

# PROPAGANDA Y DESINFORMACIÓN EN LAS REDES SOCIALES

EVA MOYA LOSADA

## RESUMEN

Esta reflexión pretende sentar unas bases para realizar un análisis previo que ayude a valorar si las campañas de propaganda y desinformación en las redes sociales pueden convertirse en una posible amenaza real a los intereses de nuestro país, no solo desde el punto de vista de un enfoque de seguridad, sino también desde la perspectiva de la Inteligencia Económica. Veremos cómo los últimos acontecimientos nos demuestran que las consecuencias del impacto de estas campañas sobre la sociedad cada vez son más peligrosas. Cabe pensar que la tendencia va en aumento y por lo tanto convendría que estuviera presente en nuestros planes contra posibles amenazas a nuestro país en el futuro.

*Palabras clave:* Propaganda, decepción, redes sociales, amenazas, Twitter, Facebook, inteligencia económica, seguridad y defensa.

## ABSTRACT

These considerations aim to set up a basis for a preliminary analysis as a help for assessing whether the propaganda and disinformation campaigns in social networks can become a possible real threat to the interests of our country, not only from security approach, but also from the perspective of Economic Intelligence. We will be able to identify how recent events show that the consequences of these campaigns impact on society are turning out more threatening. The trend is increasing, therefore it would be wise that these scenarios are considered in our plans against possible threats to our country in the future.

*Key words:* Propaganda, deception, social network, threat, Twitter, Facebook, economic intelligence, security and defence.

## 1. INTRODUCCIÓN

Se ha pretendido abordar el tema de la propaganda y decepción en redes sociales a raíz del incremento de la presencia gubernamental internacional directa o indirecta en la Red, entre otros, debido al aumento de los ciberataques y el ciberespionaje con origen en EEUU y China. Actualmente, nos enfrentamos a una Red cada vez más regulada, donde la convivencia entre las diferentes culturas, filosofías y leyes se ha vuelto muy compleja.

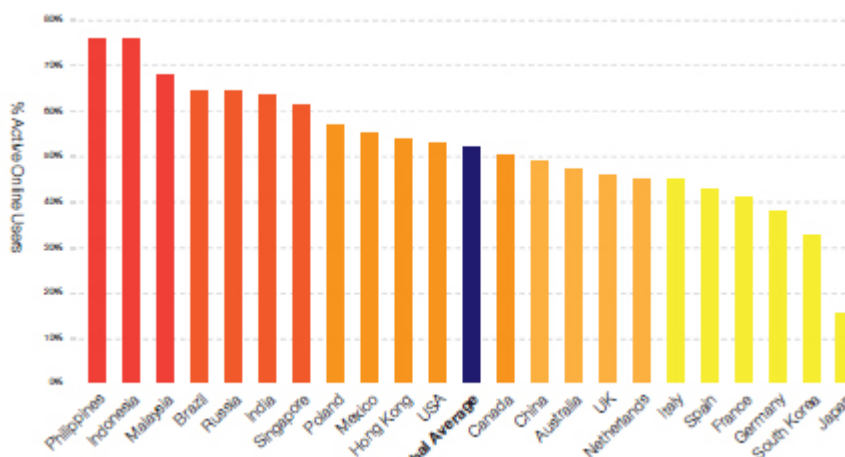
En este sentido, el término “propaganda” en este artículo se refiere a aquellas campañas de comunicación dirigidas a impactar sobre distintos públicos objetivos con la intención de sensibilizarles, hacerles partícipes e incitarles a la acción sobre alguna causa. Estas campañas se particularizan especialmente por un lenguaje emocional que sólo muestra a los públicos objetivos el lado interesado de quienes realizan la

campaña. Por tanto, no se busca informar. En cuanto al concepto “decepción”, lo consideraré como aquellas actuaciones en las redes sociales que buscan engañar, tanto con los mensajes como a través de las cuentas de usuario que lo transmiten.

Si bien es cierto, que para iniciar este camino reflexivo se hace necesario un resumen del estado de la situación actual, en relación al alcance y expansión de las redes sociales, no quiero profundizar demasiado al respecto, pues abundan los informes estadísticos que demuestran que son un fenómeno todavía en expansión y sobre todo en reformulación. Si vemos algunas de las últimas cifras entenderemos que todavía queda mucho camino por recorrer y que, lejos de desaparecer, están evolucionando hacia una nueva etapa, donde la comunicación se convierte ya en un bien innegociable para cualquier ciudadano.

Según el último informe de la Fundación Telefónica sobre la Sociedad de la Información en España, durante el año 2012 se observa que la penetración de las redes sociales crece en 6,5 puntos porcentuales hasta alcanzar el 63,7% de los internautas<sup>1</sup>. Comparando estas cifras con años anteriores, comprobamos que la curva de ascenso en su penetración es cada vez más suave y por tanto podemos llegar a la conclusión que, en España, han dejado tiempo atrás la fase de “tecnología emergente”. Ya no es una manifestación emergente o novedosa, sino que es un fenómeno que se está acercando a ser considerado de “masas”, especialmente si hablamos de los países occidentales y si fijamos nuestra atención en las jóvenes generaciones. En nuestro país no hay adolescente que no tenga una cuenta en Facebook, Tuenti o Twitter. Cabe recordar que los jóvenes de hoy serán los adultos que tomen las decisiones de mañana. Por eso es vital entender cómo se relacionan con este medio.

Por otro lado, si observamos el resto de los países del mundo, podemos comprobar que se enfrentan a una situación bastante similar a la española. Aunque de 2011, y seguramente con porcentajes aproximativos, el informe sobre penetración de las redes sociales<sup>2</sup> de la consultora Global Web Index muestra cómo los usuarios conectados en todo el mundo a las distintas plataformas sociales superan ya el 50% de su población.



Fuente: Global Web Index. **Global Social Network Penetration**

- 1 FUNDACIÓN TELEFÓNICA. La Sociedad de la Información en España en 2012, Madrid: Editorial Ariel, 2013, p. 12.
- 2 GLOBAL WEB INDEX. Global Map of Social Networking. 2011. <http://globalwebindex.net/wp-content/uploads/downloads/2011/06/Global-Map-of-Social-Networking-GlobalWebIndex-June-20112.pdf>.

Los usos siguen siendo diversos. Pero, en términos generales, podemos señalar dos que destacan muy por encima de los demás cuando se les pregunta directamente a los usuarios<sup>3</sup>: Facebook se utiliza básicamente para estar en contacto con los amigos y conocidos, mientras que Twitter tiene una finalidad meramente informativa, como si de un periódico o pase de teletipos se tratase.

Si hemos hecho este pequeño resumen de la situación actual es porque conocer en profundidad los canales y su público objetivo nos permitirá determinar las amenazas reales que pueden venir a través de ellos.

Así pues, en este sentido, podemos comenzar a extraer algunas pequeñas conclusiones iniciales, como por ejemplo que Facebook es la red social favorita para establecer relaciones y que, por lo tanto, puede ser el canal ideal a través del cual grupos terroristas y activistas peligrosos se acerquen directamente al usuario para dar a conocer sus ideologías e incluso organizar y coordinar sus futuras actuaciones. Además, Facebook puede ser una magnífica herramienta para formar a futuros miembros de estos grupos y realizar acciones de captación.

Mientras, por otro lado, aprovechando que Twitter es la red social informativa por excelencia, puede ser utilizada para poderosas campañas de desinformación, manipulando a la opinión pública de las redes con todo tipo de contenidos, y de ruido buscando incluso distraerla en un momento dado de cuestiones más importantes o sensibles. A este respecto los hashtag (palabras clave entorno a las cuales se organizan los contenidos de Twitter y que van señaladas con el símbolo “#”) podrán ser utilizados como semillas para realizar campañas de propaganda de cualquier tipo e incitados correctamente a la viralización pueden convertirse en Trending Topic (TT) en menos de 24 horas, para obtener un mayor alcance a muy bajo coste. A día de hoy quienes más han sufrido este tipo de ataques han sido grandes compañías como, por ejemplo, Nestlé en la crisis del aceite de palma. Fue cuando Greenpeace detectó que uno de sus proveedores participaba en la deforestación de los bosques de Indonesia, afectando a la supervivencia de los orangutanes que vivían en ellos, y consideró oportuno lanzar una fuerte campaña de propaganda en las redes sociales para incitar a los consumidores a dejar de consumir Kit Kat<sup>4</sup> y forzar un cambio en la política medioambiental de la compañía.

Si bien las grandes noticias vinculadas a las crisis en redes sociales han dado lugar a expresiones del tipo “las redes sociales cargan tintas contra...”, “crisis en las redes sociales...”, etc. Es fundamental comprender que son meras plataformas o herramientas de comunicación y que, cuando se utilizan este tipo de expresiones, se hace referencia al contenido que hay en ellas.

Quiero profundizar a continuación sobre esta idea, pues nos obliga a entender mejor cómo funcionan y por dónde pueden venir las vulnerabilidades asociadas a ellas.

