EMPIRIA. Revista de Metodología de las Ciencias Sociales
ISSN: 1139-5737
ISSN: 2174-0682
empiria@poli.uned.es
Universidad Nacional de Educación a Distancia
España

Quian, Alberto
Observación participante en una organización de filtraciones periodísticas: el caso WikiLeaks
EMPIRIA. Revista de Metodología de las Ciencias Sociales,
núm. 52, 2021, Septiembre-Diciembre, pp. 199-231
Universidad Nacional de Educación a Distancia
Madrid, España

DOI: https://doi.org/10.5944/empiria.52.2021.31370

Observación participante en una organización de filtraciones periodísticas: el caso WikiLeaks

Participant observation in a news leak organisation: the WikiLeaks case

Alberto Quian
Universidad Carlos III
https://orcid.org/0000-0002-8593-7999
lpampin@hum.uc3m.es (ESPAÑA)

Recibido: 19.02. 2020
Aceptado:30.07.2021

RESUMEN

Para explicar los procesos de una comunidad virtual de filtraciones de documentos secretos utilizamos el método de observación participante, introduciéndonos en la red de colaboradores de WikiLeaks. De este modo, intentamos describir los procesos de creación de noticias en estos entornos emergentes mediante la observación del espacio virtual en el que se trabaja, los instrumentos y procedimientos con los que se opera y los flujos de comunicación e información que se generan en este. El objetivo es contribuir a ampliar el conocimiento sobre los roles emergentes de investigador en la observación en línea y, particularmente, describir el funcionamiento de comunidades virtuales confidenciales, además de aportar nuevas claves metodológicas para los estudios con un enfoque en el *newsmaking*

PALABRAS CLAVE

Comunidades virtuales, filtraciones, newsmaking, observación participante, WikiLeak.

ABSTRACT

To explain the processes of a virtual community working with secret leaked documents, we use the participant observation method entering into the WikiLeaks' collaborators network. In this way, we attempt to describe the processes

of newsmaking in these emerging environments by observing the virtual space in which it works, the tools and procedures that normally are used, and the communication and information flows generated in it. The aim of this paper is to contribute to broaden knowledge about the emerging roles of researcher using online observation —and particularly in confidential virtual communities—, and to provide new methodological keys for studies focused on newsmaking.

KEY WORDS

Virtual community, leaks, newsmaking, participant observation, WikiLeaks

1. INTRODUCCIÓN

De acuerdo con las propuestas de Becker y Geer (1958), el objetivo principal de la observación participante debe ser la descripción de distintos hechos, situaciones y acciones que suceden en un escenario social concreto. Centrándonos en el proceso informativo, para Wolf ([1987], 1996) se trata del método más adecuado para estudiar la sociología de los emisores. Pero este modelo necesita actualizarse ante la emergencia de escenarios virtuales en red donde el observador y los observados no comparten un espacio social físico (Abdelnour, 1998), sino que conforman una red de nodos interconectados electrónicamente, distanciados geográficamente, pero unidos ciberespacialmente en un entorno virtual. Este escenario digital donde desarrollan su actividad cambia los procesos de inmersión, también de aceptación –cuando procede– en las comunidades virtuales y de relación e interacción entre los distintos actores que gestionan y habitan estos espacios virtuales.

"Comunidades virtuales" es un concepto que fue acuñado por Howard Rheingold en 1993 para definir las "agregaciones sociales que emergen de la red cuando un número suficiente de personas entablan discusiones públicas durante un tiempo lo suficientemente largo, con suficiente sentimiento humano, para formar redes de relaciones personales en el ciberespacio" (Rheingold, 1993: 5).

John Perry Barlow –letrista del grupo musical Grateful Dead e hijo de la contracultura estadounidense de la década de 1960, reconvertido en periodista informático y ciberlibertario en la década de 1980– se convirtió en un pionero del movimiento por los derechos en el ciberespacio y en el primer comentarista público en aplicar el término "ciberespacio" –creado por William Gibson en su novela *Neuromancer,* de la que bebieron los *cypherpunks* (criptopunnks) en la década de 1990, en su confrontación contra el Estado de secreto y en su defensa del derecho a la privacidad en la Red– para expresar el espacio virtual y fronterizo que surge del nexo entre dispositivos computacionales y redes de comunicación electrónicas, el cual exige un nuevo conjunto de metáforas, un nuevo conjunto de reglas y comportamientos (Sterling, 1992; Himanen, 2001).

En ese espacio *cíber* se configura una nueva realidad, la transrealidad, transgrediendo los límites físicos y cognitivos espacio-temporales –las dimensiones fundamentales de la vida humana–, para conectarnos *a través de* y *al otro lado*. En esta nueva era de la transrealidad, nuestra percepción del espacio y del tiempo se ha visto alterada (Castells, 1997: 408) y lo virtual y lo real se enredan en el hiperespacio, el punto de fricción entre el espacio físico y el *cíber* (Gómez Cruz, 2002; Quian, 2013b: 52).

La interacción en entornos virtuales colaborativos se ha estudiado desde los primeros años de la expansión de la World Wide Web, en la década de 1990 (Benford *et al.*, 1995; 2001). El desarrollo de esta nueva dimensión de la realidad, en la que convergen el espacio físico y el espacio *cíber*, y en la que se reconfiguran el uno al otro, abre nuevas puertas de entrada y plantea nuevos retos a la observación participante de los investigadores sociales que exploran el ciberespacio y sus comunidades y, en particular, de los que nos dedicamos a escrutar los procesos de producción de noticias.

La observación en línea de comunidades en la Red nos permite, en otras cosas, "estudiar las relaciones de poder, la coordinación del trabajo, la cooperación, el desarrollo de productos, los conflictos, la cultura del trabajo y muchos otros aspectos de los procesos profesionales relacionados con el trabajo en las comunidades virtuales" (Nørskov y Rask, 2011).

En el caso de las organizaciones virtuales, nos permite conocer la manera en que interactúan activamente para compartir conocimientos (Koh y Kim, 2004; Wellman y Gulia, 1999). Preece (2000) enumera una serie de características de la comunidad virtual: personas, un propósito compartido, políticas y sistemas informáticos. Mientras que Koh y Kim hablan de miembros (personas), interacción, ciberespacio y objetivos compartidos. La tecnología también es, por tanto, un actor que debe ser observado.

En los estudios de *newsmaking*, en el contexto de la sociedad red, la robotización o automatización periodística ha sido "una constante desde que se inició la informatización de las redacciones", lo cual "abrió el camino para la redefinición de los perfiles profesionales que participan en la producción de noticias" (Túñez-López, Toural-Bran, Frazão-Nogueira, 2020: 19).

Con el proceso de digitalización e inmersión en el ciberespacio "también han cambiado las herramientas fundamentales, los espacios físicos y las relaciones que sustentan la creación de noticias" (Moran, 2020: 2). Detalladamente, Heinrich (2011) argumenta que la digitalización ha cambiado esencialmente los métodos de recopilación de información, la producción de las noticias, la forma de compartir información entre periodistas y la manera de entregársela al público.

De manera que cada vez se hace más necesario un enfoque en el *newsmaking* que fije la atención en el sistema sociotécnico (Chadwick, 2013) y, particularmente, en las relaciones entre actores humanos (periodistas) y no humanos (tecnología) que se producen en este (De Maeyer y Delva, 2020; Saado y Hussein, 2020), pero también en las nuevas prácticas participativas en el proceso de producción de noticias, que ofrecen a nuevos actores emergentes la oportunidad de colaborar o competir con las elites mediáticas tradicionales en un nuevo sistema

de medios híbridos (Chadwick, 2013; Iannelli y Splendore, 2017). En ese marco se acomoda WikiLeaks, organización que se amolda al ciberespacio, a un nuevo territorio desterritorializado donde se protege y donde se configura como organización transnacional, apátrida, ubicua y post-estatal que se sustrae a los controles geográficos (Assange *et al*., 2012: 127-128).

El objetivo principal de este trabajo es describir y clarificar los métodos y herramientas con los que trabaja la red de WikiLeaks para producir noticias a partir de filtraciones masivas. Se pretende también contribuir a ampliar la discusión sobre los roles de investigador/observador en la observación en línea y, particularmente, en comunidades virtuales restringidas, en nuestro caso, en una red de filtraciones periodísticas, además de aportar nuevas claves para los estudios con un enfoque en el *newsmaking*.

Particularmente, se describen todas las fases del proceso mediante el cual el investigador, en un doble rol de observador/periodista, se introduce en la red de la comunidad virtual de filtraciones de WikiLeaks y accede a una inmensa base de datos confidencial para explorarla, encontrar aquello que se ocultaba a la sociedad y es de interés público y, finalmente, sacarlo a la luz pública.

Con este trabajo pretendemos clarificar el proceso de producción de noticias en una comunidad virtual de filtraciones que se enmarca en uno de los fenómenos centrales en Internet: las ciberguerras de la información –anticipadas por Arquilla y Ronfeldt (1993, 1999, 2001)– entre el poder institucional y el contrapoder de las redes hacktivistas (Wray 1998, 1999), cuyo máximo exponente es la organización WikiLeaks (Quian, 2013a).

2. CASO STRATFOR

La historia de WikiLeaks se divide en tres etapas estratégicas claves, delimitadas por el distinto impacto alcanzado por sus filtraciones (Chadwick, 2013; Quian y Elías, 2018). La primera etapa se desarrolló desde finales de 2006 –cuando se fundó WikiLeaks–, hasta el 5 de abril de 2010, cuando se publicó el vídeo *Collateral Murder*, grabado el 12 de julio de 2007 desde un helicóptero Apache estadounidense en Irak, en el que se ve cómo soldados norteamericanos acribillan al reportero de la agencia de noticias Reuters Namir Noor-Eldeen, a su ayudante y a diez civiles más. La publicación de aquel vídeo supuso el primer gran impacto global de WikiLeaks, utilizando los medios convencionales, y fue el inicio de una serie de filtraciones pactadas con la *quality press*. Durante este primer periodo, de plena autonomía editorial, WikiLeaks publicó en su sitio web numerosos documentos secretos de gran valor; sin embargo, su impacto mediático fue muy discreto (Quian, 2013a), ya que WikiLeaks operaba de manera totalmente autónoma, publicando documentos secretos en bruto, sin editar, buscando eco mediático desde su espacio propio en Internet. La ética hacker de Julian Assange le hacía colocarse por entonces en una posición radicalmente opuesta a la de la prensa convencional: la información debía ser liberada en bruto, sin suprimir datos, sin editar el contenido de los documentos, porque para él eso era lo

correcto, la absoluta transparencia. La información –toda– debía estar al alcance de todo el mundo a la vez y sin filtros.

