en Twitter de la agencia de noticias Associated Press (AP) y reportó un tiroteo en la Casa Blanca. En apenas minutos, este mensaje provocó que la bolsa de Estados Unidos se desplomara más de 150 puntos durante cinco minutos[40].

Ilustración 16.- Cuenta de Twitter de la agencia Associated Press.

7.6 CUENTAS AUTOMATIZADAS DE COMPORTAMIENTOS NO HUMANOS

La creación de cuentas anónimas, gestionadas de manera automatizada en redes sociales, es otro mecanismo empleado para **difundir de manera masiva mensajes en una campaña de desinformación.**

Gran parte de las plataformas digitales de comunicación social permiten la creación de cuentas anónimas y la utilización de software que automatizan la gestión de estos perfiles. Esto permite

[40] USA TODAY. 2013. "AP Twitter feed hacked; no attack at White House". https://www.usatoday.com/story/theoval/2013/04/23/obama-carney-associated-press-hack-white-house/2106757/

a grupos encubiertos lanzar campañas de desinformación que alcanzan un gran volumen y difusión en redes sociales.

La detección de perfiles digitales automatizados en una campaña de desinformación depende del nivel de sofisticación empleado en la creación de tales perfiles. En cualquier caso, es posible definir algunas características para determinar si detrás de una cuenta digital existe una persona real o estamos ante una herramienta automatizada para difundir masivamente un determinado mensaje.

- **No correspondencia con una persona real verificable.** El primer rasgo de un perfil digital automatizado es que, ni el nombre, ni la fotografía, ni la información de la cuenta coincide con una persona real identificable en otras fuentes.

  Así mismo, en el historial de contenidos del perfil no se observa ningún detalle ni comentario relativo a la vida personal de un individuo o una institución real.

- **Alta o inusual actividad diaria.** Las cuentas automatizadas destacan por su inusual comportamiento temporal. Cientos de mensajes sobre un mismo tema durante un solo día; un número de mensajes inusualmente elevado (más de cincuenta por día); mensajes publicados durante las 24 horas del día los siete días de la semana, …

- **Ausencia de seguidores o seguidores sospechosos de ser cuentas automáticas.** Los perfiles digitales empleados en campañas de desinformación destacan por el escaso número de seguidores que tienen en su perfil o, alternativamente, por tener un elevado número de seguidores que también podrían ser cuentas automáticas tipo *bot*.

- **Unilateralidad.** Los perfiles digitales automatizados no suelen dialogar en las redes sociales, sólo se limitan a difundir mensajes en conversaciones donde se encuentran sus audiencias potenciales.

- **Ausencia de contenido original.** Una de las principales características de las cuentas digitales de comportamiento no humano es la ausencia de contenido original. La mayoría de estos perfiles redifunden o interactúan con contenido creado por otros perfiles.

- **Poca variedad temática.** Los perfiles digitales automatizados se centran en publicar y dar la mayor difusión a aquellos mensajes políticos o sociales para los que han sido creados.

- **Escasa variedad de fuentes.** De igual manera, estas cuentas propias de campañas de desinformación utilizan de manera exclusiva aquellas fuentes que forman parte de la misma estrategia y crean y difunden mensajes similares con los mismos enfoques.

Asimismo, la **utilización automatizada de redes sociales** es, por ejemplo, la técnica que emplea de manera habitual el grupo terrorista DAESH para difundir sus campañas en redes sociales. Los terroristas generan una media de cien perfiles digitales nuevos, sin apenas seguidores, para difundir cada una de sus campañas de comunicación, y gestionan estas cuentas mediante *bots* que automatizan la distribución de mensajes.

La *viralización* de los contenidos la realizan mediante la parasitación de los *hashtags* más populares entre las conversaciones de sus audiencias potenciales.

Ilustración 17.- Ejemplo de *bot utilizado por el grupo terrorista DAESH para difundir su propaganda a través de las redes sociales.*

7.7 LAS COBERTURAS DIGITALES O CUENTAS HÍBRIDAS

Las campañas de desinformación utilizan cada vez estrategias más complejas para dificultar la detección de las cuentas automatizadas encargadas de difundir sus mensajes. Los responsables de las estrategias ofensivas de desinformación son conscientes de que las cuentas automatizadas con las características descritas anteriormente son fácilmente detectables y carecen de la credibilidad necesaria para lograr que un mensaje se *viralice* de manera eficiente.