---

3 THE COCKTAIL ANALYSIS. 5ª oleada del Observatorio de Redes Sociales, 16 de abril de 2013, p12. <http://es.slideshare.net/TCAnalysis/5-oleada-observatorio-redes-sociales>

4 GREENPEACE. Nestlé and palm oil, 17 de marzo de 2010. <http://www.greenpeace.org.uk/nestle-palm-oil>

## 2. LAS REDES SOCIALES SON HERRAMIENTAS, NO CONTENIDOS

El lenguaje es uno de los grandes avances del ser humano. Gracias a él podemos comunicarnos y, a veces, hasta entendernos. El lenguaje es algo vivo que nos acompaña a lo largo de toda nuestra vida, desde que balbuceamos nuestras primeras palabras. Es, pues, un compañero que nos apoya en nuestras relaciones personales y profesionales.

En un contexto tan cambiante como el actual, y ante la celeridad en la aparición de nuevas tecnologías, el lenguaje se adapta en la formulación de conceptos para describir nuevos contextos y nuevas herramientas.

Si queremos profundizar en el estudio de la comunicación online es imprescindible conocer varios aspectos propios de la naturaleza de Internet. Saber, por ejemplo, cómo funcionan aquellas aplicaciones a través de las cuales puede realizarse una campaña de propaganda o de decepción nos permite prever cómo pueden ser originadas, sus puntos fuertes y sus puntos débiles para ser contenidas, etc. Pero, eso sí, no debemos confundir la herramienta que nos ofrece múltiples opciones creativas, con el contenido que se transmite a través de ellas.

### 2.1. EL ENTORNO “WEB 2.0”

La web 2.0 es un concepto nacido de una tormenta de ideas en el FOO Camp de 2004. Surge de la mano de Tim O’Reilly, ferviente impulsor del software libre y código abierto, para definir la nueva generación de software que aparecía en Internet en aquellos años. Por aquel entonces se percibía que algo había cambiado en la gran Red y se analizaban nuevos modelos de negocio que estaban apareciendo con bastante éxito y que nada tenían que ver con la etapa anterior, uno de ellos por ejemplo es la conocida tienda online Amazon.

“Tú controlas tu propios datos”<sup>5</sup> es la clave del meme que resume la tormenta de ideas de O’Reilly Media y que nos interesa especialmente para este artículo. Porque en la nueva Internet nosotros decidimos qué datos publicamos o qué información compartimos, aunque la mayoría de las veces subamos a las redes sociales de forma espontánea cualquiera de nuestros comentarios derivados de nuestro estado emocional del momento. A este respecto, hoy día hay abierto un debate muy importante sobre la privacidad de los individuos en estas plataformas. Debate en el que no vamos a entrar a reflexionar en este documento, porque su extensión bien daría lugar a un monográfico.

A medida que se avanzaba en las reflexiones sobre la evolución del mundo de Internet, el propio O’Reilly desveló en ocho claves las bases que definirían los modelos de negocio web 2.0 de hoy en día (2006: O’Reilly). De estas ocho claves he querido resaltar aquellas que afectarán directamente al comportamiento del usuario, que es quien en la mayoría de los casos genera el contenido, a través de sus consultas o compartiendo cualquier tipo de información.

Veamos tres de las ocho claves que he decidido vincular a tres elementos fundamentales que facilitan el éxito de las redes sociales como herramientas de

---

5 O’REILLY, Tim. Design Patterns and Business Models for the Next Generation of Software, 2005. <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1#mememap>

comunicación y que, por tanto, convienen a nuestro objeto de reflexión:

1. Aprovechamiento de la Inteligencia Colectiva – Participación. Los desarrollos tecnológicos en Internet en los últimos años contemplan estructuras que facilitan la interpretación de los datos y metadatos generados por los usuarios. Es por ello que este tipo de software fomenta la participación y la interacción, volviendo la Red más democrática y social. Son los propios usuarios los que comparten, intercambian, debaten, etc. Cuanta más información, más interesante se volverá la herramienta. Un ejemplo claro es la Wikipedia.
2. Enriquecimiento de las experiencias de usuario – Facilidad en la comunicación. Los usuarios se están adaptando rápidamente a las nuevas posibilidades de las aplicaciones en Internet, evolucionando con ella y demandando constantemente mejoras y nuevas opciones, a cada cual más creativa. El caso de Pinterest es otro ejemplo claro de cómo un cambio en la distribución de contenidos publicados en una red social puede agilizar y enriquecer la comunicación. Desde su aparición son ya varias redes sociales las que están copiando su estructura. Importante es también hablar de los nuevos formatos en los que se “encapsula la información”. La posibilidad de compartir vídeos en Youtube ha demostrado cómo los formatos multimedia vuelven mucho más atractivo cualquier contenido llegando a generar más de varios billones de vídeos visitados al día en todo el mundo.
3. Software por encima del nivel de un dispositivo único – O Internet ubicua<sup>6</sup>. Sin límites temporales ni espaciales. Los avances en las telecomunicaciones y los dispositivos móviles han favorecido el salto de Internet más allá de las fronteras marcadas por el ordenador de mesa. Los usuarios pueden acceder a una misma aplicación desde cualquier tipo de dispositivo en cualquier momento y lugar. Por ejemplo, podemos consultar nuestro email desde cualquier dispositivo que tengamos a nuestro alcance.

## 2.2. LA TECNOLOGÍA DE LAS REDES SOCIALES COMO PUERTA DE ENTRADA A LA PROPAGANDA Y LA DESINFORMACIÓN

La primera red social virtual surgió en 1997 bajo el nombre de SixDegrees aludiendo al relato “Chains” de Frigyes Karinthy para sugerir una aplicación práctica derivada del concepto desarrollado años después por el sociólogo Duncan Watts sobre la posibilidad de estar conectados con cualquier persona del planeta en seis “saltos relacionales”. Por aquel entonces, la primera red social, aunque limitada, ya contemplaba la creación de perfiles personales que se podían conectar entre sí.

Aunque SixDegrees se mantuvo abierta sólo unos años, le siguieron otras como Myspace u Orkut, que demostraron que este tipo de plataformas tecnológicas podían llegar a conectar a millones de usuarios en todo el mundo sin demasiados problemas ni limitaciones.

Finalmente, y más de nuestros tiempos, podemos disfrutar de herramientas como Facebook, Twitter, Youtube, Instagram o FourSquare.

6 BIRKENBIHL, Klaus; QUESADA, Encarna y PRIESCA BALBÍN, Pablo. Presente y futuro de la world wide web, Madrid: Novática, Revista de la Asociación de Técnicos de Informática, 2009, nº197, p.5.

Estas nuevas redes sociales son plataformas donde cualquier individuo, desde cualquier parte del mundo y de forma anónima, puede inyectar en la Red global cualquier contenido en forma de textos, imágenes, fotografías, animaciones, vídeos, urls, geoposicionamientos, códigos QR, videojuegos, etc.

Pero estas herramientas tienen dos debilidades, entre otras, que pueden motivar y facilitar especialmente actuaciones propagandísticas o de desinformación.

La primera de ellas, que trataremos brevemente, es la posibilidad de vivir en el anonimato. Contrariamente a lo que sucede con un email, las IP de los perfiles creados en redes sociales no se pueden rastrear directamente hasta el usuario (salvo aquellas en las que el propio usuario ha decidido “geolocalizarse”), sino que el resultado nos llevará a Silicon Valley o a cualquier otro lugar relacionado con las IP propias de las plataformas que estamos intentando rastrear. Es por ello que muchos perfiles mal intencionados utilizan sus cuentas de usuario anónimas para realizar amenazas, generar bulos o incluso funcionan como malware. Por tanto, lanzar una campaña de propaganda y/o desinformación a través de estas plataformas puede tener cierta cobertura de anonimato si se desea, al menos en sus comienzos.

Por otro lado, este anonimato puede ser más o menos mantenido y organizado mientras las conversaciones entre los coordinadores de la campaña sean privadas. Por tanto es un medio mucho más seguro que la comunicación vía email. Por ello, el gobierno americano lleva tiempo solicitando a estas grandes compañías informaciones propias de usuario que pueda ayudarles a obtener más información como parte de una estrategia global de ciberespionaje ordenada por el presidente Barack Obama<sup>7</sup>, en la que no quieren que se les escape nada.

La segunda de las vulnerabilidades vamos a abordarla con más profundidad por las consecuencias que puede generar.

### **Los ciberataques a las cuentas de usuario como vía para las campañas de propaganda y decepción.**

Una de las vulnerabilidades tecnológicas principales de estas herramientas y que se está utilizando a día de hoy, especialmente para campañas de desinformación, es el pirateo de cuentas de usuario.

Llevamos unos años ya conociendo, a través de los medios de comunicación, cómo piratas informáticos se introducen en cuentas de Facebook o Twitter para falsear los mensajes de sus usuarios. Las víctimas favoritas: artistas y personajes relevantes como futbolistas, del mundo de la farándula, etc. Pero en los últimos tiempos también los políticos, como le ha pasado al presidente Maduro en Venezuela<sup>8</sup>, al que Anonymous ha metido en varios apuros.