Con el vídeo *Collateral Murder* se inició la segunda etapa. Para alcanzar el máximo impacto en la esfera pública, Assange decidió entablar colaboraciones con algunos de los más influyentes medios de información de Occidente (Chadwick, 2013; Quian, 2013a). Este cambio de estrategia coincidió con un hecho fundamental: WikiLeaks estaba recibiendo a principios de 2010 el mayor alijo de documentos secretos jamás filtrados, cientos de miles enviados a la organización por la soldado Chelsea Manning (por entonces, Bradley Manning, antes de su cambio de género) sobre las guerras de Irak y Afganistán, y sobre la diplomacia estadounidense. Así, se juntaron dos necesidades: una, la de aprovecharse de algunos de los medios más influyentes del mundo occidental para lograr el máximo impacto mediático y político, y en segundo lugar, la de contar con un equipo de colaboradores amplio y profesional que pudiese gestionar y editar una cantidad ingente de material en bruto, para pasarlo por el filtro periodístico y hacerlo digerible para el gran público. Así fue como WikiLeaks alcanzó su cenit, en términos de impacto mediático y político, como han demostrado nuestras investigaciones (Quian, 2013a; Quian y Elías, 2018); primero, con el vídeo *Collateral Murder*, que marca el primer punto de inflexión en la historia de WikiLeaks, al darse a conocer mundialmente, y luego, con las filtraciones masivas que se sucedieron durante aquel año: los *Papeles de la Guerra de Afganistán*, en julio de 2010, los *Diarios de la Guerra de Irak*, en octubre, y finalmente, el *Cablegate*, a finales de noviembre, con el que alcanzó su máximo impacto, como confirmamos en nuestras investigaciones.

En 2011 se inició la tercera etapa, tras la ruptura de relaciones con los medios con los que había colaborado hasta entonces. Después de un agrio debate público con sus excolaboradores, en el que subyacía la tensión entre el modelo periodístico tradicional y los valores de la ética hacker (Quian, 2013a), WikiLeaks emprendió un nuevo camino con una mayor variedad de socios. La nueva estrategia se consolidó en el año 2012, con colaboraciones más abiertas, dando acceso a sus archivos a periodistas independientes, científicos y activistas.

El 27 de febrero de 2012, WikiLeaks comenzó una colaboración con medios de comunicación de todo el mundo para la publicación de cinco millones y medio de correos electrónicos de la empresa de inteligencia global Strategic Forecasting, Inc., más conocida como Stratfor, con sede central en el estado de Texas. La filtración masiva fue atribuida a una incursión de miembros de Anonymous en el sitio web de Stratfor (Ball, 2012). En concreto, sus autores fueron hackers de AntiSec –contracción de Anti-Security–, facción surgida en verano de 2011, en plena fragmentación de Anonymous en un archipiélago de islas hackers (Coleman, 2014: 283). Aquella fue la acción más memorable de AntiSec.

Bautizados como *The Global Intelligence Files*[1], estos documentos, fechados entre julio de 2004 y finales de diciembre de 2011, revelan el funcionamiento y técnicas utilizadas por Stratfor, y las relaciones de esta compañía privada de

[1] Disponible en http://wikileaks.org/the-gifiles.html (consulta: 14 de agosto de 2019).

espionaje con sus clientes, entre los que se encuentran la CIA, ministerios de Defensa y Exteriores, embajadas y compañías multinacionales.

Deterioradas las relaciones con los cinco grandes medios colaboradores en el *Cablegate –The Guardian, The New York Times, Le Monde, El País* y *Der Spiegel–*, WikiLeaks recurrió para esta filtración masiva –la mayor, por su volumen– a veintinueve medios de todo el mundo, más repartidos geográficamente, culturalmente más heterogéneos y de naturaleza diversa, pero, en general, menos populares e influyentes a nivel mundial que los socios que tuvo en 2010:

- *ABC Color* – Paraguay.
- *Al Akhbar* – Líbano.
- *Al Masry Al Youm* – Egipto.
- *Asia Sentinel* - Hong Kong.
- *Bivol* – Bulgaria.
- *Carta Capital* – Brasil.
- *CIPER* – Chile.
- *Dawn Media* – Pakistán.
- *L'Espresso* – Italia.
- *La Repubblica* – Italia.
- *La Jornada* – México.
- *La Nación* – Costa Rica.
- *Malaysia Today* – Malasia.
- *McClatchy* – Estados Unidos.
- *Nawaat* – Túnez.
- *NDR/ARD* – Alemania.
- *Owni* – Francia.
- *Pagina 12* – Argentina.
- *Plaza Pública* – Guatemala.
- *Pública* – Brasil.
- *Público* – España.
- *Rolling Stone* – Estados Unidos.
- *Russia Reporter* – Rusia.
- *Sunday Star-Times* – Nueva Zelanda.
- *Ta Nea* – Grecia.
- *Taraf* – Turquía.
- *The Hindu* – India.
- The Yes Men[2] – Global.

[2] The Yes Men es un dúo de activistas formado por Andy Bichlbaum y Mike Bonanno que practica lo que llaman "corrección de identidad": desenmascarar a corporaciones multinacionales y a todo el entramado de intereses políticos y económicos tendentes a su protección, en perjuicio de los ciudadanos de todo el planeta. En: http://es.wikipedia.org/wiki/The_Yes_Men (consulta: 14 de agosto de 2019).

Tras varias semanas de publicaciones, WikiLeaks decidió ampliar su red de socios mediante un sistema de invitaciones personales a periodistas, investigadores académicos y activistas, seleccionados por esta organización para diversificar el trabajo y amplificar el eco de las filtraciones en tres campos estratégicos: los medios de comunicación de masas, la Academia y las organizaciones no gubernamentales de derechos humanos, en cualquier idioma y con distintos radios de influencia. Este sustancial giro en su estrategia colaborativa fue lo que nos permitió participar como socios de WikiLeaks en el proceso periodístico de los *GI Files*.

3. METODOLOGÍA

El 4 de agosto de 2012, WikiLeaks nos ofreció la posibilidad de unirnos a su grupo de investigación internacional dedicado a los *GI Files*, un inmenso archivo de 5.543.061 correos electrónicos de la empresa de inteligencia global Stratfor –"una especie de CIA corporativa" (Assange 2014: 21)–, datados entre julio de 2004 y diciembre de 2011. La invitación confidencial que recibimos[3] nos permitió introducirnos dentro del flujo comunicativo y, mediante una adaptación del método de observación participante, recoger y obtener información fundamental sobre las rutinas productivas operantes en este.

Esta invitación de WikiLeaks tuvo un doble valor para nosotros:

1) Pudimos conocer de primera mano, desde dentro, los métodos y procesos colaborativos de WikiLeaks y su estrategia para tratar la información y difundirla con el máximo impacto posible, lo cual nos permitió aplicar la línea de investigación observacional conocida como *newsmaking* –centrada en las rutinas productivas de los emisores (Elías, 2003; Retegui, 2017)– en un ecosistema de trabajo novedoso, virtual, propiciado por una organización red, donde cada nodo es independiente y goza de plena autonomía en el proceso de exploración, selección, producción, publicación y difusión de la información, aunque WikiLeaks impone ciertas condiciones para participar en este proceso colaborativo que veremos más adelante.

2) Nos dio la oportunidad de desarrollar la propia labor de investigación, edición y publicación periodística aplicada en complejos procesos de gestión y difusión de enormes volúmenes de información confidencial y secreta, enfrentándonos además a profundos dilemas éticos que necesitábamos experimentar en primera persona para comprender mejor la lucha dialéctica entre privacidad y secreto.

Como aconseja Wolf ([1987], 1996), la fase de observación estuvo ligada a nuestra hipótesis –en una investigación sobre el fenómeno WikiLeaks (Quian,

[3] La invitación se dirigió a título individual al correo electrónico personal del autor de este trabajo, Alberto Quian, como periodista previamente registrado en la red WLFriends (apartado 4.1). Una vez aceptada, el autor completó el proceso para acceder a la base de datos de los *GI Files* en representación del periódico digital *Galicia Confidencial*, utilizando una cuenta de correo corporativa, siguiendo las instrucciones de WikiLeaks (apartados 4.2.1.2 y 4.2.1.3).

2013; Quian y Elías, 2018)– de que el impacto de la red creada por Assange depende de la atención que le presten los grandes medios de información convencionales y de que las filtraciones sean controladas con las labores clásicas del periodismo, y no simplemente liberadas en bruto en un sitio web.

Nuestra investigación, mediante una adaptación del método de observación participante, responde al interés en ofrecer una explicación en el campo de la investigación académica sobre los procesos colaborativos y de producción de la noticia en el universo WikiLeaks, en un entorno nuevo, ciberespacial, en el que esta organización opera como proveedor central de información sensible y en bruto almacenada de manera masiva en repositorios virtuales y protegida mediante sistemas de encriptación, antes de su liberación. Alrededor de este nodo central se organiza toda una red ciberespacial de colaboradores que se conectan con este de manera independiente.

A diferencia de lo que sucede en las tradicionales experiencias físicas del investigador que se introduce, observa y participa en la vida cotidiana de la gente que está siendo objeto de estudio (Becker y Geer, 1958), nuestra inmersión se produce en un entorno virtual y secreto en el que no existe interacción humana propiamente dicha, sino mediada por tecnología. Esta nueva realidad de entornos virtuales, de organizaciones ciberespaciales y de nodos conectados por redes electrónicas nos obliga a redefinir y actualizar las descripciones que sobre el método de observación participante han dado diversos autores. Así, por ejemplo, si para McCall y Simmons (1969) es condición *sine qua non* "utilizar una cierta cantidad de interacción auténticamente social" (Elías, 2003: 149), en nuestro caso la interacción social se transforma en interactividad virtual y experiencia unipersonal y solitaria en una pantalla.

La observación, en este caso, es sobre el entorno virtual en el que se trabaja, sobre los instrumentos y procedimientos con los que se opera en este y sobre los flujos de comunicación e información, permitiéndonos describir las herramientas con las que se trabaja, los métodos y procesos colaborativos, y la estrategia de gestión y difusión de la información buscando el máximo impacto posible.

Dado que la nuestra es una observación participante mediada por la virtualidad tecnológica, en un entorno en el que no existe interacción humana en su sentido convencional, en el que las comunicaciones son electrónicas y automatizadas (o robotizadas) –a diferencia de lo que sucedió en las filtraciones de 2010, cuando la interacción humana fue determinante–, donde todo se produce en una pantalla y nuestra experiencia es unipersonal, subyace una autoobservación del propio sujeto investigador, que es a la vez sujeto investigado por sí mismo, que registra los procedimientos de su participación y los resultados de su propia actividad. Pero también hay introspección y autoevaluación de nuestra propia experiencia para generar un conocimiento autorreflexivo crítico adquirido por autoobservación.