Por ese motivo, **las campañas de desinformación están empleando, cada vez con mayor frecuencia, perfiles digitales que aparentan un comportamiento humano**, pero que, en realidad, forman parte de un ejército de identidades falsas creadas y controladas por un grupo organizado que trabaja de forma encubierta.

Estos perfiles digitales tratan de ocultar las características propias de las cuentas automatizadas; parecen estar asociadas a personas reales con nombre apellidos, fotografía, aficiones, fecha de nacimiento; cuentan con un número considerable de seguidores; tienen una trayectoria temporal considerable y, en ocasiones, interactúan con otros usuarios. Sin embargo, todo esto es parte de la cobertura cuidadosamente elaborada para ganar la confianza de otros usuarios y distribuir de manera eficaz mensajes desinformativos.

Un ejemplo de este tipo de cuentas es el perfil desde el que se difundió la noticia falsa que vinculaba a Hillary Clinton con una red de explotación de menores en una pizzería. Las informaciones que surgieron desde foros digitales anónimos ganaron credibilidad en el momento en el que fueron difundidas por una cuenta en una red social que aparentaba representar a una persona real: David Goldberg (@davidgoldbergNY), un abogado de la ciudad de Nueva York, que incluso se presentaba con una fotografía.

Sin embargo, ninguna persona real se encontraba detrás de esa cuenta, que fue utilizada únicamente para difundir una información falsa sobre la candidata a la presidencia de Estados Unidos. El perfil fue eliminado por la red social Twitter cuando se comprobó su falsedad.

Ilustración 18.- Mensaje publicado desde la cuenta @davidgoldbergNY.

Otro ejemplo de cuentas en redes sociales falsas, que aparentaban representar a personas reales, se produjo durante la difusión de noticias relativas a la celebración del referéndum ilegal de independencia en Cataluña en octubre de 2017.

Entre los perfiles digitales más activos distribuyendo noticias criticando la actitud del gobierno de España se encontraba el perfil de Iván (@ivan226622), un ciudadano asiático (con fotografías reales) que decía ser un apasionado de la tecnología, los negocios y las noticias. Contaba con 1.287 seguidores y había publicado 580.000 mensajes desde noviembre de 2012.

Sin embargo, Iván no se correspondía con ninguna persona real, sino que formaba parte de una red de perfiles digitales falsos que, de manera coordinada, se dedicó a difundir noticias negativas sobre España durante las primeras semanas de octubre de 2017. De hecho, se pudo comprobar cómo @ivan226622 publicaba las mismas noticias negativas sobre España al mismo tiempo que otras cuentas como @rick888 o @bobbit2266, lo que sugiere que todas estas cuentas estaban gestionadas por una misma persona u organización. A las pocas semanas de ser detectadas, la red social Twitter eliminó estas cuentas al comprobarse su falsedad.

Ilustración 19.- Mensajes de Twitter con la publicación de la misma noticia desde cuentas diferentes.

Asimismo, a las coberturas digitales o cuentas híbridas también se asocia el *"falso comportamiento coordinado"*[41], término que emplea Facebook para referirse a las páginas y perfiles que trabajan de manera conjunta para engañar a los usuarios sobre quiénes son o qué

[41] GELICHER, Natahniel, '*Coordinated Inauthentic Behaviour*', Facebook, https://newsroom.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/

hacen. Por cuestiones ideológicas o financieras, estas cuentas hacen creer que son empleadas desde una parte del mundo, que difiere de su origen real.

En este sentido, la red social Facebook también ha detectado la creación de perfiles falsos en su plataforma, cuentas que ha procedido a eliminar una vez identificado su origen. El pasado 31 de enero de 2019[42], en su página oficial, la red social comunicaba el cierre de 207 páginas de Facebook, 800 perfiles y 456 grupos, *"ligadas al sindicato online Saracen Group de Indonesia"*. Según publicó Facebook en su página web, dichas cuentas se eliminaron por su comportamiento engañoso y no por el contenido que publicaban.

7.8 LAS ESTRELLAS INVITADAS

Otro elemento utilizado para difundir mensajes en una campaña de desinformación es mediante la **colaboración de personajes influyentes, que gozan de cierta credibilidad entre las audiencias potenciales** y que, sobre todo, no aparentan tener ningún tipo de vinculación o interés directo con los asuntos políticos o sociales que en discusión.

Esta aparente distancia dota a los mensajes emitidos por estos personajes influyentes de mayor credibilidad y objetividad. Sin embargo, existe la posibilidad de que estas personas tengan vinculaciones políticas o económicas con agentes encubiertos y que sus mensajes formen parte de una estrategia de desinformación que las audiencias finales desconocen.