Cuando nos enteramos que la cuenta de Twitter de un actor o cantante famoso ha sido vulnerada puede incluso hacernos gracia o despertar cierta simpatía. El impacto,

---

7 Obama tells intelligence chiefs to draw up cyber target list – full document text, The Guardian, 7 de junio de 2013. <http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text>

8 Piratean de nuevo la cuenta de Nicolás Maduro en Twitter, CNN España, 12 de mayo de 2013. <http://cnnespanol.cnn.com/2013/05/12/piratean-de-nuevo-la-cuenta-de-nicolas-maduro-en-twitter/>

dependiendo del mensaje, no va más allá de una sorpresa, enfado y unas disculpas del propietario real cuando es consciente de que le han robado su identidad.

En este sentido, uno de los últimos ejemplos que puede parecer trivial, porque muestra el poder de este tipo de actividades, fue otro de los llevados a cabo por Anonymous. Aprovechando la rivalidad, conocida a nivel mundial, entre los dos gigantes de comida rápida McDonalds y Burger King reventó la cuenta de Burger King y la personalizó como si fuera de McDonalds.

Así quedó Burger King después de que Anonymous entrara en ella. *“Burger King ha sido vendida a Mc Donalds porque la whopper es un fracaso”*.



*Fuente: BurgerKing Twitter*

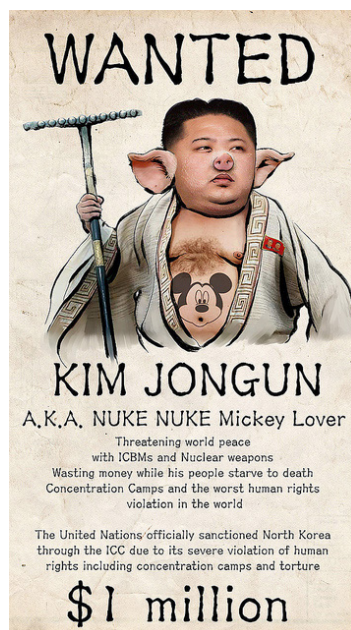
Por suerte, no tardaron demasiado tiempo en darse cuenta y retomar el control de la situación. Y para evitar tensiones derivadas de un choque entre rivales, la propia McDonalds se solidarizó con Burger King contestando con un mensaje neutral en tono de humor. Finalmente todo acabó como una pequeña broma sin consecuencias demasiado graves.

Pero, ¿qué ocurre cuando las cuentas pirateadas son de perfiles tan relevantes como políticos, organizaciones o agencias de comunicación? ¿Cuáles pueden ser los riesgos y/o amenazas?

Quizá el lector pueda pensar que las consecuencias tampoco serían demasiado graves. Ciertamente hay casos dirigidos simplemente a dañar la reputación como le sucedió a Kim Jong en abril de 2013. Como consecuencia del aumento de la tensión entre Corea del Norte y la comunidad internacional, la cuenta en Twitter @uriminzok utilizada por el gobierno Coreano para realizar sus propias campañas de propaganda<sup>9</sup> fue pirateada<sup>10</sup> con mensajes e imágenes como la siguiente.

9 North Korea using Twitter for propaganda, The Sidney Morning Herald, 15 de agosto de 2010. <http://www.smh.com.au/technology/technology-news/north-korea-using-twitter-for-propaganda-20100815-1250u.html>

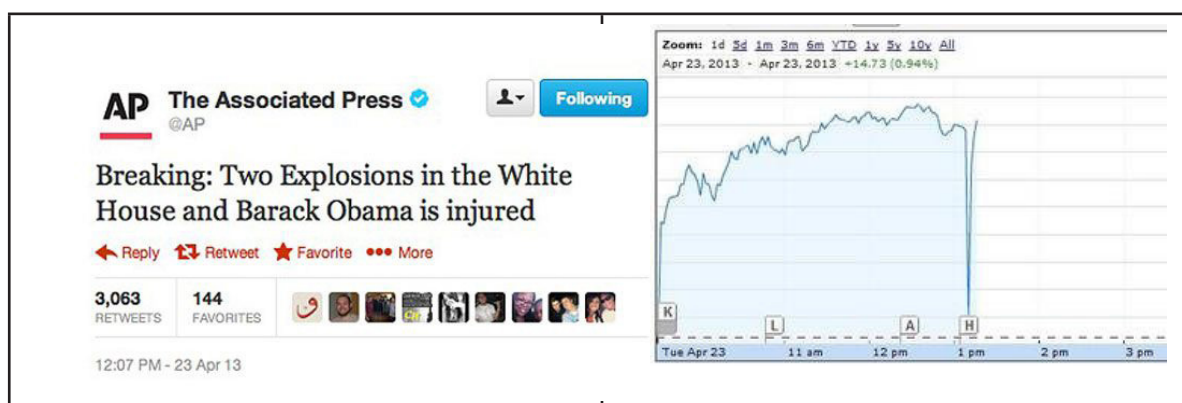
10 LEE, Youkyung. NKorea's Twitter account hacked amid tension, The Associated Press, 4 de abril de 2013. <http://bigstory.ap.org/article/nkoreas-twitter-account-hacked-amid-tension>



Fuente: Twitchy.com<sup>11</sup>

Evidentemente, este ciberataque no va más allá de una mofa internacional que puede haber herido más o menos el orgullo de los norcoreanos.

Sin embargo, ya tenemos un primer caso más serio. Sucedió después de que el perfil en Twitter de la agencia de noticias AP fuera pirateado por los autoproclamados Syrian Electronic Army (SEA). El siguiente mensaje “*Dos explosiones en la Casa Blanca. Obama está herido*” generó el pánico en Wall Street durante unos pocos segundos, hasta que se confirmó la falsedad de la noticia. Inmediatamente después se 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 pueden provocar en la sociedad. ¿Somos conscientes que por un segundo se perdieron 145 puntos en el índice bursátil más referenciado del mundo?



Fuente: La Vanguardia<sup>12</sup>

- 11 Hacking of North Korea's Twitter and Flickr accounts includes pic of Kim Jong Un with a snout, Twitchy, 4 de abril de 2013. <http://twitchy.com/2013/04/04/hacking-of-north-koreas-twitter-and-flickr-accounts-includes-pic-of-kim-jong-un-with-a-snout/>
- 12 FORT, Màrius. 'Minicrash' en Wall Street por un falso tuit sobre un atentado contra Obama, La Vanguardia, 24 de abril de 2013. <http://www.lavanguardia.com/economia/20130423/54372747540/minicrash-wall-street-hackeada-cuenta-twitter-associated-press.html>.



Como hemos comentado anteriormente Twitter se ha convertido en los últimos años en una fuente de información relevante gracias a su flexibilidad, frescura e inmediatez. Prueba de ello es que, un año más, el uso de esta red social por parte de periodistas ha aumentado. Según el 6º Informe de la consultora Oriella, en 2012 el número de periodistas que usaban Twitter era del 47%, mientras que en 2013 ya es un 59%<sup>13</sup>. Es evidente que situaciones vividas como las revoluciones del mundo árabe o la catástrofe del terremoto de Chile han empujado al sector de la información a adaptarse a este nuevo medio.

Así pues, miles de profesionales viven pendientes de lo que se comenta y se anuncia en esta red social. Incluso los analistas de inteligencia estamos aprendiendo a utilizar este nuevo recurso como fuente de información para nuestros informes basados en OSINT (Open Source Intelligence).

Si bien es cierto que actualmente Twitter trabaja en un sistema de doble contraseña para reforzar la seguridad de sus cuentas de usuario, no debemos dejar todo el peso de la seguridad sobre la plataforma tecnológica.

Cabe preguntarse si desde la comunicación corporativa, tanto pública como privada, en nuestro país se contemplan estas situaciones como amenazas potenciales que podrían darse en un momento dado. ¿Qué ocurriría si la cuenta en Twitter de la Policía Nacional (@policía) pudiera ser pirateada y emitiera un mensaje que incitara al pánico? Actualmente es una cuenta que siguen más de 400.000 seguidores. ¿Imaginamos el impacto y la velocidad de viralización que tendría en toda la Red? Evidentemente hay cuentas más o menos fáciles de piratear en función de lo cuidadosos que sean sus gestores. Pero considero que es algo que debemos contemplar y profesionalizar en nuestros planes de crisis de comunicación y/o reputación, especialmente en relación a cuentas sensibles de nuestro país en las redes sociales.

### 3. NUEVOS ACTORES, NUEVAS ESTRATEGIAS

El éxito demostrado en el aumento de la visibilidad derivada de una buena presencia en las redes sociales ha generado una aparición de nuevos actores que no se había visto hasta hace muy poco tiempo. 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.