En este entorno ciberespacial, las comunicaciones se producen del nodo central a los distintos nodos de la red WikiLeaks, que reciben los protocolos y herramientas para acceder a un espacio compartido pero protegido, donde cada nodo opera de manera independiente y goza de plena autonomía en el proceso

de exploración, selección, producción, publicación y difusión de la información, aunque WikiLeaks impone ciertas condiciones para participar en este proceso, pero sin afectar a la labor de sus colaboradores.

Con nuestro método nos sumamos a la discusión teórica sobre el estudio de los procesos y prácticas en el periodismo y las reconstrucciones de la producción de noticias –más compleja ahora, en entornos líquidos–, donde la "posición panóptica" de los periodistas es estratégica, ya que son los "únicos actores de la cadena de noticias que aún pueden ver la cadena completa" (Reich y Barnoy, 2020: 969).

Por último, nuestra aportación complementa la aproximación de Ihamäki (2014) a las comunidades virtuales generadas por WikiLeaks. En su caso, como observadora pasiva en el *ágora* de la comunidad virtual de WikiLeaks, su Foro Oficial (*https://www.wikileaks-forum.com/*); en el nuestro, como observadores participantes en la *fábrica secreta* de noticias.

4. RESULTADOS

A continuación detallamos todo el proceso de nuestra participación en el caso Stratfor: nuestro registro como socios colaboradores de WikiLeaks, los protocolos de seguridad, el acceso a la base de datos, el sistema de archivado, los sistemas de búsqueda de información, la producción periodística y la publicación y difusión coordinada con WikiLeaks de las informaciones que elaboramos a partir de los correos electrónicos y documentos adjuntos encontrados en nuestra fase de exploración de los *Global Intelligence Files*.

4.1. Primer registro: Wlfriends

El 20 de mayo de 2012, WikiLeaks anunció en su cuenta en Twitter (figura 1) su intención de lanzar WLFriends –también llamada FoWL (Friends of WikiLeaks) y presentada como el "Facebook encriptado"–, una red social creada para rivalizar con su antagonista natural: Facebook (Quian, 2013a).

Figura 1: WikiLeaks [wikileaks]. (2012, May 20). WikiLeaks 'encrypted Facebook' is almost ready to launch https://t.co/xWcS5ckQ [Tweet]. Recuperado de https://twitter.com/wikileaks/status/204269367100321793.

La organización anunció WLFriends como una red independiente de la actividad de la propia organización que mantendría a salvo los datos de sus usuarios de forma codificada, empleando criptografía de grado militar. En su cuenta en Twitter, explicó en doce puntos la esencia de esta red social[4]:

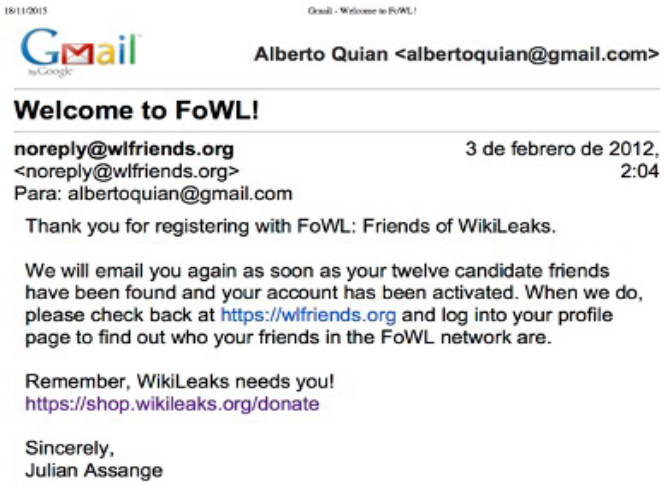
1. WLFriends te pone en contacto con personas que quieres conocer, pero que aún no conoces. Facebook te conecta con gente que ya conoces, lo cual no tiene sentido.
2. Facebook es una herramienta de vigilancia masiva. Tú pones a tus amigos en ella, tú traicionas a tus amigos. ¿Los amigos traicionan a los amigos? WLFriends no conoce a tus amigos. Te presenta nuevos amigos.
3. Facebook registra todo lo que haces, se lo entrega al Gobierno de Estados Unidos y a las corporaciones. WLFriends no lo hace.
4. WLFriends mantiene tus datos encriptados, ni siquiera los administradores del sistema pueden descifrarlos.
5. WLFriends utiliza criptografía de grado militar y los mejores estándares de la industria (OpenPGP + Elliptic Curves)
6. WLFriends incluso utiliza cifrado homomórfico para ciertas operaciones, de manera que WLFriends no sabe cuántos amigos tienes en esta red.
7. Cuanto más utilices WLFriends, menos lo estarás utilizando. La red está diseñada para construir, no para controlar, una robusta red de valores compartidos.

[4] Traducción propia. Textos originales disponibles en la cuenta de Twitter de WikiLeaks (https://twitter.com/wikileaks).

8. WLFriends está diseñada para algo más que WikiLeaks. Es una solución general para construir una robusta red de apoyo ante condiciones hostiles.
9. Amigos de Israel, de Palestina, del Tea Party, del catolicismo son todos posibles con WLFriends.
10. WLFriends está diseñado para que las infiltraciones sean muy costosas. Ninguna persona puede considerarse más importante que otra o que cualquier objetivo individual.
11. WLFriends construye una fuerte red de apoyo de manera instantánea para cualquier creencia compartida, conectando a partidarios de esta de un modo que maximiza la comunicación.
12. La red WLFriends para cualquiera causa común ha sido diseñada para que, conforme pase el tiempo, crezca matemáticamente cada vez más fuerte.
13. (WikiLeaks, 20 de mayo de 2012).

El 3 de febrero de 2012 procedimos al registro de una cuenta de usuario en esta red social (figura 2) con la intención de escrutar con fines investigativos WLFriends y de entrar en contacto con partidarios de WikiLeaks, para iniciar nuestra observación participante de esta comunidad virtual. Fue un ejercicio en vano, ya que nunca llegó a ser una red plenamente operativa y fue desactivada finalmente. Entre el 3 de febrero de 2012 y el 25 de enero de 2013 –fecha de la última comunicación que recibimos de WLFriends–, nos llegaron por correo electrónico un total de diecisiete avisos de esta red social para: completar y confirmar nuestro registro, el 3 de febrero de 2012; otros dos –uno en inglés el 21 de junio y otro en español el 25 de junio– para avisarnos de que la red estaría pronto plenamente operativa y de que se había actualizado su sistema de seguridad; otro, el 4 de julio para anunciarnos que la red había sido finalmente lanzada el día 2 de ese mismo mes y que se iniciaba el proceso de asignación de amistades basándose en intereses temáticos y áreas geográficas; y el resto de comunicaciones, hasta el 25 de enero de 2013, para avisarnos de nuevas asignaciones de amistades e informarnos sobre cuestiones relativas a la operatividad de la red, la financiación de WikiLeaks y acontecimientos relacionados con las filtraciones de documentos, a modo de boletín de noticias.

Figura 2: Registro y participación en la red social WLFriends.


18/11/2015 Gmail - Welcome to FoWL!

Gmail by Google

Alberto Quian <albertoquian@gmail.com>

Welcome to FoWL!

noreply@wlfriends.org 3 de febrero de 2012, 2:04
<noreply@wlfriends.org>
Para: albertoquian@gmail.com

Thank you for registering with FoWL: Friends of WikiLeaks.

We will email you again as soon as your twelve candidate friends have been found and your account has been activated. When we do, please check back at https://wlfriends.org and log into your profile page to find out who your friends in the FoWL network are.

Remember, WikiLeaks needs you!
https://shop.wikileaks.org/donate

Sincerely,
Julian Assange

Fruto de nuestro registro como periodistas e investigadores en WLFriends, recibimos ese mismo año una invitación de WikiLeaks para unirnos al grupo de investigación internacional dedicado a los *GI Files*.

4.2. FASES

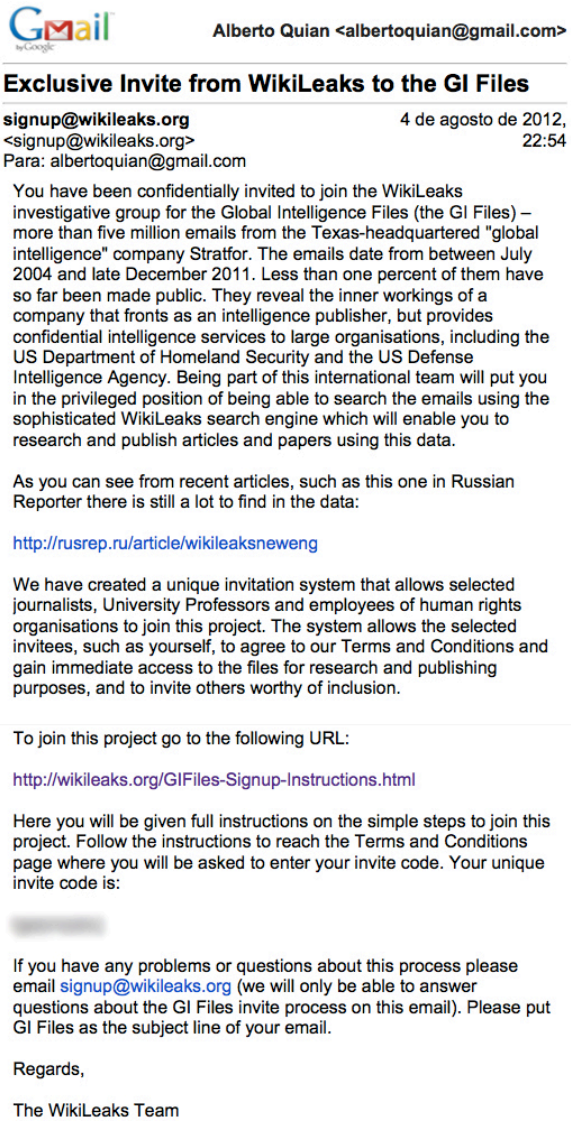
4.2.1. Fase 1: Registro y aceptación de términos y condiciones

4.2.1.1. Introducción

El 4 de agosto de 2012 recibimos la invitación en nuestro correo electrónico. Hasta ese momento, apenas un uno por ciento de los 5.543.061 de correos electrónicos filtrados de Stratfor había sido publicado desde el 27 de febrero de aquel año (WikiLeaks, comunicación por correo electrónico, 4 de agosto de 2012), cuando se anunció esta filtración masiva, la mayor ejecutada por WikiLeaks por volumen de archivos.

Según la propia organización, estos correos revelan el funcionamiento interno de una empresa que actúa como un "editor de inteligencia" que "provee servicios de inteligencia confidenciales a grandes organizaciones, entre ellas, el Departamento de Seguridad Nacional y la Agencia de Inteligencia de Defensa de Estados Unidos" (figura 3).