7.9 ALGORITMOS, CÁMARAS DE RESONANCIA Y REDES DE CONFIANZA

Los algoritmos que utilizan las nuevas plataformas de comunicación digital, como las redes sociales, se han convertido en aliados involuntarios de las campañas de desinformación. Estas tecnologías no priorizan que el usuario final reciba informaciones variadas y plurales sobre la actualidad política, social o económica. Por el contrario, los algoritmos usados por estas empresas tecnológicas están diseñados para que el usuario reciba e interactúe, únicamente, con mensajes que potencialmente pueden ser de su agrado y reafirmen sus ideas.

De esta manera, las plataformas de comunicación ofrecen información a sus usuarios en función de sus preferencias políticas, no en función de la calidad, pluralidad o veracidad de los contenidos.

Esta circunstancia favorece la creación de cámaras de resonancia en la conversación digital, donde **desaparece el debate y las comunidades digitales en disputa únicamente radicalizan y reafirman sus posturas en lugar de dialogar en un debate razonado**.

7.10 LOS ANUNCIOS PAGADOS

La creación de estas cámaras de resonancia por parte de los algoritmos ha favorecido la difusión masiva de acciones de desinformación por parte de agentes encubiertos. Los responsables de las campañas de desinformación han comprobado la eficacia de crear contenidos sobre aquellos

[42] GELICHER, Nathaniel, *`Taking down coordinated inauthentic behavior in Indonesia'*, Facebook, https://newsroom.fb.com/news/2019/01/taking-down-coordinated-inauthentic-behavior-in-indonesia/

temas más polémicos en el debate digital de un país y **promocionarlos mediante campañas de pago entre cada una de las cámaras de resonancia que se crean en estos debates**. De esta manera, cada una de las comunidades enfrentadas se siente identificada con este contenido, interactúa con él y se fomenta la polarización social y el enfrentamiento entre la opinión pública.

Esta fue la estrategia que, según un informe del Comité de Inteligencia de la Casa de los Representantes de Estados Unidos, utilizó Rusia para interferir en las elecciones presidenciales del año 2016. Según esta investigación, la Agencia de Investigación de Internet (IRA, por sus siglas en inglés) con base en Rusia, pagó a Facebook la promoción de más de 3.000 mensajes[43] (no firmados ni identificados) destinados a polarizar a los ciudadanos estadounidenses en torno a los debates más polémicos del país.

De esta manera, la IRA pudo financiar de manera encubierta campañas a favor de la integración de la comunidad musulmana y, al mismo tiempo, campañas que fomentaban la islamofobia, tal y como se muestra en las siguientes imágenes, incluidas en el informe de la Casa de Representantes de Estados Unidos.

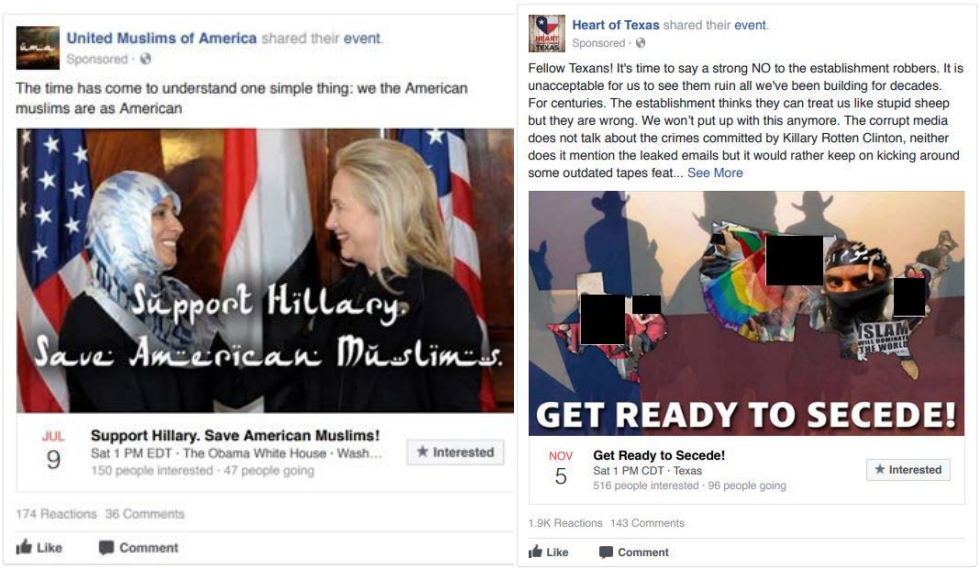

Ilustración 20.- Imágenes incluidas en el informe de la Casa de Representantes de Estados Unidos.