Un interesante ejemplo del uso de Twitter como canal de comunicación gubernamental fue protagonizado por el gobierno egipcio, de los Hermanos Musulmanes, cuando utilizaron una de sus cuentas de Twitter para darle un tirón de orejas público al Departamento de Estado de los EEUU por lo que ellos consideraban una falta de respeto a la religión musulmana, a raíz de unos comentarios satíricos realizados por la portavoz Victoria Nuland contra Bassem Youssef y las religiones. La peculiaridad no es sólo el contenido del mensaje, sino el hecho de ver cómo Los Hermanos Musulmanes de Egipto utilizan los códigos de Twitter para dirigirse al gobierno americano, llegando a mencionarle directamente a través de la "@" e incluyendo un hashtag bastante popular como es el #FJP (Freedom and Justice

13 ORIELLA PR NETWORK. Global Digital Journalism Study 2013. <http://www.oriellapnetwork.com/research>

Party) para hacer todo el ruido posible con la esperanza de convertirlo en un tweet viral.



*Fuente: Ikhwanweb Twitter*

Cabe preguntarse qué pasaría si un gobierno cualquiera decidiera emitir a través del social media cualquier mensaje mencionando a nuestro país. ¿Tenemos los protocolos y recursos para responder? Quizá a día de hoy nos parezca que esto nos queda lejos. Pero la evolución de la tendencia es evidente: muchos gobiernos del mundo, no sólo presidentes o corte política, ya tienen su propia voz en Twitter para hablar cara a cara con los ciudadanos, sin intermediarios de ningún medio de comunicación que reinterprete sus palabras. ¿Cómo respondería la cuenta de uno de nuestros ejércitos si recibiera una crítica a través de las redes sociales acusándole de bombardear a civiles despiadadamente? Podría ser perfectamente parte de una campaña contra la presencia de la OTAN surgida en cualquiera de los países en los que estamos presentes. Por tanto ni siquiera España tendría que ser el objetivo final de la campaña. Evidentemente nos pondría en un aprieto si los medios de comunicación lo convirtieran en noticia hasta que se demostrara la falsedad.

Ahora bien, en este tipo de medios, la premura es vital. ¿Estamos preparados como país para escuchar lo que se dice de nosotros en las redes sociales? Y recordemos que no estar en las redes con cuentas de usuario gubernamentales ya no es una defensa, incluso puede considerarse un posible riesgo, puesto que el ataque viene por este canal y habrá que saber canalizarlo a través de él.

Sin duda, uno de los países que hoy por hoy utiliza la estrategia más agresiva en la gran Red, y que es un ejemplo claro de propaganda, es la que lleva ya tiempo realizando el estado de Israel. Además de haberse tomado muy en serio la formación de una unidad de ciberguerreros<sup>14</sup>, ha optado por utilizar varias de sus cuentas de Twitter como canales de propaganda, cubriendo las 24 horas del día Twitter con mensajes de todo tipo y en todos los idiomas, con la intención de llegar a cualquier rincón del mundo virtual. Como podemos ver en estos dos ejemplos de tweets sus campañas son realmente muy directas.

14 GREENWOOD, Phoebe. Israel invests millions in drive for elite 'cyber warriors', Telegraph, 1 de noviembre de 2013. <http://www.telegraph.co.uk/news/worldnews/middleeast/israel/9648820/Israel-invests-millions-in-drive-for-elite-cyber-warriors.html>



**FDI**  
@FDIonline

**¡No te dejes engañar! La prioridad de #Hamás es el terror; ayudar a los civiles de #Gaza queda en segundo lugar [goo.gl/ySiqZ](http://goo.gl/ySiqZ)**

8:00 PM - 30 May 2013



**IDF** ✓  
@IDFSpokesperson



**New #Hamás Legislation: Gender Segregation for #Gaza's Schools [ow.ly/jIg8e](http://ow.ly/jIg8e)**

9:00 PM - 3 Apr 2013

*Fuente: FDIonline y IDFSpokesperson Twitter*

Hasta ahora hemos hablado de gobiernos como nuevos actores. Pero también podemos hablar de políticos o presidentes. En este sentido otro gran personaje con presencia relevante en las redes sociales, especialmente en Facebook, es la actual presidenta de Argentina Cristina Fernández Krichner, una gran fan del social media, de hecho su influencia en Klout pasa de los 80 puntos<sup>15</sup>, un valor de influencia en los medios sociales muy elevado. Conocedora de este tipo de medios, mantiene sus cuentas de Twitter<sup>16</sup> y Facebook<sup>17</sup> muy activas y las utiliza para dar su punto de vista sobre todo lo que sucede en Argentina. Puede que desde España nos resulte extraña la hiperactividad que demuestra en la Red, sin embargo no podemos negar que le da muy buenos resultados. Hace poco tuvo que asumir varias críticas por su gestión en las recientes inundaciones. Aprovechando que una de ellas le había llegado a través de su cuenta en Facebook, decidió contestar públicamente sabiendo que tendría un impacto sobre su reputación mucho más elevado que haciendo un simple 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” demuestran que la señora Krichner es una gran conocedora de la comunicación en este tipo de plataformas. Además, aprovechó para utilizar fotografías que demostraban cómo había respondido inmediatamente con hechos, no sólo palabras. En definitiva, convirtió una situación que podía haber dañado su reputación en otra de la que salió todavía más reforzada.

15 <http://klout.com/#/CFKArgentina>

16 [@CFKArgentina](https://twitter.com/CFKArgentina)

17 <https://www.facebook.com/CFKArgentina>

Cristina Fernández de Kirchner Fotos Me gusta

### Ayuda a los damnificados por el temporal en Villa Elvira

Actualizado Hace aproximadamente 2 meses

Para Cecilia Cavallaro de Villa Elvira: Quiero contarte que llegamos a las familias del arroyo Maldonado gracias a tu mensaje del sábado. Es lógico que tengas dudas y está bueno que las expreses. Te envío las fotos por si no pudiste enterarte del trabajo realizado por un grupo de jóvenes militantes. Los chicos salieron desde la Fac. de Periodismo y fueron hasta el lugar con maderas, chapas, colchones y todos los elementos para ayudar al prójimo. El responsable del grupo es Horacito Ríndose, diputado nacional, hijo de detenidos desaparecidos. Nunca conoció ni conocerá a sus padres. No sé si te interesa el tema pero es bueno ver a jóvenes, que tendrían derecho a estar enojados con el mundo y desconfiar

de todo y de todos y sin embargo, no. A lo mejor es cuestión de ADN, no? Me acuerdo del último cumpleaños de Néstor, 25/2/2010. Horacito estaba junto a Abuelas y Madres de Plaza de Mayo en Olivos. Ríndose se acercó a Néstor y a mí y nos dijo "Ya que no puedo sacarme una foto con mis viejos me saco una con ustedes". A mí se me aflojaron las piernas y casi me pongo a llorar, la foto la tengo en mi despacho en la Rosada. Estoy con una cara, haciendo pucheros, él y Néstor riéndose. Para suerte de todos los argentinos están con la alegría del que puede ayudar al otro. Gracias Cecilia por avisarnos, no te conozco pero te mando un abrazo. Cristina.

Cecilia Cavallaro Buenas medidas, como ud dijo, esperamos que lleguen a las que realmente lo necesitan. Yo vivo en Villa Elvira y me allí tocado ver con mis propios ojos, situaciones de familias tan para sus familiares, que no se atreven ni a pedir, ni recibir nada. Dudo que tengan internet, en las casitas de madera y cartón que "TIENDAS" porque ya no las tienen, a los orillas del brazo del Arroyo Maldonado. Dudo que puedan entender de las medidas que ud está anunciando, dudo que, así como ningún camino de colchones, ropa, alimentos, ni medio de comunicación para por allí, alguien se llegue para ofrecerles salir de esa trampa mortal en donde viven. Fundamentalmente las viviendas afectadas son 80/90 entre 10.1.12.13.14. Los vecinos de algunas cuadras de allí, los veían pasar felando sobre el arroyo, desde los techos, sin poder hacer nada. Chico de un grupo de la iglesia de la zona, que se encargaron de distribuir que ellos, comentaban que se les llevaron CHOCOS, SI CRUSTRAS, cosa que los chicos no sabían. La mayoría de ellos son inmigrantes, cosa que a mí me interesa, son vecinos y punto. Sus caras siempre llevan la expresión de "Perdidos", siempre llevan el ánimo de creer que no están haciendo lo correcto al recibir, es por eso que lo repito se sabe públicamente que sus hijos "ya no están". Una vaca fue arrestrada por la corriente, y se arrojó de cabeza en el barro, entre varios hombres de allí, la camioneta... así es. ¿Ojala haya un grupo de asistentes sociales que recorran estas zonas, y puedan comprobar lo que yo aquí manifiesto, para que se tomen las medidas prioritarias las urgencias... Saludo a ud altamente. Excelente gestión...