Figura 3: Invitación para investigar los *GI Files*.



Gmail Alberto Quian <albertoquian@gmail.com>

Exclusive Invite from WikiLeaks to the GI Files

signup@wikileaks.org 4 de agosto de 2012, 22:54
<signup@wikileaks.org>
Para: albertoquian@gmail.com

You have been confidentially invited to join the WikiLeaks investigative group for the Global Intelligence Files (the GI Files) – more than five million emails from the Texas-headquartered "global intelligence" company Stratfor. The emails date from between July 2004 and late December 2011. Less than one percent of them have so far been made public. They reveal the inner workings of a company that fronts as an intelligence publisher, but provides confidential intelligence services to large organisations, including the US Department of Homeland Security and the US Defense Intelligence Agency. Being part of this international team will put you in the privileged position of being able to search the emails using the sophisticated WikiLeaks search engine which will enable you to research and publish articles and papers using this data.

As you can see from recent articles, such as this one in Russian Reporter there is still a lot to find in the data:

http://rusrep.ru/article/wikileaksneweng

We have created a unique invitation system that allows selected journalists, University Professors and employees of human rights organisations to join this project. The system allows the selected invitees, such as yourself, to agree to our Terms and Conditions and gain immediate access to the files for research and publishing purposes, and to invite others worthy of inclusion.

To join this project go to the following URL:

http://wikileaks.org/GIFiles-Signup-Instructions.html

Here you will be given full instructions on the simple steps to join this project. Follow the instructions to reach the Terms and Conditions page where you will be asked to enter your invite code. Your unique invite code is:

If you have any problems or questions about this process please email signup@wikileaks.org (we will only be able to answer questions about the GI Files invite process on this email). Please put GI Files as the subject line of your email.

Regards,

The WikiLeaks Team

Dada la complejidad de estas filtraciones, con un archivo de más de cinco millones y medio de correos electrónicos imposibles de abordar para los veintinueve medios seleccionados en un principio por WikiLeaks, la investigación y publicación se abrió a más potenciales colaboradores. WikiLeaks creó un siste-

ma de invitación única y confidencial para "periodistas, profesores universitarios y trabajadores de organizaciones de derechos humanos seleccionados para unirse a este proyecto". El sistema permitía a los invitados que aceptasen los 'Términos y Condiciones' de WikiLeaks "obtener acceso inmediato a los archivos con fines de investigación y publicación, e invitar a otras personas dignas de ser incluidas" (WikiLeaks, comunicación por correo electrónico, 4 de agosto de 2012). Es decir, WikiLeaks buscaba ampliar su red de colaboradores para acelerar y extender la publicación de los correos y documentos adjuntos de los *GI Files* que fuesen de interés académico, periodístico y humanitario.

4.2.1.2 Instrucciones

La invitación incluía un manual de instrucciones y un código de invitación único para "entrar en un mundo secreto". El equipo de WikiLeaks reconoce que el propósito de este sistema de invitaciones selectivas y confidenciales, para acceder a los correos y documentos adjuntos, es "maximizar el impacto global de los *GI Files*, restringiendo el acceso a aquellas personas con más probabilidades de investigar y publicar sobre éstos". Además, los usuarios que demostrasen su "habilidad de investigación y publicación" serían considerados socios para otras publicaciones de WikiLeaks[5] (WikiLeaks, comunicación por correo electrónico, 4 de agosto de 2012).

A continuación, exponemos los pasos a seguir, indicados por WikiLeaks:

14. Tener instalado el navegador web Tor (The Onion Router), herramienta que nos conecta a la red distribuida y de conexiones encriptadas Tor, que garantiza el anonimato y la privacidad de nuestras comunicaciones. Solo a través de Tor se podía acceder a la página de 'Términos y Condiciones' de los *GI Files* y a su base de datos[6].
15. Ejectutar Tor y dirigirse al siguiente sitio web: http://7f4lihm464gdcwfc.onion/invite/step1 (solo era operativo usando Tor).
16. Introducir el código de invitación único recibido para tener acceso a los 'Términos y Condiciones' de los *GI Files*.

[5] El 12 de septiembre de 2012 recibimos otra invitación de WikiLeaks para participar en la investigación y publicación de los conocidos como *Syria Files*, más de dos millones de correos electrónicos de figuras políticas y ministerios sirios, y de empresas asociadas al Gobierno de este país, fechados entre agosto de 2006 y marzo de 2012 (ver Anexo). Los procesos y procedimientos de invitación, registro, sistema de búsqueda, publicación y difusión son los mismos que en el caso descrito de los *GI Files*. La invitación fue aceptada, pero nos centramos en la investigación de los correos de Stratfor fundamentalmente por dos razones: una, por el enorme esfuerzo que ya suponía para una sola persona explorar, seleccionar, cotejar, verificar, producir y publicar la información obtenida de Stratfor; otra, porque queríamos centrarnos en un caso que era paradigmático para nuestra investigación: la filtración de documentos de una empresa de inteligencia que se dedica al tráfico de información local, regional, nacional y global.

[6] Tor se puede descargar en https://www.torproject.org/ (consulta: 17 de agosto de 2019).

17. En la página de 'Términos y Condiciones', introducir nuestro nombre, el de la organización a la que representamos (en este caso, el periódico digital *Galicia Confidencial*), una dirección de correo electrónico que no puede ser de uso personal, sino laboral, y un número de teléfono de contacto.
18. Leer todos los puntos de los 'Términos y Condiciones' y asegurarnos de que entendemos las responsabilidades que debemos asumir.
19. Marcar la casilla de verificación para confirmar el acuerdo.
20. Abrir el mensaje posteriormente recibido en la dirección de correo electrónico proporcionada, con el usuario y clave asignados para acceder a la base de datos de los *GI Files*.
21. Entrar en el sitio de los *GI Files* en la URL http://7f4lihm464gdcwfc.onion/ introduciendo el nombre de usuario y contraseña recibidos. A esta URL solamente se puede acceder mediante Tor.
22. Una vez iniciada la sesión en el sitio web de los *GI Files*, se tiene acceso a la página de usuario, la interfaz de búsqueda y la interfaz de edición.
23. En la página de usuario existen cinco códigos de invitación que se pueden enviar a otros tantos investigadores. Se establecen una serie de condiciones: a) el invitado debe ser una persona real; b) debe ser un periodista, un profesor de universidad o un trabajador de una organización que actúe en defensa de los derechos humanos; c) la organización a la que represente el invitado debe ser diferente a la del usuario que envía la invitación y a las de los otros invitados; d) no debe usar un correo personal; e) el dominio del correo electrónico de un invitado debe ser diferente al del usuario que envía la invitación y a los de los otros invitados; e) el invitado debe usar sus privilegios como usuario para trabajos de investigación y sus resultados deben ser comunicados al público.
24. Si se viola cualquiera de los 'Términos y Condiciones', la cuenta del investigador y de aquéllos a los que haya invitado pueden ser canceladas.
25. Por último, WikiLeaks ofrece dos canales de chat que se pueden utilizar exclusivamente para resolver dudas sobre este proceso: uno para tratar problemas relacionados con Tor y otro para plantear cuestiones relativas a la base de datos y el trabajo de investigación.

4.2.1.3 Acuerdo entre las partes

El siguiente paso es el registro y aceptación de los 'Términos y Condiciones' de WikiLeaks para el acceso a los *GI Files*. Para ello, accedemos mediante Tor a la página web de 'Terms and Conditions Agreement for GI Files', donde introducimos nuestro nombre, el de la organización a la que representamos y los

datos de contacto. Bajo las casillas para el registro se disponen los 'Términos y Condiciones', que constituyen un acuerdo entre nosotros –como individuos, no como organización– y WikiLeaks para el uso de estos archivos[7]:

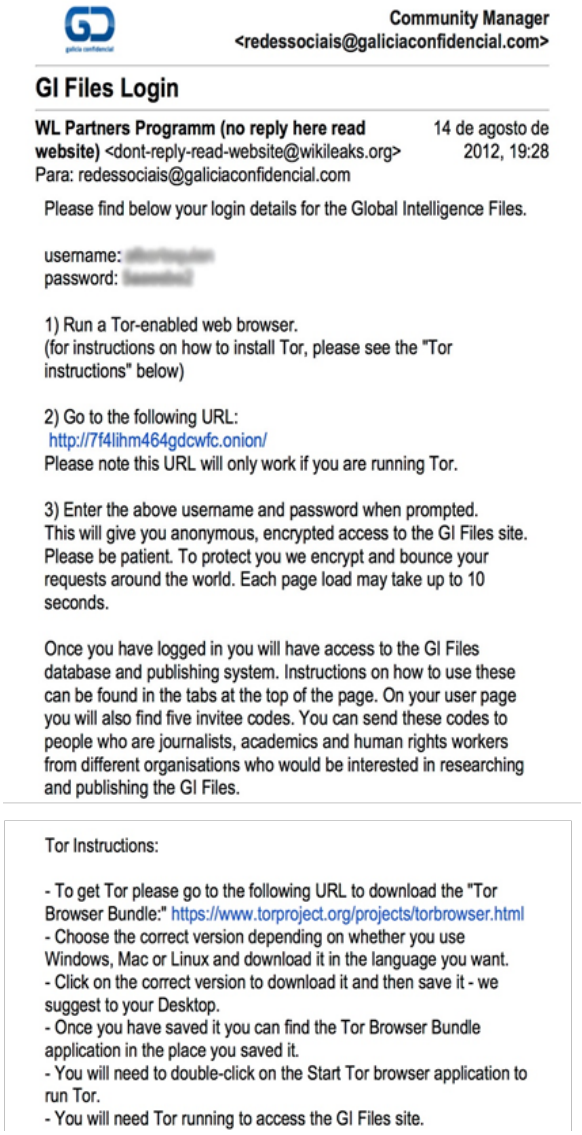
1. WikiLeaks proporciona el acceso a los *GI Files* a través de la base de datos de WikiLeaks y su sistema de búsqueda. Esta debe usarse según las instrucciones del sitio y no pueden utilizarse robots en el sistema.
2. El investigador tiene la potestad exclusiva de decidir qué información se publica en artículos de prensa o académicos, pero deberá atribuir a WikiLeaks el origen de su investigación y reconocer que los documentos han sido obtenidos por esta organización.
3. El investigador debe hacer una referencia clara a los documentos obtenidos por WikiLeaks utilizados en los artículos publicados, y proporcionar un enlace a los datos en la página web de WikiLeaks.
4. Las fuentes de WikiLeaks están sujetas a las protecciones éticas y legales a las que tienen derecho como fuentes confidenciales. De acuerdo con la ética periodística y profesional, no se puede especular sobre sus identidades. En relación con el suministro de información confidencial por parte de WikiLeaks, esta organización debe ser tratada como fuente periodística confidencial. Por lo tanto, aunque el investigador debe reconocer públicamente que la información documental ha sido obtenida por WikiLeaks, no se debe decir que esta ha sido proporcionada directamente por WikiLeaks, para la protección legal de la propia organización, de sus fuentes y del propio investigador.
5. Antes de publicar cualquier historia o material basado en los *GI Files* el investigador debe informar a WikiLeaks del número de identificación de los datos utilizados en su trabajo, que debe registrar en la plataforma de publicación de WikiLeaks antes de que se publique en cualquier otro sitio, de manera que WikiLeaks pueda liberar los datos originales al mismo tiempo. De esta manera, el investigador se asegura además la exclusividad de su trabajo. El investigador debe proporcionar previamente a WikiLeaks, mediante un sistema de registro, el enlace a la URL del sitio web en la que aparecerá la historia o el material documental, un título descriptivo del contenido y la fecha y hora de publicación programadas. Este sistema de liberación proporcionado por WikiLeaks debe ser tratado con respeto, es decir, no se debe programar la publicación de grandes cantidades de datos con antelación simplemente para reservarse la exclusividad sobre éstos ni se permite el uso de robots en el sistema (para evitar un uso abusivo, el sistema de WikiLeaks solo permite programar historias con un mes de antelación). Las fechas y horas programadas para la liberación de la información deben cumplirse siempre, para garantizar el buen uso de los datos.