8. DECÁLOGO DE RECOMENDACIONES

Evitar ser víctimas de una campaña de desinformación no es responsabilidad de un único agente. **Las instituciones públicas tienen la obligación de desarrollar las capacidades necesarias para prevenir, detectar y neutralizar las ofensivas de desinformación** que se generan contra un Estado.

Asimismo, **las empresas privadas tienen la obligación de evitar que sus plataformas digitales se conviertan en herramientas empleadas en campañas maliciosas** contra los ciudadanos y los sistemas de gobierno legítimos.

[43] THE WALL STREET JOURNAL. 2018. Release of Thousands of Russia-Linked Facebook Ads Shows How Propaganda Sharpened, by Deepa Seetharaman, Georgia Wells and Byron Tau. https://www.wsj.com/articles/full-stock-of-russia-linked-facebook-ads-shows-how-propaganda-sharpened-1525960804

Por otro lado, **la Academia tiene que seguir investigando este nuevo fenómeno y generando evidencias científicas sobre las metodologías y consecuencias** que las campañas de desinformación tienen en la opinión pública y en la gobernanza.

Sin embargo, la primera y última víctima de las guerras de comunicación son los ciudadanos. Por ese motivo, es necesario que **los usuarios de medios digitales estén prevenidos para detectar una campaña de desinformación y tengan las capacidades para evitar ser manipulados**.

	Decálogo de seguridad frente a las campañas de desinformación
1	**Analiza la fuente de las noticias que recibes y consumes:** diariamente, se reciben en nuestros dispositivos móviles decenas de impactos comunicativos con noticias que nos sorprenden, nos indignan o nos emocionan. En ocasiones, estas noticias provienen de plataformas digitales "no tradicionales" con escasa transparencia. Es importante conocer qué medio publica una noticia, cuál es su trayectoria, y qué periodistas, empresas o países se encuentran detrás de la publicación[44]. En este sentido conviene que existan enlaces que redirigen la información a sus fuentes originales o a otros textos que validan los datos.
2	**Duda de los pantallazos o *screenshots* que recibas por redes sociales:** cuando recibas alguna noticia en formato de imagen, es recomendable mostrar siempre una dosis de prudencia y escepticismo. Existen multitud de software y programas informáticos, de muy fácil uso, que permiten retocar o modificar imágenes con falsos titulares de medios de comunicación tradicionales o de cuentas y perfiles en redes sociales de personas reales. Del mismo modo, es muy común sacar imágenes fuera de contexto, disociando la toma real con el titular, y dando verosimilitud a una historia falsa. Si dudas de la realidad de algunos de estos mensajes, es recomendable acudir siempre a la fuente original con sus enlaces en Internet o hacer lo que se denomina "búsqueda inversa" para saber si una foto ya fue publicada antes en Internet[45].También es posible comprobar si una imagen es original o ha sido copiada a través de la información EXIF.
3	**¿Quién te ha compartido la noticia y en qué contexto?:** no des credibilidad a todos los mensajes que lees en redes sociales, especialmente a mensajes o comentarios publicados por cuentas y perfiles anónimos. Pregúntate, aunque te lo haya enviado un amigo, qué fecha tiene la información, quién es la fuente y qué otros medios lo han difundido. Incluso conviene buscar el titular en algún buscador, porque, si es verdadero, otros medios lo habrán recogido. Da credibilidad sólo a noticias compartidas por fuentes reales[46].
4	**Ojo con las falsas cuentas "humanas":** cada vez con mayor frecuencia, están surgiendo en las redes sociales cuentas con aparente aspecto humano, pero que, en realidad, están manejadas por robots o por terceras personas a cargo de controlar diversos perfiles. Antes de seguir o de confiar del contenido publicado por un perfil digital, analiza a cuántas personas sigue, cuántas personas le siguen, si genera contenido propio, si hace un excesivo uso de la red social… Todos ellos son indicadores para detectar falsos perfiles digitales en las redes sociales.[47]