El sábado a las 15:29 - Me gusta - 43



Fuente: Captura del Facebook de Cristina Fernández Kirchner

El propio Barack Obama nos ha sorprendido hace meses utilizando en varias ocasiones el Hangout de Google para charlar directamente con los ciudadanos<sup>18</sup>. Y no es el único que usa las redes sociales para hablar a los ciudadanos. Mohamed Mursi ha utilizado varias veces el Facebook oficial para dar su opinión y defender su posición ante los ciudadanos y gobiernos extranjeros<sup>19</sup>.

¿Y qué podemos decir de las organizaciones Internacionales? Ellas tampoco quieren desperdiciar la oportunidad de llegar a los ciudadanos directamente, sin intermediarios.

Uno de los mejores ejemplos de que las cosas están cambiando es que, hace muy poco, la propia OTAN ha decidido dar el salto a la Red creando su propio punto de encuentro en las redes sociales, como por ejemplo a través de la creación de un canal propio en Youtube, donde muestran ejemplos de sus campañas y su labor "más social".

Aunque evidentemente exponerse a luz pública a través de las redes sociales significa un riesgo igual para todos. Las grandes organizaciones internacionales son igual de vulnerables. Por ejemplo, la ONU, que lleva tiempo familiarizándose con estas plataformas, ha tenido que lidiar recientemente con una pequeña situación embarazosa que sufrió a través de su cuenta de Twitter, una cuenta que utiliza para informar al mundo de sus actividades. Los investigadores, decididos a analizar a quién consideran perfiles de influencia, es decir, de referencia, descubrieron que junto a personajes relevantes de

18 Watch: President Obama Answers Your Questions in a Google+ Hangout, The White House, 14 de febrero de 2013. <http://www.whitehouse.gov/blog/2013/02/14/watch-president-obama-answers-your-questions-google-hangout>

19 El presidente de Egipto anuncia en Facebook que "no aceptará renunciar de forma humillante", La información, 3 de julio de 2013. [http://noticias.lainformacion.com/mundo/el-presidente-de-egipto-anuncia-en-facebook-que-no-aceptara-renunciar-de-forma-humillante\\_biz5yKmELT9Tj5aiVclFj6/](http://noticias.lainformacion.com/mundo/el-presidente-de-egipto-anuncia-en-facebook-que-no-aceptara-renunciar-de-forma-humillante_biz5yKmELT9Tj5aiVclFj6/)



para la propaganda, es el momento de abordar el lado más oscuro, falta de ética o incluso peligroso en un momento dado para un estado y sus ciudadanos. Comenzaré por cómo se traspasa la línea ética en las redes sociales desde el mundo de la empresa para derribar a la competencia. Algo que bien podría sucederle a cualquiera de las empresas españolas en un momento dado.

#### 4.1. La desinformación en el mundo de la empresa.

Como venimos comentando desde el principio del artículo, el Social Media se caracteriza por ser una plataforma virtual donde todo el mundo puede hablar de lo que le apetezca.

En este sentido, uno de los grandes avances ha sido la posibilidad de opinar sobre un determinado producto o servicio, con la intención de crear un halo de confianza y transparencia sobre él. La Red se ha plagado de barras de estrellas a través de las cuales puntuar, por ejemplo, ese libro que hemos leído, ese hotel que hemos visitado, ese producto que hemos probado, etc. Y en algunas ocasiones, además de las barras de estrellas, tenemos la opción, incluso, de comentar directamente lo que nos ha parecido. Llegados a este punto me gustaría lanzar una pregunta, ¿cuántos de nosotros miramos los comentarios sobre un hotel cuando estamos buscando en Internet dónde alojarnos en nuestras vacaciones?.

Las empresas lo saben. Saben que el nuevo consumidor (prosumer) ya no se fía de la información que da la compañía y toma la decisión de compra guiado por las opiniones de otras personas, incluso aunque no las conozca.

Si bien desde el ámbito empresarial se habla con frecuencia de buenas prácticas en las redes sociales, no conviene hacer oídos sordos a la realidad. Una realidad que demuestra que en numerosas ocasiones, y puesto que borrar un comentario genera más problemas que mantenerlo, se siembran cientos de comentarios falsos por toda la Red. Con dos intenciones:

- Reforzar la visibilidad de un producto o servicio con comentarios positivos.
- Destruir la reputación de la competencia con comentarios negativos.

Un ejemplo de la segunda intención, relativamente reciente, es el caso de Samsung, que deseoso de empujar las ventas de su gama de los Galaxy, contrató a varios estudiantes universitarios para que hablaran mal y en falso sobre los productos de su competencia directa HTC en las redes sociales. Samsung fue descubierto y tuvo que verse ante la vergüenza de tener que pedir disculpas públicamente<sup>22</sup>.

Lamentablemente este no es el único caso. Debido al peso reciente que tienen las redes sociales sobre las ventas o sobre el valor reputacional de una compañía, hay quien recurre a este tipo de prácticas sin demasiadas reflexiones. Y las empresas españolas pueden verse afectadas en un momento dado por un ataque de estas características.

#### 4.2. Las Redes Sociales para las organizaciones vinculadas a defensa y seguridad.

---

22 Samsung probed in Taiwan over 'fake web reviews', BBC News, 16 de abril de 2013. <http://www.bbc.co.uk/news/technology-22166606>

Aunque en este artículo se aborda sólo el enfoque de las redes sociales desde el punto de vista de la difusión, considero de interés mencionar, por lo menos, que como herramientas de comunicación puede servir a los analistas de inteligencia y a las organizaciones vinculadas a defensa y seguridad desde muchos puntos de vista. Para demostrarlo, conjuntamente con J. M. Blanco Navarro (Guardia Civil), elaboramos un cuadro basado en un análisis SWOT. Nuestra intención: mostrar a simple vista cómo las oportunidades son mucho mayores que las amenazas y que, por tanto, pueden ser tenidas en cuenta como herramientas muy interesantes y económicas para alcanzar distintos objetivos dentro del ámbito de la seguridad y la defensa.

	<b>INTERNO</b>	<b>EXTERNO</b>
<b>POSITIVO</b>	<b>FORTALEZAS</b> <ul style="list-style-type: none"> <li>- Coste</li> <li>- Inmediatez</li> <li>- Sencillez</li> <li>- Interactividad</li> <li>- Ubicuidad</li> <li>- Velocidad</li> <li>- Transparencia</li> <li>- Comunicación y diálogo</li> <li>- Diversidad</li> <li>- Movilidad</li> <li>- Difusión</li> <li>- Sin limitación horaria</li> <li>- Fácil de compartir con el equipo</li> </ul>	<b>OPORTUNIDADES</b> <i>Estratégicas:</i> <ul style="list-style-type: none"> <li>- Información</li> <li>- Comunicación</li> <li>- Participación</li> <li>- Cultura de seguridad</li> <li>- Gestión del conocimiento</li> <li>- Inteligencia colectiva</li> <li>- Gestión de marca/reputación</li> <li>- Formación</li> <li>- Compromiso con los ciudadanos</li> <li>- Open Government</li> <li>- Transparencia</li> <li>- Comunicación interna</li> <li>- Influencia</li> <li>- Vía de cambio y valor</li> </ul> <i>Operativas:</i> <ul style="list-style-type: none"> <li>- Gestión de crisis y emergencias</li> <li>- Inteligencia e inteligencia colectiva.</li> <li>- Monitorización de información</li> <li>- Investigación policial. Perfiles.</li> <li>- Predicción</li> </ul>
<b>NEGATIVO</b>	<b>DEBILIDADES</b> <i>Relativas a características de social media:</i> <ul style="list-style-type: none"> <li>- Barreras de entrada</li> <li>- Adaptación al medio y miedo al descontrol de las oportunidades</li> <li>- Cambio veloz</li> <li>- Descentralización</li> <li>- Volumen</li> <li>- Ruido</li> <li>- En algunos casos falta de madurez</li> </ul> <i>Relativa a su gestión:</i> <ul style="list-style-type: none"> <li>- Falta de formación</li> <li>- Infravaloración</li> <li>- Falta de tiempo</li> <li>- Falta de personal y recursos</li> <li>- Gestión del error</li> <li>- Incapacidad para la gestión e integración de todo el conocimiento</li> </ul> <i>Relativa a clásicos debates:</i> <ul style="list-style-type: none"> <li>- Debate público-privado</li> <li>- Debate libertad-seguridad</li> <li>- Debate transparencia-secreto</li> </ul>	<b>AMENAZAS</b> <i>Relativas a la información:</i> <ul style="list-style-type: none"> <li>- Infoxicación</li> <li>- Manipulación</li> <li>- Credibilidad y fiabilidad</li> <li>- Bots</li> <li>- Múltiples capas y puntos de vista</li> </ul> <i>Relativa a características de social media:</i> <ul style="list-style-type: none"> <li>- La parte negativa de las fortalezas</li> <li>- Imposibilidad de control</li> <li>- Sobrevaloración</li> <li>- División digital de los ciudadanos</li> <li>- Limitaciones de la comunicación</li> </ul> <i>Relativas a seguridad:</i> <ul style="list-style-type: none"> <li>- Viejos y nuevos delitos</li> <li>- Ingeniería social</li> <li>- Intimidad</li> <li>- Seguridad informática</li> <li>- Seguridad física</li> <li>- Uso terrorista y extremismo</li> <li>- Procesos maliciosos de influencia</li> </ul>

Fuente: Modelo Moya-Blanco sobre la utilidad de las redes sociales desde el punto de la seguridad y la defensa.