[7] Ofrecemos una traducción propia adaptada del documento original.

6. El investigador debe tratar los documentos obtenidos de la base de datos de WikiLeaks como confidenciales, a menos que ya hayan sido publicados por otros investigadores o hasta que se liberen. Por lo tanto, el investigador debe proteger la seguridad de esos materiales hasta que sean publicados.
7. Dado que los periodistas de WikiLeaks, empleados, consultores y su propia infraestructura sufren el acecho de las agencias de inteligencia estatales y privadas y un bloqueo financiero, es necesario proteger su capacidad de publicar protegiendo sus identidades y ubicaciones. A menos que se indique lo contrario, esto incluye, pero no se limita a: la identificación de detalles de todo el personal de WikiLeaks, métodos de seguridad, sistemas o métodos de comunicación, localizaciones, planes estratégicos, información sobre amenazas contra WikiLeaks, la cantidad de personal que trabaja para WikiLeaks en diferentes áreas, nombres de usuario, contraseñas o acuerdos financieros, incluyendo métodos de transporte financiero.
8. Está prohibido comerciar con la cuenta de usuario de los *GI Files*. No se puede vender, compartir o transferir la cuenta personal ni vender u ofrecer públicamente las invitaciones.
9. El usuario entiende que cualquier violación de estos 'Términos y Condiciones', o la mala gestión de la base de datos o de la plataforma para liberar los documentos, supone una retirada de los privilegios para acceder a los *GI Files*, tanto para el propio usuario como para cualquier persona que haya invitado. El usuario es responsable de su propia cuenta y de las de las personas a las que invite.

Bajo estos 'Términos y Condiciones' se debe marcar una casilla para confirmar que el investigador se compromete a cumplirlos. Una vez hecho todo esto, se envía el registro al sistema de WikiLeaks, que nos devuelve un correo electrónico de confirmación con el nombre de usuario y contraseña para acceder a la base de datos (figura 4).

Figura 4: Invitación para investigar los *GI Files*.



Community Manager
<redessociais@galiciaconfidencial.com>

GI Files Login

WL Partners Programm (no reply here read website) <dont-reply-read-website@wikileaks.org>
14 de agosto de 2012, 19:28
Para: redessociais@galiciaconfidencial.com

Please find below your login details for the Global Intelligence Files.

username: [redacted]
password: [redacted]

1) Run a Tor-enabled web browser.
(for instructions on how to install Tor, please see the "Tor instructions" below)

2) Go to the following URL:
http://7f4lihm464gdcwfc.onion/
Please note this URL will only work if you are running Tor.

3) Enter the above username and password when prompted.
This will give you anonymous, encrypted access to the GI Files site.
Please be patient. To protect you we encrypt and bounce your requests around the world. Each page load may take up to 10 seconds.

Once you have logged in you will have access to the GI Files database and publishing system. Instructions on how to use these can be found in the tabs at the top of the page. On your user page you will also find five invitee codes. You can send these codes to people who are journalists, academics and human rights workers from different organisations who would be interested in researching and publishing the GI Files.

Tor Instructions:

- To get Tor please go to the following URL to download the "Tor Browser Bundle:" https://www.torproject.org/projects/torbrowser.html
- Choose the correct version depending on whether you use Windows, Mac or Linux and download it in the language you want.
- Click on the correct version to download it and then save it - we suggest to your Desktop.
- Once you have saved it you can find the Tor Browser Bundle application in the place you saved it.
- You will need to double-click on the Start Tor browser application to run Tor.
- You will need Tor running to access the GI Files site.

4.2.2. Fase 2: Acceso y exploración

4.2.2.1. Introducción

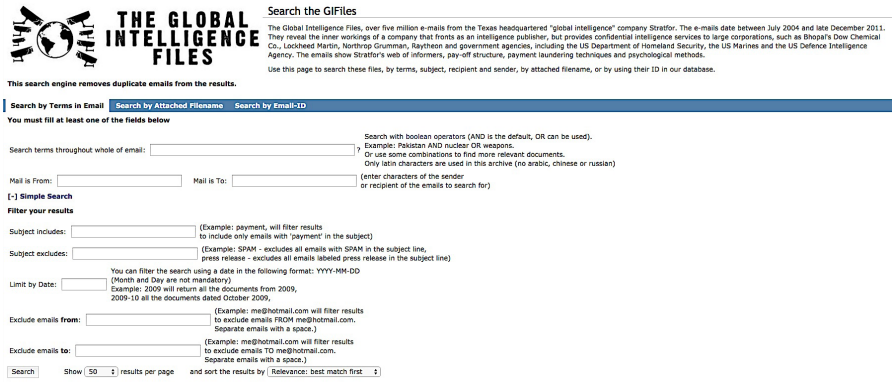
Una vez recibidos el usuario y clave asignados, procedemos a ingresar en el sitio web de los *GI Files*. Para ello, se nos proporciona una URL que solo es operativa a través de Tor. En esta página de destino es donde introducimos nuestros datos para obtener el acceso anónimo y encriptado a la base de datos.

Todo el proceso de carga de páginas a partir de aquí es lento debido al sistema de seguridad que se aplica. De media, una página puede tardar hasta diez segundos en cargarse en este sistema, aunque en numerosas ocasiones se demora más, sufriendo incluso algunos cortes temporales en las conexiones, lo que ralentiza aún más el proceso de exploración en una base de datos inmensa como esta.

4.2.2.2. Sistema de búsqueda

WikiLeaks pone a disposición del investigador un "sofisticado buscador" (figura 5) para encontrar correos electrónicos que coincidan con sus criterios de búsqueda. A continuación, describimos sus características.

Figura 5: Buscador para los GI Files.



a) Búsqueda por términos

En la caja de búsqueda podemos introducir cualquier término para obtener correos electrónicos que puedan contener las palabras introducidas, tanto en los campos del remitente, destinatario y asunto del *email*, como en el propio texto de los correos y en los documentos adjuntos. El sistema admite el uso de operadores *booleanos* de búsqueda similares a los que permite Google para refinar las búsquedas. Por ejemplo, se puede usar el signo + entre términos para forzar su inclusión, de manera que solo obtendremos los archivos que contengan todas las palabras indicadas, o se puede incluir *OR* entre dos términos para que el sistema busque contenidos con una u otra palabra. También se pueden usar caracteres

comodines, por ejemplo, el símbolo del asterisco (*) para buscar una cadena de caracteres (si, por ejemplo, introducimos *block**, obtendremos resultados para *block*, *blocked*, *blockade*, *blocking*, etc.).

a.1) Filtros

a.1.1) Filtro por remitente y destinatario

Uno de los filtros que podemos aplicar a las búsquedas por términos es incluir el remitente y/o destinatario de los correos que estamos buscando, de manera que el sistema nos devolverá solo los documentos que incluyen nuestros términos de búsqueda y que han sido enviados y/o recibidos por cuentas de correo particulares. No es necesario introducir la dirección completa, basta con incluir solo el nombre identificador (a la izquierda de la arroba y del dominio). Por ejemplo, podemos hacer una búsqueda para la palabra *Spain* e incluir el nombre *Bart* en los cuadros 'Mail from' o 'Mail to' para identificar todos los correos enviados desde o a la cuenta bart@stratfor.com[8] referidos a España.

a.1.2) Filtro por el asunto de los correos

Disponemos de una caja llamada 'Subject includes' para limitar la búsqueda de nuestros términos solo a los correos electrónicos que tienen una determinada palabra en el campo 'Asunto'. Por ejemplo, si hacemos una búsqueda para la palabra *wikileaks* en el campo general de términos e introducimos la palabra *alfa* en la casilla 'Subject includes', obtenemos solo los mensajes de correo electrónico que se refieren a WikiLeaks y que contienen la palabra *alfa* en la línea de asunto del correo electrónico. De igual modo, disponemos de una caja 'Subject excludes' que limita los resultados de uno o varios términos de búsqueda a los mensajes de correo electrónico que no tengan una determinada palabra en su campo Asunto.

a.1.3) Filtro temporal

Podemos también filtrar contenidos por su fecha de envío, en la caja 'Limit by Date'. Esta opción permite buscar correos electrónicos para uno o más términos limitados a un año concreto, a un mes de un año concreto o a un día concreto de un mes y año determinados.

Todas estas opciones pueden ser combinadas para refinar las búsquedas, pero siempre se debe introducir al menos una palabra en la caja de búsqueda por términos.

Los correos devueltos en la búsqueda pueden ser desplegados en pantalla en grupos de diez, veinte, cincuenta, cien, doscientos, quinientos o mil, agrupados en una página de resultados, y pueden ser ordenados por relevancia, por fecha de publicación (ordenados desde los más recientes hasta los más antiguos, o viceversa) o por orden alfabético de los remitentes (de la A a la Z, o viceversa).

Búsqueda por nombre de archivos

[8] Este es un ejemplo ficticio de cuenta de correo electrónico de Stratfor.

El sistema de WikiLeaks ofrece también hacer búsquedas por palabras incluidas en los nombres de los archivos adjuntos a los correos electrónicos. Por ejemplo, si introducimos en este buscador la palabra *payment*, obtenemos todos los correos electrónicos que tienen un archivo adjunto con este término.

Búsqueda por ID de documento

Otra opción es buscar un correo electrónico específico por su identificador, si se conoce previamente el ID numérico.