[44] Existen diversos organismos, medios de comunicación y portales web destinados a confirmar o desmentir datos. Es el caso de la web española Maldito bulo, miembro del grupo de expertos de Alto Nivel de la Comisión Europea, BSDetector, Snopes o FactCheck.
[45] Existen diversas herramientas que lo permiten, como RevEye, que funcionan como una extensión para los navegadores Chrome y Firefox y busca en varios bancos de imágenes de la web. Google Imágenes también tiene una función similar, así como TinEye. También es posible contar con herramientas que verifican los vídeos como Google Earth (para comparar la geografía o los sitios de interés donde fue grabado) o YouTube Data Wiewer para saber la hora en la que el video fue subido y que extrae pantallazos para saber si hay otras versiones del video disponibles en internet, y si fueron publicadas antes o después.
[46] Las propias redes sociales, en su mayoría, cuentan con información y buenas prácticas para evitar las noticias falsas y caer en cadenas de difusión. Es el caso de Facebook, Google o Twitter
[47] *Crowdtangle* es una herramienta que Facebook adquirió en 2016 y monitoriza cómo se está 'moviendo' un contenido en redes sociales o **Foller.me** que determina si un perfil es engañoso o no. Son indicios el que el perfil "converse" con pocas cuentas, si tiene picos muy altos de actividad o su fecha de creación.

5	**No seas parte del algoritmo:** las plataformas digitales que utilizamos diariamente para comunicarnos e informarnos están basadas en un complejo algoritmo que nos ofrece información personalizada en función de nuestros supuestos gustos, aficiones u opiniones. De esta manera, las propias plataformas digitales nos ofrecen aquella información que el software considera que va a ser de nuestro agrado. Si queremos desarrollar una opinión bien formada, crítica y contrastada, es recomendable obtener fuentes de información alternativas a aquellas que, por defecto, nos muestran los algoritmos de las plataformas de comunicación.
6	**Lee la letra pequeña:** las acciones de desinformación más exitosas son aquellas que se sustentan en medias verdades. Las noticias falsas son relativamente fáciles de detectar y desmontar. Sin embargo, en muchas ocasiones, los promotores de la desinformación utilizan fotos y datos verdaderos que, presentados de manera sugerente en un titular y acompañados de una fotografía, pueden ser interpretados de manera errónea. Cuando te informes en formatos digitales, no te quedes sólo con la sensación que puede generar un titular y una fotografía. Lee la noticia completa y analiza si los datos están contrastados y si las citas y opiniones recogen pluralidad de opiniones.
7	**Mantente alerta con los contenidos patrocinados de origen desconocido:** las plataformas digitales obtienen ingresos económicos a cambio de que los usuarios patrocinen determinado contenido para que aparezca de manera destacada en el perfil de una audiencia determinada. Desconfía de todo contenido político o polémica que aparezca patrocinado por perfiles anónimos o no identificados con asociaciones, partidos políticos o instituciones reales.
8	**Desconfía de estrellas invitadas:** con frecuencia se producen casos en los que relevantes agentes políticos, sociales o culturales se involucran de manera activa en discusiones políticas o sociales de países extranjeros. La libertad de expresión y de opinión es uno de los bienes más respetables de una democracia liberal. Sin embargo, también hay que tener en cuenta que algunos de estos actores influyentes participan en determinadas discusiones en función de agendas políticas y económicas muy determinadas y que no son conocidas por la audiencia final.
9	**Pensamiento crítico y cabeza fría:** determinados agentes políticos, tanto nacionales como subnacionales, utilizan la comunicación digital para enfrentar a la opinión pública de un país extranjero y movilizar el legítimo descontento de parte de sus ciudadanos en torno a cuestiones políticas, sociales o económicas polémicas y de debate. Participar en los debates políticos enriquece la democracia y la pluralidad política. Sin embargo, es recomendable hacerlo desde la racionalidad, el respeto y el pensamiento crítico, evitando generar espirales de odio y descalificaciones, que, en ocasiones, pueden estar promovidas por agentes o grupos encubiertos.
10	**Tú puedes parar un conflicto:** las acciones de desinformación contemporáneas están basadas en la rapidez y la *viralidad* con la que se extienden las noticias, los rumores y los comentarios. Todos formamos parte y somos eslabones de las campañas de desinformación. Es importante ser conscientes de que podemos ser utilizados como peones de estrategias patrocinadas y gestionadas por agentes desconocidos con intereses políticos no declarados. Por eso, es importante estar siempre alerta de los contenidos informativos que recibimos a diario en nuestros ordenadores o dispositivos móviles y no contribuir a difundir informaciones no contrastadas o de dudosa trazabilidad y procedencia.