Hablemos, por tanto, ahora desde un punto de vista más centrado en los posibles riesgos a la seguridad y la defensa. Para hacerlo propongo varios ejemplos de casos reales que pueden resultar muy reveladores y llevarnos hacia una profunda reflexión sobre las consecuencias de la propaganda en las redes sociales.

### **Propaganda de extrema derecha**

La extrema derecha ha querido aprovechar desde el principio esta plataforma virtual de reciente creación para realizar sus propias campañas de propaganda. Siguiendo las palabras del profesor José San Martín, experto en la materia: “a diferencia de otras minorías ideológicas, la extrema derecha no se considera así, y busca todos los resquicios, prospecta todas las fisuras, para avanzar posiciones, desde soportes distintos, incluso contradictorios en las formas, pero coherentes en la apostasía al democratismo occidental”<sup>23</sup>. Por otro lado, el experto en fascismo Joan Antón Mellón nos recuerda que la esencia del fascismo se encuentra en la convicción de que la civilización avanza cuando existe un orden político “natural” por el cual los no selectos están al servicio (incluso esclavizados) de los selectos<sup>24</sup>.

A pesar de sus intentos, no les está resultando fácil ser uno más en las redes sociales, pues es la propia comunidad de Internet la que en muchos casos se moviliza para expulsarles del medio social. Este es el caso, por ejemplo, de un grupo de extrema derecha neonazi creado en Perú, al que Facebook bloqueó su cuenta. El grupo fue abierto por dos jóvenes neonazis conocidos por hacer disparos al aire libre en una plaza peruana en 2009. Fueron denunciados por una gran cantidad de usuarios de FB a raíz de la publicación de unas fotos donde se les veía saludando a un retrato de Adolf Hitler<sup>25</sup>.

Caso más sensible ha sido el bloqueo de la cuenta en Twitter de Besseres Hannover, grupo declarado neo-nazi y disuelto por la policía alemana debido a su vinculación al crimen organizado. Alemania solicitó que se diera de baja la cuenta, que hacía apología del nazismo. Twitter aceptó tras comprobar la peligrosidad de sus miembros<sup>26</sup>.

A pesar de todo, siguen existiendo grupos que utilizan libremente las redes para realizar sus propias campañas de propaganda, como por ejemplo la cuenta @NSRevolution\_ en Twitter que a día de hoy sigue sembrando la Red con mensajes como este: “Golden Dawn: No dejéis a los banqueros judíos asesinaros, matad a los banqueros judíos!”:

---

23 SAN MARTÍN, José. La coartada intelectual de la extrema derecha europea, Claves de Reazón Práctica, Madrid: Promotora General de Revistas, 2012, Volumen 223, p.13.

24 ANTÓN-MELLÓN, Joan. El Eterno Retorno. ¿Son fascistas las ideas-fuerza de la Nueva Derecha Europea (ND)?, Revista Foro Interno, Madrid: Universidad Complutense, 2011, p. 90. <http://revistas.ucm.es/index.php/FOIN/article/view/37009/35818>

25 Facebook bloquea a neonazis peruanos, Publimetro, 11 de agosto de 2011. <http://publimetro.pe/actualidad/147/noticia-no-esta-prohibido-nazismo>

26 Twitter blocks neo-Nazi account to users in Germany, BBC News, 18 de octubre de 2012. <http://www.bbc.co.uk/news/technology-19988662>





NSRevolution

@NSRevolution\_

Golden Dawn: "Don't Let the  
Jewish Bankers Murder You, Kill  
the Jew Bankers!"

[crushzion.konsl.org/golden-dawn-do...](http://crushzion.konsl.org/golden-dawn-do...)

11:58 AM - 25 May 2013

Fuente: @NSRevolution\_ Twitter

### Extrema izquierda

Las reflexiones realizadas sobre extrema derecha serían también extrapolables a movimientos de extrema izquierda, que manejan con elevado grado de conocimiento las redes sociales. En ocasiones, las redes han sido el campo de batalla virtual para ataques "verbales" entre grupos, que en algunas ocasiones se trasladan posteriormente al mundo físico, como los casos de Alpedrete en noviembre de 2014 o de Tetuán unas semanas antes. Datos oficiales de la policía y del Centro de Estudios e Iniciativas sobre Discriminación y Violencia muestran un repunte de actividad, tanto en actividades ligadas al fútbol, como fuera de él. Destacan en esos informes la edad, cada vez más temprana, de los arrestados. La edad es un factor fundamental para la actividad intensa en la red. Proliferan cuentas en redes, blogs, foros. La red se convierte en un medio fundamental para la información, la comunicación y la preparación de acciones.

### Ciberactivismo y Ciberhacktivismo

Especialmente interesante en los últimos años es el avance del ciberactivismo en Internet. Puesto que las redes sociales facilitan la difusión de cualquier opinión o deseo, se han convertido en unas plataformas magníficas para la crítica social o para incitar a cualquier tipo de ciberactivismo o ciberhackeo de cuentas o páginas en Internet objetivo. La propia ONG Amnistía Internacional tiene una guía fácil para las personas que quieran convertirse en ciberactivistas<sup>27</sup>.

Sin duda, el grupo más activo de ciberactivismo, basado en ciberhacking, es Anonymous, quien en numerosas ocasiones parece traspasar la línea del cibercrimen.

En abril de 2013, el grupo de hackers Anonymous decidió lanzar una campaña muy agresiva contra el estado de Israel con la intención de bloquear y eliminar la presencia de Israel en Internet. La campaña perseguía solidarizarse con la causa Palestina y buscar el apoyo de otros grupos de hackers activistas en el mundo para conseguir su objetivo. Para explicar los motivos concretos que les han llevado a crear esta operación deciden dar un comunicado de prensa a través de un vídeo subido a Youtube dirigido al estado de Israel<sup>28</sup>.

27 AMNISTÍA INTERNACIONAL. Herramientas y sugerencias para un ciberactivismo eficaz. <http://www.amnesty.org/es/stay-informed/publications/books/herramientas-ciberactivismo-eficaz>

28 ANONYMOUS. #OPIsrael (V. 2.0). <http://anonnews.org/press/item/2238/>

Comenzaron con la difusión de la campaña y los hackeos de páginas en Internet el 5 de abril y finalizaron el 7, con la intención de hacerlo coincidir con el día de la Memoria del Holocausto.

Durante los tres días se pudieron ver mensajes como este, en el que se bromeaba con la desaparición de Israel del ciberespacio. Mensajes que se convirtieron en altamente virales y dieron la vuelta al mundo.



Ahora podemos preguntarnos, ¿qué pasaría si España se convirtiera en un objetivo de este tipo de campañas en las redes sociales?

### La desinformación en catástrofes naturales

Desde un punto de vista empírico, y a raíz de uno de los terremotos más virulentos de Chile (27/02/2010), el centro de recursos de Yahoo! decidió investigar en profundidad el comportamiento de la difusión de los mensajes informativos suministrados por los propios usuarios de la red social que disponían de información de primera mano sobre el terremoto. En su estudio dedicaron una parte especial a la difusión de falsos rumores que contaminaban la realidad de lo que estaba sucediendo. Tras su análisis, descubrieron algunas cuestiones muy interesantes. Veamos la tabla.

Table 4: Classification results for cases studied of confirmed truths and false rumors.