Clasificación de los correos

Stratfor clasifica sus correos en grandes grupos mediante códigos incluidos en el campo 'Asunto'. Los encabezados más comunes son: 'OS' (Open-Source), 'Analysis', 'Insight', 'Report', 'Discussion' y 'Question'. La mayoría son fáciles de comprender y son útiles para aplicar filtros en las búquedas. Sin embargo, otros códigos son más limitados en su uso, pero son relevantes, como por ejemplo 'Alpha', utilizado en correos relacionados con las fuentes e informantes de Stratfor en el extranjero, y que pertenecen al departamento de operaciones de la compañía.

En muchos casos, la información relevante se obtiene rastreando las comunicaciones de individuos específicos, por lo que es útil introducir sus nombres y/o direcciones de correo electrónico, pero sin copiar la dirección completa, dado que la función de búsqueda general no reconoce el símbolo @, excepto cuando se introduce la dirección completa de correo electrónico entre comillas.

También es importante destacar que en los correos posteriores al año 2006 las referencias a las fuentes e informantes de Stratfor se hacen con códigos, en lugar de utilizar sus nombres, para proteger sus identidades; por ejemplo: ME213.

4.2.3. Fase 3: Producción, publicación y difusión

4.2.3.1. Introducción

Fruto de nuestra exploración en la base de datos de los *GI Files*, publicamos once piezas periodísticas entre el 21 de agosto de 2012 y el 20 de mayo de 2013, en el periódico digital *Galicia Confidencial* (*galiciaconfidencial.com*) –medio en lengua gallega–, la mayor parte basadas en correos y documentos relacionados con temas políticos y económicos que afectan directamente a Galicia, aunque también publicamos algunos artículos con contenidos sobre realidades más amplias que fueron exclusivas nacionales o internacionales (tabla 1).

Tabla 1: Artículos publicados fruto de la investigación.

NOTICIA	ENLACE	FECHA
A maior compañía de espionaxe do mundo vixía o independentismo galego	http://www.galiciaconfidencial.com/noticia/11285-maior-compania-espionaxe-mundo-vixia-independentismo-galego	21-08-2012
Un analista de Stratfor aconsellou facer un seguimento a Resistencia Galega	https://www.galiciaconfidencial.com/noticia/11331-analista-stratfor-aconsellou-facer-seguimento-resistencia-galega	27-08-2012
"O plan en España é que o Santander tome o control como un banco central"	https://www.galiciaconfidencial.com/noticia/11345-plan-espana-santander-tome-control-banco-central	31-08-2012
Os negocios sucios do fretador do 'Prestige'	https://www.galiciaconfidencial.com/noticia/11470-negocios-sucios-fretador-prestige	13-09-2012
España xa advertiu do "enorme poder" de Alemaña na UE	https://www.galiciaconfidencial.com/noticia/12058-espana-advertiu-enorme-poder-alemana-ue	05-11-2012
Os negocios de España na guerra libia	http://www.galiciaconfidencial.com/noticia/12786-negocios-espana-guerra-libia	10-01-2013
Os intereses europeos na guerra en Libia	https://www.galiciaconfidencial.com/noticia/12815-intereses-europeos-guerra-libia	14-01-2013
Que pactou o PP cos mercados antes do 20N?	https://www.galiciaconfidencial.com/noticia/13297-pactou-pp-mercados-20n	20-02-2013
Pemex (I): corrupción, crimes e inseguridade no novo dono de Barreras	http://www.galiciaconfidencial.com/noticia/14300-pemex-i-corrupcion-crimes-inseguridade-novo-dono-barreras	09-05-2013
Pemex (II): opacidade, creba técnica e deslocalización de Barreras	https://www.galiciaconfidencial.com/noticia/14336-pemex-ii-opacidade-creba-tecnica-deslocalizacion-barreras	13-05-2013
Pemex (III): a 'caixa chica' de políticos e paraíso de sindicalistas corruptos	https://www.galiciaconfidencial.com/noticia/14322-pemex-iii-caixa-chica-politicos-paraiso-sindicalistas-corruptos	20-05-2013

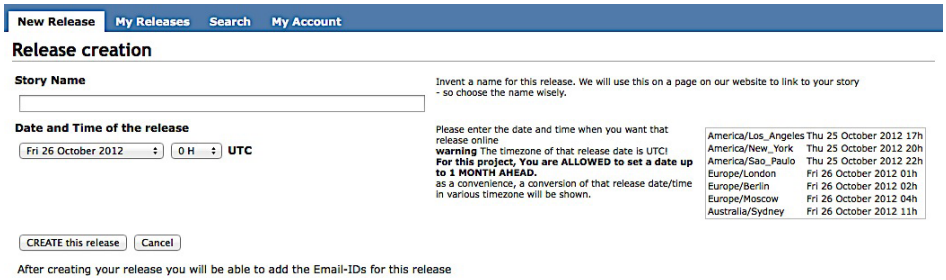
Todas estas investigaciones se basan en correos electrónicos y documentos encontrados en la base de datos de los *GI Files*, aunque también se usaron otras fuentes de información para verificar, contrastar y completar el trabajo periodístico.

Con la elección de este medio quisimos comprobar si era posible, y de qué manera, integrar y hacer participar a un medio regional en un fenómeno de dimensiones globales.

4.2.3.2. Programación de las publicaciones

La publicación de informaciones y documentos de los *GI Files* debía ser coordinada con WikiLeaks, según los términos y condiciones del acuerdo de colaboración. Antes de publicar cualquier material, una vez editado y preparado para su liberación, debíamos registrar en el sistema de WikiLeaks la URL donde se publicaría, un título de la información, los identificadores de los correos electrónicos y documentos utilizados, así como la fecha y hora previstas para la publicación en nuestro medio, de manera que WikiLeaks pudiese también hacer un seguimiento de la publicación y difundirla desde la propia página web de WikiLeaks y desde sus cuentas en Twitter y Facebook (figura 6).

Figura 6: Sistema de registro de publicaciones en WikiLeaks.



Los pasos fueron:

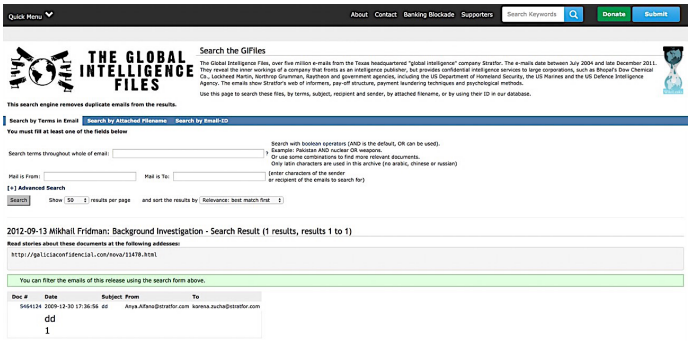
1. Ir a la pestaña ‘New release’ en nuestra cuenta de usuario.
2. En la casilla ‘Story name’, introducir un título descriptivo y comprensible de nuestra publicación.
3. En el cuadro ‘Date and Time of the release’, introducir la fecha y hora exacta programadas para la liberar la información.
4. Una vez hecho todo esto, ejecutar la acción ‘Create this release’. Hasta que no se realiza, no se pueden introducir los identificadores de los correos electrónicos utilizados.
5. En la casilla ‘Story urls’ hay que introducir el o los hiperenlaces del sitio web donde se publica la información. De esta manera, WikiLeaks, además de publicar estos enlaces en sus canales de comunicación, asocia las URL a los correos electrónicos, una vez liberados, para que quede constancia de dónde es tratada esa información.

6. En el cuadro ‘Email IDs to include in this release’, introducir el identificador de los correos electrónicos utilizados en la investigación y ejecutar la acción ‘Add this email ID’ para incluirlo en la publicación.
7. Tras introducir estos detalles el registro se puede guardar de dos maneras: 1) guardar un borrador en el apartado ‘My releases’ si es necesario editar más información antes de liberar los documentos, o 2) confirmar y bloquear el registro para su publicación, de manera que ya no podrá ser editado. En este último paso es necesario marcar la casilla ‘Ready’ y luego ejecutar la función ‘Save’ para confirmar la programación de la publicación. Una vez hecho esto, el sistema nos confirma la URL pública de WikiLeaks en la que serán liberados los correos y el enlace a la página web donde publicamos nuestra información. También se nos informa si alguno de estos correos ha sido antes confirmado y publicado por otro socio colaborador o si va a ser liberado por otros antes de la fecha y hora programadas por nosotros.

4.2.3.3. Difusión

Todas las piezas informativas se publicaron a la vez en la página web de *Galicia Confidencial* y en la de WikiLeaks, donde nuestro trabajo fue incluido en el registro público de las filtraciones de los *GI Files* (figura 7).

Figura 7: Registros de los correos y documentos en el buscador de WikiLeaks incluyen enlaces a nuestras informaciones.



A medida que fuimos publicando nuestras informaciones, WikiLeaks fue liberando en su sitio web los correos electrónicos y documentos adjuntos confidenciales para que cualquier persona pudiese consultarlos en su sitio web (figuras 8 y 9). De esta manera, y gracias a su red de colaboradores, WikiLeaks fue creando un gran registro público con la información en bruto (correos y do-

cumentos) y enlaces a la información editada que se iba publicando (trabajos de los socios investigadores).

Figura 8: Ficha de nuestro trabajo sobre Mikhail Fridman.

Barack Obama's Courtship of Bashar al-Assad	2012-09-14
Mikhail Fridman: Background Investigation	2012-09-13
FBI and Stratfor Two Dysfunctional Peas in a Pod	2012-09-12
Greetings - Our govt is capable of anything	2012-09-11
Obama Leak Investigation	2012-09-10
The Hondura's chaos: Fox News and Roger F. Noriega can tell us the Hugo Chavez's secret plan	2012-09-09

Figura 9: Nuestro trabajo sobre Mikhail Fridman, en la lista de los *GI Files* de WikiLeaks.

Barack Obama's Courtship of Bashar al-Assad	2012-09-14
Mikhail Fridman: Background Investigation	2012-09-13
FBI and Stratfor Two Dysfunctional Peas in a Pod	2012-09-12
Greetings - Our govt is capable of anything	2012-09-11
Obama Leak Investigation	2012-09-10
The Hondura's chaos: Fox News and Roger F. Noriega can tell us the Hugo Chavez's secret plan	2012-09-09

WikiLeaks colaboró además en la difusión de nuestros trabajos en las redes sociales en línea. Mientras nosotros hacíamos circular los enlaces por los canales sociales que *Galicia Confidencial* utiliza para difundir sus informaciones, WikiLeaks estaba utilizando paralelamente los suyos para hacer llegar nuestras informaciones a su comunidad de seguidores en Twitter y Facebook. En sus

publicaciones en las redes sociales incluían dos enlaces: uno a la información editada y publicada en *Galicia Confidencial* y otro a la información en bruto liberada en el sitio web de WikiLeaks (Figura 10).

Figura 10: WikiLeaks [wikileaks]. (2012, Sep. 15). WikiLeaks: Os negocios sucios do fretador do 'Prestige' http://t.co/0IqSeHw8 http://t.co/mYvBxyrs [Tweet]. Recuperado de https://twitter.com/wikileaks/status/246794427480285184

5. DISCUSIÓN Y CONCLUSIONES

Siguiendo a McCall y Simmons (1969), la observación participante se presenta como el método idóneo para investigar y comprender cómo funciona una organización compleja –en nuestro caso, WikiLeaks– y su flujo informativo. Si atendemos, además, a Wolf ([1987], 1996), este método es el más adecuado para estudiar la sociología de los emisores en el proceso informativo.

Sin embargo, para Wolf, el observador puede correr el riesgo de confundirse con un "participante de pleno derecho", fase conocida como "*going native*", un proceso de socialización en el que la objetividad y la crítica se diluyen, y la actividad pasa a ser dominada por la adhesión a los valores de la organización objeto de estudio y una implicación personal del investigador con los objetivos de esta. Ese riesgo de volverse "nativo" (Kerr y Hiltz, 1982) está relacionado con la pérdida de una perspectiva neutral en la descripción y análisis del observador (Paccagnella, 1997).

Este riesgo se intentó minimizar al máximo, primero, participando solamente en una de las dos filtraciones a las que nos dio acceso WikiLeaks –*GI Files* y *Syria Files*–, priorizando el análisis del proceso investigativo de un caso concreto y paradigmático por su volumen de registros (los correos de Stratfor), frente a la tentación periodística de abarcar y publicar el mayor número de documentos e informaciones posibles, en el marco de una filtración masiva de impacto mundial; en segundo lugar, relacionado con lo anterior, marcando un final del proceso –una vez publicadas las once piezas informativas elaboradas–, tras el cual la colaboración con WikiLeaks se dio por concluida para proceder al análisis de la experiencia investigadora siguiendo las pautas de Schlesinger (1981), quien propone un "*disengagement*", esto es, la interrupción o la conclusión del periodo de trabajo de campo y la desconexión con el sistema en estudio; por último, aprovechando la virtualidad de un entorno de trabajo en el se puede afirmar que las interacciones propiamente humanas no existen (no hay encuentro físico ni conversación), creemos que queda anulado cualquier tipo de proceso de socialización que condicione la observación.

WikiLeaks responde a la descripción de organización virtual de Walker (2006), la cual articula un entorno de realidad virtual en red construido con fines de interacción, aunque en nuestro caso podríamos hablar de una interacción operativa, buscando la máxima eficacia productiva y efectividad emisora. Y en la que se dan características propias de lo que Hirschhorn y Gilmore (1992) denominan "organización sin límites", caracterizada por su flexibilidad y por liberarse de los tradicionales límites jerárquicos, funcionales y geográficos, articulando una estructura en red (Drucker, 1988; Byrne, 1993).

El modelo WikiLeaks adopta y vigoriza la idea de una "redacción extensa" (Pastor, 2010) y las propuestas de un periodismo en red que combina el periodismo tradicional y las nuevas tecnologías, que es participativo durante el proceso de producción y difusión, abriéndose a periodistas, activistas, académicos y ciudadanos de todo el mundo, y que se centra más en el proceso informativo que en el producto final (Jarvis, 2006; Beckett y Mansell, 2008).

Un problema que observan Reich y Barnoy (2020) es que "los procesos de elaboración de noticias se están volviendo menos observables" por el colapso de las salas de redacción, el número limitado de historias informadas desde el lugar físico donde se producen los hechos, la desmaterialización de la información y su fragmentación en un número creciente de plataformas operadas dentro y fuera de las redacciones, y por la naturaleza cada vez más iterativa de los procesos de noticias. "La observabilidad es aún más restringida cuando las historias involucran temas delicados, fuentes anónimas" (Reich y Barnoy, 2020:969). En el caso de WikiLeaks, los límites a la observación se acrecientan por su naturaleza ciberespacial, nómada y confidencial, y por el uso de tecnología de cifrado digital y su modelo de invitaciones exclusivas. Consideramos que aquí reside la relevancia de este estudio, al describir, desde dentro, el proceso de entrada y participación en una red de filtraciones periodísticas exclusivas de impacto global y acceso restringido como WikiLeaks.

Coincidimos además con Reich y Barnoy (2020: 969) en que son los propios periodistas lo que pueden disfrutar de una "perspectiva más panóptica" sobre los procesos de producción de noticias –incluida la intervención tecnológica–, de ahí la importancia del desdoble de roles como investigador (académico) e informador (periodista) en esta investigación, pudiendo explorar sistemáticamente, participar activamente, testar y comprender el proceso completo.

Los estudios de *newsmaking* se remontan a la década de 1970, cuando se empieza a ver la noticia como resultado de un proceso complejo donde intervienen múltiples factores y donde prevalece un enfoque sistemático de corte cualitativo con la aplicación de técnicas etnográficas, de observación participante en los propios medios y de entrevistas en profundidad (Retegui, 2017). Pero la aparición de Internet, el desarrollo de comunidades virtuales y la expansión del uso de alta tecnología diseñada para garantizar la seguridad de nuestras comunicaciones en línea obligan a pensar nuevas vías de aproximación a las rutinas y procesos de construcción de la noticia, para lo cual creemos necesaria una nueva base epistemológica acorde con la nueva realidad, construida a partir de la descripción de esas rutinas y procesos –mediados y prácticamente monopolizados por la tecnología–, como pretende este estudio. El caso WikiLeaks es un buen ejemplo de que "cuanto más fragmentado y virtualizado se vuelve el entorno periodístico, que involucra una gama cada vez mayor de agentes humanos y tecnológicos, más necesitamos métodos que puedan rastrear a estos contribuyentes diversificados hasta las noticias publicadas" (Reich y Barnoy, 2020: 977).

Desde el enfoque del *newsmaking*, proponemos esta adaptación de la observación participante, asumiendo el rol de reportero, como el mejor método para describir las rutinas productivas operantes en el flujo de esta organización.

Los procesos de producción de la noticia en una red de filtraciones masivas como la estudiada obligan a repensar la teoría del *newsmaking*, para adaptarla a una nueva tipología de organización informativa transnacional, en red, ciberespacial y colaborativa que "desafía los paradigmas convencionales de la cobertura de noticias" (Wahl-Jorgensen, 2014) y el modelo tradicional de organización informativa (Hood, 2011; Braman, 2014; Jurgenson y Rey, 2014), y que se en-

frenta al discurso dominante mediante contranarrativas alternativas (Uricchio, 2014: 2568) que surgen, precisamente, de su modelo de producción de noticias.

Como conclusiones, a partir de nuestra experiencia en las filtraciones de los correos electrónicos de Stratfor, comprobamos la gran dificultad, la complejidad y el enorme trabajo y dedicación que implica tratar alijos de información confidencial tan grandes como los que provee WikiLeaks. Y constatamos la necesidad que tiene esta organización de ampliar su red de colaboradores para dar salida a toda la información que guarda y conseguir, así, la mayor cobertura y difusión posibles.

Concluimos también que WikiLeaks permite a los periodistas trabajar con plena autonomía, sin injerencias de ningún tipo ni condiciones que comprometan su libertad e independencia en todo el proceso periodístico, desde la selección de los temas noticiables y de los materiales, hasta la publicación y difusión de la noticia, pasando por el tratamiento y edición de la información y su contextualización. El único control, mínimo, que impone WikiLeaks se aplica sobre la publicación de la información, que debe ser coordinada entre ambas partes para operar con la máxima eficacia y eficiencia en el proceso de difusión. Así, el investigador debe incorporar previamente una referencia y enlace a su publicación en los registros de WikiLeaks para dar contexto y explicación al material en bruto, que se libera en el sitio web de esta organización al mismo tiempo que el investigador hace público su trabajo, de manera que la información editada y los documentos en bruto se publican y se difunden por distintos canales simultáneamente.

Estamos, por lo tanto, ante un modelo de publicación híbrido en el que la información en bruto y la información procesada y editada periodísticamente se publican de manera sincronizada y enlazada para que cualquier individuo tenga acceso a una versión comprensible de los contenidos de los documentos filtrados y a la vez pueda cotejar la información en bruto y editada, además de poder usar libremente los documentos originales una vez liberados.

Esta aportación complementa la propuesta de Chadwick (2013) sobre el sistema de medios híbridos y, particularmente, sobre WikiLeaks como ejemplo, al describirse en este estudio cómo se ejecuta la hibridación entre el material editado y en bruto, esto es, entre el modelo de periodismo tradicional y el nuevo estándar propuesto por Assange de "periodismo científico" (Khatchadourian, 2010), que copia el modelo de publicación de la literatura científica para que cualquier pieza periodística pueda ser verificable, sometida a las reglas del método científico: falsabilidad, reproducibilidad y repetibilidad.

De la experiencia adquirida valoramos que WikiLeaks diese ese primer acceso a toda una variedad de periodistas, académicos y activistas, asegurando así una mayor libertad y pluralidad en el tratamiento de la información, frente a la exclusividad otorgada en las filtraciones de 2010 a un grupo reducido de la elite mediática. Particularmente, resaltamos la apertura a la participación de medios alternativos y regionales, y con lenguas no dominantes, incluyéndolos en la narración de las mayores filtraciones de la historia hasta aquel momento, considerando que queda patente –tras nuestra experiencia en estas filtraciones–

la importancia que fenómenos globales y la liberación masiva de información y de datos, en una sociedad estructurada en red, tienen para comunidades locales o regionales y sus medios de comunicación. Creemos que este estudio aporta evidencias sobre el potencial del periodismo en red para vigorizar el periodismo que se enfoca a las historias locales, como defienden Beckett y Mansell (2008).

Con este trabajo pretendemos arrojar luz sobre la observación participante en los espacios *cíber* donde se desenvuelven y colaboran comunidades virtuales, particularmente fuera de los circuitos masivos y comerciales; aportar claves para un enfoque del *newsmaking* centrado en las relaciones entre actores humanos y tecnológicos y en las nuevas prácticas colaborativas en red para la producción de noticias, en un sistema de medios híbridos y sociotécnico, y en particular, esclarecer el *modus operandi* de WikiLeaks, organización que, como señala Chadwick (2013: 109), es una "amenaza para el periodismo de investigación tradicional porque, de alguna manera, ofrece un modelo más eficaz".

6. REFERENCIAS

ABDELNOUR, J. (1998): "Virtual environments as spaces of symbolic construction and cultural identity", en Cultural attitudes towards technology and communication, Sydney, University of Sydney, pp. 149-151.

ARQUILLA, J.; & RONFELDT, D. (1993): "Cyberwar Is Coming!", en In Athena's Camp: Preparing for Conflict in the Information Age, Santa Monica, California, RAND Corporation, pp. 23-60.