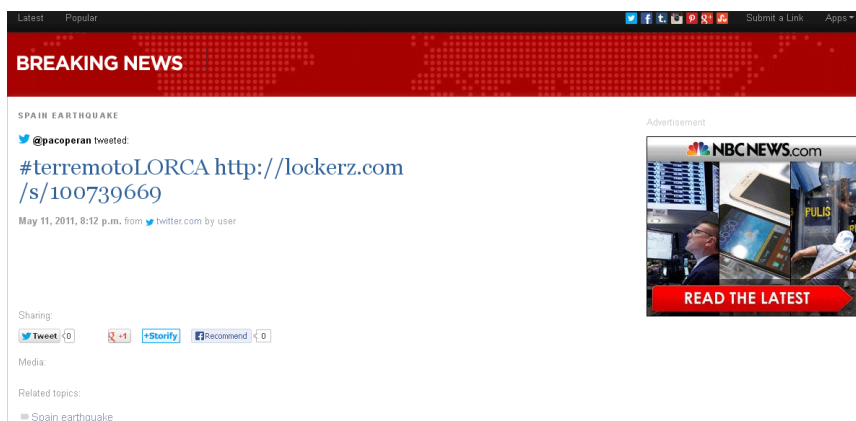
Case	# of unique tweets	% of re-tweets	# of unique "affirms"	# of unique "denies"	# of unique "questions"
<b>Confirmed truths</b>					
The international airport of Santiago is closed	301	81	291	0	7
The <i>Viña del Mar International Song Festival</i> is canceled	261	57	256	0	3
Fire in the Chemistry Faculty 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
<b>False rumors</b>					
Death of artist Ricardo Arjona	50	37	24	12	8
Tsunami warning in Valparaiso	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

Fuente: *Twitter Under Crisis: Can we trust what we RT?*<sup>29</sup>

29 MENDOZA, Marcelo; POBLETE, Bárbara y CASTILLO Carlos. *Twitter Under Crisis: Can we trust what we RT?*, 1st Workshop on Social Media Analytics, Washington: Yahoo! Research, 2010, p. 7. [http://research.yahoo.com/files/mendoza\\_poblete\\_castillo\\_2010\\_twitter\\_terremoto.pdf](http://research.yahoo.com/files/mendoza_poblete_castillo_2010_twitter_terremoto.pdf)

Si observamos con detenimiento comprobaremos que el número de mensajes falsos en general es bastante más elevado que el número de mensajes confirmados. Las causas pueden ser múltiples, pero probablemente una de las razones sea porque son mensajes más sorprendentes y emotivos, por tanto más susceptibles de ser compartidos. Sin embargo, cuando analizamos el número de mensajes que afirmaban el contenido, vemos que es mucho mayor el relacionado con aquellos que aseveraban que el mensaje era cierto (1.123), frente a los que atestiguaban que los rumores falsos eran correctos (502). Por último, además, resultó que había más mensajes que negaban la veracidad de una noticia falsa (836) frente aquellos que desmentían una noticia verdadera (4). Por tanto, una vez más, el medio social demuestra lo que es. Cualquiera puede decir cualquier cosa, sin embargo, un buen análisis de redes sociales demuestra que son los propios usuarios quienes también actúan como periodistas validando o desmintiendo la noticia.

¿Cómo pueden aprovechar nuestros cuerpos y fuerzas de seguridad del estado la información vertida en Twitter de primera mano, muy útil en distintas situaciones, sin contaminarse con falsos rumores? Por ejemplo, en casos de emergencia como el sucedido en el terremoto de Lorca, donde el hashtag #terremotoLORCA se convirtió en un repositorio con todo tipo de información<sup>30</sup> útil sobre números de teléfono de ayuda, fotografías de cómo estaba la situación, etc. Entre esos mensajes también pudimos descubrir otros falsos como éste, que cuando pulsabas en la dirección web te redirigía a un portal comercial que aprovechaba la popularidad del hashtag para vender sus productos. Como gancho hacía pensar que incluía contenido importante, especialmente tras aparecer en un conocido portal de noticias en Internet llamado Breaking News, dentro de la categoría “Spain Earthquake”.



Fuente: Captura de Breaking News<sup>31</sup>

Un caso significativo, y lamentable, fue la utilización del caso de ébola en España para difundir falsos rumores sobre la existencia de más casos en diferentes hospitales de la geografía nacional. Muchos de estos rumores iban acompañados por falsificaciones de portadas de medios de prensa. La cuenta en twitter de Guardia Civil estuvo horas desmintiendo esas situaciones.

30 GONZALO, Paula. #TerremotoLorca despierta la solidaridad en Twitter, Periodismo Ciudadano, 13 de mayo de 2013. <http://www.periodismociudadano.com/2011/05/13/terremotolorca-despierta-la-solidaridad-en-twitter/>

31 @pacoperan. #terremotoLORCA, Breaking News, 11 de mayo de 2013. <http://www.breakingnews.com/item/ahZzfmJyZWFraW5nbmV3cy13d3ctaHJkcg0LEgRTZWVkgMX9qwMM/2011/05/11/terremotolorca-httplockerzcoms100739669>



Fuente: Cuenta en twitter de Guardia Civil @guardiacivil<sup>32</sup>

## 5. ¿CONTROLAR LO INCONTROLABLE?

Evidentemente todos los estados del mundo se plantean algún tipo de control sobre las redes sociales con la intención de vigilar que éstas no se conviertan en un problema de seguridad nacional, especialmente después del efecto amplificador que tuvo en el llamado “despertar árabe”.

Para ello cada cual está desarrollando su propia estrategia de seguridad. A continuación me gustaría mencionar algunas de ellas por lo dispares que son, buscando abrir un espacio a la reflexión y el debate de qué fórmula sería la más adecuada para España.

- *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 noticia<sup>33</sup>.

32 Más información: <http://www.clasesdeperiodismo.com/2014/10/14/guardia-civil-de-espana-alerta-de-falsas-portadas-sobre-ebola/>

33 REYNOLDS, Paul. Censura en el aniversario de Tiananmen, BBC Mundo, 2 de junio de 2013. [http://www.bbc.co.uk/mundo/internacional/2009/06/090602\\_1552\\_tiananmen\\_internet\\_jg.shtml](http://www.bbc.co.uk/mundo/internacional/2009/06/090602_1552_tiananmen_internet_jg.shtml)

- *Táctica del “Miedo”*. Turquía sigue reflexionando a día de hoy qué hacer con las redes sociales. Si bien ha decidido que no las prohibirá, sí las vigila muy de cerca para conocer en profundidad todo lo que dicen sus conciudadanos con la intención de procesarles o multarles en función de lo que expresen<sup>34</sup>. Para tenerlos más controlados, además, ha decidido que prohibirá la apertura de cuentas falsas o enmascaradas por motivos de seguridad. Por tanto, todos los ciudadanos turcos que quieran usar las redes sociales deberán identificarse<sup>35</sup>.
- *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 compañías de Internet, como Facebook y Google, para que les permitan acceder a contenido privado de usuarios que consideran “de riesgo”<sup>36</sup>. Sin embargo, como era de esperar, no sólo EE.UU. utiliza este tipo de vigilancia digital. Según Le Monde Francia también tiene un programa de estas características<sup>37</sup>.
- *Táctica de “La siembra”*. Ésta es más bien una táctica dirigida a modificar la percepción y reputación 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. ha destinado \$630,000 en Internet para comprar “fans”<sup>38</sup>.

## 6. CONCLUSIÓN

Las redes sociales virtuales cada vez están más presentes en nuestras vidas. Más allá de los usuarios individuales que han sido quienes las han convertido en un éxito de la comunicación online, se vienen creando desde hace años perfiles que representan a distintas organizaciones internacionales públicas y privadas. Una buena gestión de estos perfiles y de la comunicación, que se realiza a través de ellos, evita la exposición a ciertos riesgos y amenazas de nueva creación, que están apareciendo conforme las redes sociales evolucionan con los nuevos actores y los nuevos intereses.

34 EFE. Un pianista turco condenado a 10 meses de cárcel por criticar el islam en Twitter, El País Internacional, 15 de abril de 2013. [http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587\\_412492.html](http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587_412492.html)

35 Fake social media accounts to be prevented: Turkish deputy PM, Turkish weekly, 21 de junio de 2013. <http://www.turkishweekly.net/news/152201/fake-social-media-accounts-to-be-prevented-turkish-deputy-pm.html>

36 GREENWALD, Glenn y MACASKILL, Ewen. NSA Prism program taps in to user data of Apple, Google and others, The Guardian, 7 de junio de 2013. <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>

37 FOLLOROU, Jaques y JOHANNÈS, Frank. Révélations sur le Big Brother français, Le Monde, 4 de julio de 2013. [http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais\\_3441973\\_3224.html](http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html)

38 US State Department Facebook ‘Likes’: DOS Spent \$630,000 On Buying Fans, International Business Times, 4 de Julio de 2013. <http://www.ibtimes.com/us-state-department-facebook-likes-dos-spent-630000-buying-fans-1334457#>

## BIBLIOGRAFÍA

Amnistía Internacional. (2009). Herramientas y sugerencias para un ciberactivismo eficaz. Disponible en: <http://www.amnesty.org/es/stay-informed/publications/books/herramientas-ciberactivismo-eficaz>

Anonymous. (V. 2.0).

Antón-Mellón, J. (2011). El Eterno Retorno. ¿Son fascistas las ideas-fuerza de la Nueva Derecha Europea (ND)? . Revista Foro Interno, 11, 69-92. Madrid: Universidad Complutense. Disponible en: <http://revistas.ucm.es/index.php/FOIN/article/view/37009/35818>

Birkenbihl, K., Quesada, E., y Priesca, P. (2009). Presente y futuro de la world wide web. Novática: Revista de la Asociación de Técnicos de Informática, 197, 5-7. Madrid. Disponible en: <http://www.ati.es/novatica/2009/197/Nv197-Presentacion.pdf>

Calderón, V. La propaganda militar en 140 caracteres. El País. 20/11/2012. Disponible en: [http://internacional.elpais.com/internacional/2012/11/20/actualidad/1353433014\\_417902.html](http://internacional.elpais.com/internacional/2012/11/20/actualidad/1353433014_417902.html)

Calderón, V. Propaganda a golpe de Tuit. El País. 03/02/2013. Disponible en: [http://sociedad.elpais.com/sociedad/2013/02/03/vidayartes/1359919995\\_815589.html](http://sociedad.elpais.com/sociedad/2013/02/03/vidayartes/1359919995_815589.html)

Castillo, M. Facebook bloquea a neonazis peruanos. Publimetro. 11/08/2011. Disponible en: <http://publimetro.pe/actualidad/147/noticia-no-esta-prohibido-nazismo>

Chozick, A., y Perlroth, N. Twitter Speaks, Markets Listen and Fears Rise. The New York Times. 28/04/2013. Disponible en: [www.nytimes.com/2013/04/29/business/media/social-medias-effects-on-markets-concern-regulators.html](http://www.nytimes.com/2013/04/29/business/media/social-medias-effects-on-markets-concern-regulators.html)

EFE. Un pianista turco condenado a 10 meses de cárcel por criticar el islam en Twitter. El País. 15/04/2013. Disponible en: [http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587\\_412492.html](http://internacional.elpais.com/internacional/2013/04/15/actualidad/1366037587_412492.html)

El presidente de Egipto anuncia en Facebook que “no aceptará renunciar de forma humillante”, La Información. 03/07/2013. Disponible en: [http://noticias.lainformacion.com/mundo/el-presidente-de-egipto-anuncia-en-facebook-que-no-acceptara-renunciar-de-forma-humillante\\_blz5yKmELt9Tj5aiVclFj6/](http://noticias.lainformacion.com/mundo/el-presidente-de-egipto-anuncia-en-facebook-que-no-acceptara-renunciar-de-forma-humillante_blz5yKmELt9Tj5aiVclFj6/)

Fake social media accounts to be prevented: Turkish deputy PM. Journal of Turkish Weekly. 21/06/2013. Disponible en: <http://www.turkishweekly.net/news/152201/fake-social-media-accounts-to-be-prevented-turkish-deputy-pm.html>

Follorou, J., y Johannès, F. Révélations sur le Big Brother français, Le Monde, 04/07/2013. Disponible en: [http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais\\_3441973\\_3224.html](http://www.lemonde.fr/societe/article/2013/07/04/revelations-sur-le-big-brother-francais_3441973_3224.html)

Fontana, J. (2013). El futuro es un país extraño. Una reflexión sobre la crisis social de comienzos del siglo XXI. Barcelona: Pasado y Presente.

Fort, M. ‘Minicrash’ en Wall Street por un falso tuit sobre un atentado contra Obama. La Vanguardia. 23/04/2013. Disponible en: <http://www.lavanguardia.com/economia/20130423/54372747540/minicrash-wall-street-hackeada-cuenta-twitter-associated-press.html>

Fundación Telefónica. (2013). La sociedad de la Información en España 2012. Madrid: Ariel. Disponible en: [http://www.fundaciontelefonica.com/arte\\_cultura/sociedad-de-la-informacion/informe-sociedad-de-la-informacion-en-espana-2012/](http://www.fundaciontelefonica.com/arte_cultura/sociedad-de-la-informacion/informe-sociedad-de-la-informacion-en-espana-2012/)

Global Web Index. Global Map of Social Networking 2011. Disponible en: <https://globalwebindex.net/wp-content/uploads/down>

[loads/2011/06/Global-Map-of-Social-Networking-GlobalWebIndex-June-20112.pdf](https://globalwebindex.net/wp-content/uploads/down)

Gonzalo, P. #TerremotoLorca despierta la solidaridad en Twitter. Periodismo Ciudadano. 13/05/2011. Disponible en: <http://www.periodismociudadano.com/2011/05/13/terremotorca-despierta-la-solidaridad-en-twitter/>

Greenwald, G., y MacAskill, E. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. 07/06/2013. Disponible en: <http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data>

Greenwood, P. Israel invests millions in drive for elite 'cyber warriors'. The Telegraph. 01/11/2012. Disponible en: <http://www.telegraph.co.uk/news/worldnews/middleeast/israel/9648820/Israel-invests-millions-in-drive-for-elite-cyber-warriors.html>

Lee, Y. NKorea's Twitter account hacked amid tension. Associated Press. 04/04/2013. Disponible en: <http://bigstory.ap.org/article/nkoreas-twitter-account-hacked-amid-tension>

Lumezanu, C., Feamster, N., y Klein, H. (2012). #bias: Measuring the Tweeting Behavior of Propagandists. Sixth International AAAI Conference on Weblogs and Social Media. Disponible en: <http://www.aaai.org/ocs/index.php/ICWSM/ICWSM12/paper/view/4588/4985>

Mendoza, M., Poblete, B., y Castillo, C. (2010). Twitter Under Crisis: Can we trust what we RT?. 1st Workshop on Social Media Analytics (SOMA '10). Washington, DC, USA. Disponible en: [http://research.yahoo.com/files/mendoza\\_poblete\\_castillo\\_2010\\_twitter\\_terremoto.pdf](http://research.yahoo.com/files/mendoza_poblete_castillo_2010_twitter_terremoto.pdf)

Moya, E., y Blanco, J. M. (2015). "Redes sociales y seguridad ciudadana". En I. Criado y F. Rojas (Eds.), Casos de éxito en redes sociales digitales de las administraciones públicas. Escola d'Administració Pública de Catalunya.

Musser, J., y O'Really, T. (2007). Web 2.0 Principles and Best Practices. O'Reilly Radar. Disponible en: <http://repo.mynooobliflife.org/.priv8/Ebook/Web%202.0%20Principles%20and%20Best%20Practices.pdf>

North Korea using Twitter for propaganda. The Sidney Morning Herald. 15/08/2010. Disponible en: <http://www.smh.com.au/technology/technology-news/north-korea-using-twitter-for-propaganda-20100815-1250u.html>

Obama tells intelligence chiefs to draw up cyber target list – full document text. The Guardian. 07/06/2013. Disponible en: <http://www.guardian.co.uk/world/interactive/2013/jun/07/obama-cyber-directive-full-text>

O'Really, T. What Is Web 2.0: Design Patterns and Business Models for the Next Generation of Software. O'Really. 30/09/2005. Disponible en: <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1#mememap>

Oriella PR Network. Global Digital Journalism Study 2013. Disponible en: <http://www.oriellaprnetwork.com/research>

Ortíz, A. La ONU sigue a una actriz porno en su cuenta oficial de Twitter. ABC. 07/05/2013. Disponible en: <http://www.abc.es/tecnologia/redes/20130507/abci-pornstar-twitter-201305071614.html>

Piratean de nuevo la cuenta de Nicolás Maduro en Twitter. CNN. 12/05/2013. Disponible en: <http://cnnespanol.cnn.com/2013/05/12/piratean-de-nuevo-la-cuenta-de-nicolas-maduro-en-twitter/>

Reynolds, P. Censura en el aniversario de Tiananmen. BBC. 02/06/2013. Disponible en: [http://www.bbc.co.uk/mundo/internacional/2009/06/090602\\_1552\\_tiananmen\\_internet\\_jg.shtml](http://www.bbc.co.uk/mundo/internacional/2009/06/090602_1552_tiananmen_internet_jg.shtml)

Samsung probed in Taiwan over 'fake web reviews'. BBC. 16/04/2013. Disponible en: <http://www.bbc.co.uk/news/technology-22166606>

Sanmartín, J. J. (2012). La coartada intelectual de la extrema derecha europea. Claves de Razón Práctica, 223. Madrid.

Schulman, K. Watch: President Obama Answers Your Questions in a Google+ Hangout. The White House. 14/02/2013. Disponible en: <http://www.whitehouse.gov/blog/2013/02/14/watch-president-obama-answers-your-questions-google-hangout>

Spain Earthquake. Breaking News. 11/05/2011. Disponible en: <http://www.breaking-news.com/item/ahZzfmJyZWFraW5nbmV3cy13d3ctaHJkcg0LEgRTZWVvGMX-9qwMM/2011/05/11/terremotorca-httplockerzcoms100739669>

The Cocktail Analysis. (2013). 5º Oleada Observatorio Redes Sociales. Disponible en: <http://es.slideshare.net/TCAnalysis/5-oleada-observatorio-redes-sociales>

Twitter blocks neo-Nazi account to users in Germany. BBC. 18/10/2012. Disponible en: <http://www.bbc.co.uk/news/technology-19988662>

United States Department of State and the Broadcasting Board of Governors. (2013). Inspection of the Bureau of International Information Programs. Office of Inspector General. Disponible en: <http://oig.state.gov/system/files/211193.pdf>

Waltz, E. (1998). Information Warfare: Principles and Operations. Artech House.

Weimann, G. (2006). Terror on the Internet: The New Arena, the New Challenges. Washington, DC: United States Institute of Peace Press.

Fecha de recepción: 14/11/2014. Fecha de aceptación: 17/12/2014