ARQUILLA, J.; & RONFELDT, D. (1999): The Emergence of Noopolitik: Toward an American Information Strategy, Santa Monica, California, RAND Corporation.

ARQUILLA, J.; & RONFELDT, D. (2001): Networks and netwars: The Future of Terror, Crime and Militancy, Santa Monica, California, RAND Corporation.

ASSANGE, J. *et al.* (2012): Cypherpunks: Freedom and the Future of the Internet, New York – London, OR Books.

BALL, J. (2012, 27 de febrero): WikiLeaks publishes Stratfor emails linked to Anonymous attack, disponible en http://www.theguardian.com/media/2012/feb/27/wikileaks-publishes-stratfor-emails-anonymous [consulta: 4 de julio de 2019].

BECKER, H.S., & GEER, B. (1958): "Participant observation and interviewing: a rejoinder", Human Organization, vol. 17, nº 2, pp. 39-40.

BECKETT, C., & MANSELL, R. (2008): "Crossing boundaries: New media and networked journalism", Communication, Culture and Critique, 1, 92-104.

BENFORD, S., BOWERS, J., FAHLEN, L., GREENHALGH, C., & SNOWDON, D. (1995): "User embodiment in collaborative virtual environments", ACM Conference on Human Factors in Systems (CHI'95), Denver, Colorado, USA.

BENFORD, S., GREENHALGH, C., RODDEN, T., & PYCOCK, J. (2001): "Collaborative virtual environments", Communications of the ACM, Vol. 44, Nº 7, pp. 79-86.

BRAMAN, S. (2014). "«We Are Bradley Manning»: Information Policy, the Legal Subject, and the WikiLeaks Complex", International Journal of Communication, 8, pp. 2603-2618.

BYRNE, J. A. (1993): "The Virtual Corporation", Business Week, 8 de febrero, pp. 37-41.
CASTELLS, M. (1997): La era de la información: economía, sociedad y cultura. Vol. 1. La sociedad red, Madrid, Alianza Editorial.
CHADWICK, A. (2013): The hybrid media system: Politics and power, New York, Oxford University Press.
COLEMAN, G. (2014): Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous, London - New York, Verso.
DE MAEYER, J., & DELVA, J. (2020): "When Computers were New: Shifts in the Journalistic Sensorium (1960s-1990s)", Digital Journalism, pp. 1-18.
DRUCKER, P. (1988): "The coming of the new organization", Harvard Business Review, vol. 66, nº 1, pp. 45-53.
ELÍAS, C. (2003): "Adaptación de la metodología de observación participante al estudio de los gabinetes de prensa como fuentes periodísticas", Empiria - Revista de Metodología de Ciencias Sociales, nº 6, pp. 145-159.
GÓMEZ CRUZ, E. (2002): "Espacio, ciberespacio e hiperespacio: nuevas configuraciones para leer la comunicación mediada por computadora", Anuario de Investigación de la Comunicación CONEICC IX, México, pp. 272-285.
HEINRICH, A. (2011): Network journalism: Journalistic practice in interactive spheres (Vol. 3), New York - London, Routledge.
HIMANEN, P. (2001): The Hacker Ethic and the Spirit of Information Age, New York, Random House.
HIRSCHHORN, L., & GILMORE, T. (1992): "The new boundaries of the 'boundaryless' company", Harvard Business Review, vol. 70, nº 3, pp. 104-115.
HOOD, C. (2011): "From FOI World to WikiLeaks World: A New Chapter in the Transparency Story?", Governance, vol. 24, nº. 4, pp. 635-638.
IANNELLI, L., & SPLENDORE, S. (2017): "Participation in the Hybrid Political Newsmaking and Its Consequences on Journalism Epistemology", Comunicazioni Sociali, 3, pp. 436-447.
IHAMÄKI, P. (2014): "User experiences in the Official WikiLeaks Forum", International Journal of Information and Communication Technology, vol. 6, nº. 3/4, pp. 381-402.
JARVIS, J. (2006, 5 de julio): Networked journalism, disponible en http://buzzmachine.com/2006/07/05/networked-journalism [consulta: 18 de abril de 2021].
JURGENSON, N., & REY, P.J. (2014): "Liquid Information Leaks", International Journal of Communication, 8, pp. 2651-2665.
KHATCHADOURIAN, R. (2010, 7 de junio): No secrets: Julian Assange's mission for total transparency, disponible en https://www.newyorker.com/magazine/2010/06/07/no-secrets [consulta: 18 de abril de 2021].
KERR, E., & HILTZ, S.R. (1982): Computer-mediated communication systems: Status and evaluation, New York, Academic Press.
KOH, J., & KIM, Y-G. (2004): "Knowledge sharing in virtual communities: an e-business perspective", Expert Systems with Applications, vol. 26, nº 2, pp. 155-166.
MCCALL, G.J., & SIMMONS, J.L. (1969): Issues in Participant Observation: A Text Reader, Reading (Massachussetts), Addison-Wesley.
MORAN, R.E. (2020): "Subscribing to Transparency: Trust-Building within Virtual Newsrooms on Slack", Journalism Practice, pp. 1-17.

MITRA, A., & SCHWARTZ, R.L. (2001): "From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces", Journal of Computer-Mediated Communication, 7, 0-0.

NØRSKOV, S., & RASK, M. (2011): "Observation of Online Communities: A Discussion of Online and Offline Observer Roles in Studying Development, Cooperation and Coordination in an Open Source Software Environment", Forum Qualitative Sozialforschung, vol. 12, nº 3, art. 5.

PACCAGNELLA, L. (1997): "Getting the Seats of Your Pants Dirty: Strategies for Ethnographic Research on Virtual Communities", Journal of Computer-Mediated Communication, 3, 0-0.

PASTOR, Ll. (2010): Periodismo zombi en la era de las audiencias participativas. La gestión periodística del público (II), Barcelona, Editorial UOC.

PREECE, J. (2000): Online Communities: Designing Usability, Supporting Sociability, New York, Wiley.

QUIAN, A. (2013a): Impacto mediático y político de WikiLeaks, Barcelona, Editorial UOC.

QUIAN, A. (2013b): "Supermercados de la información en la era de la transrealidad", Versión Estudios de Comunicación y Política - Nueva Época, 31, pp. 51-65.

QUIAN, A., & ELÍAS, C. (2018): "Estrategias y razones del impacto de WikiLeaks en la opinión pública mundial", Revista Española de Investigaciones Sociológicas, 162, pp. 91-110.

REICH, Z., & BARNOY, A. (2020): "How News Become 'News' in Increasingly Complex Ecosystems: Summarizing Almost Two Decades of Newsmaking Reconstructions", Journalism Studies, 21:7, pp. 966-983.

RETEGUI, L. (2017). "La construcción de la noticia desde el lugar del emisor: una revisión del newsmaking", Revista Mexicana de Opinión Pública, vol. 23, pp. 103-121.

RHEINGOLD, H. (1993): "The Virtual Community: Finding Connection in a Computerized World", Chicago, IL, Addison-Wesley Longman Publishing Co., Inc.

SAADO, K., & HUSSEIN, A. (2020). "From laboratory life to newsroom practice: The use of actor-network theory and community of practice to explain newsroom practice and culture: Kurdish Network News as case study", Journal of University of Raparin, 7(2), pp. 686-705.

SCHLESINGER, P. (1981): "Between Sociology and Journalism", The Sociological Review, 29, pp. 341-369.

STERLING, B. (1992): "The Hacker Crackdown: Law and Disorder on the Electronic Frontier". New York: Bantam Books.

TÚÑEZ-LÓPEZ, J. M., TOURAL-BRAN C., & FRAZÃO-NOGUEIRA A. G. (2020): "From Data Journalism to Robotic Journalism: The Automation of News Processing", en Journalistic Metamorphosis: Media Transformation in the Digital Age, Cham, Springer, pp. 17-28

URICCHIO, W. (2014): "True Confessions: WikiLeaks, Contested Truths, and Narrative Containment", International Journal of Communication, 8, pp. 2567-2573.

WAHL-JORGENSEN, K. (2014): "Is WikiLeaks Challenging the Paradigm of Journalism? Boundary Work and Beyond", International Journal of Communication, 8, pp. 2581-2592.

WALKER, H. (2006): "The virtual organisation: A new organisational form?", International Journal of Networking and Virtual Organisations, vol. 3, nº 1, pp. 25-41.

WELLMAN, B., & GULIA, M. (1999): "Virtual communities as communities: net surfers don't ride alone", en Communities in Cyberspace, London, Routledge, pp.167-194.
WOLF, M. (1987): La investigación en la comunicación de masas: críticas y perspectivas, Barcelona, Paidós, 1996.
WRAY, S. (1998): "Electronic civil disobedience and the world wide web of hacktivism: a mapping of extraparliamentarian direct action net politics", Switch, vol. 4, nº 2.
WRAY, S. (1999): "On Electronic Civil Disobedience", *Peace Review*, vol. 11, nº 1, pp. 107-111.

ANEXO: INVITACIÓN PARA INVESTIGAR LOS 'SYRIA FILES'.

Exclusive WikiLeaks Invite for the Syria Files

signup@wikileaks.org 12 de septiembre de 2012, 21:11
<signup@wikileaks.org>
Para: albertoquian@gmail.com

You have been confidentially invited to join the WikiLeaks investigative group for the Syria Files – more than two million emails from Syrian political figures, ministries and associated companies, dating from August 2006 to March 2012. This extraordinary data set derives from 680 Syria-related entities or domain names, including those of the Ministries of Presidential Affairs, Foreign Affairs, Finance, Information, Transport and Culture. The Syria Files shine a light on the inner workings of the Syrian government and economy, but they also reveal how the West and Western companies say one thing and do another. The range of information extends from the intimate correspondence of the most senior Baath party figures to records of financial transfers sent from Syrian ministries to other nations. Being part of this international team will put you in the privileged position of being able to search the emails using the sophisticated WikiLeaks search engine which will enable you to research and publish articles and papers using this data.

We have created a unique invitation system that allows selected journalists, University Professors and employees of human rights organisations to join this project. The system allows the selected invitees, such as yourself, to agree to our Terms and Conditions and gain immediate access to the files for research and publishing purposes, and to invite others worthy of inclusion.

To join this project go to the following URL:

http://wikileaks.org/SyriaFiles-Signup-Instructions.html

Here you will be given full instructions on the simple steps to join this project. Follow the instructions to reach the Terms and Conditions page where you will be asked to enter your invite code. Your unique invite code is:

[redacted]

If you have any problems or questions about this process please email signup@wikileaks.org (we will only be able to answer questions about the Syria Files invite process on this email). Please put Syria Files as the subject line of your email.

Regards,

The WikiLeaks Team