HERRAMIENTAS DE APOYO A LA INFRAESTRUCTURA TECNOLÓGICA DE LOS GRUPOS ORGANIZADOS QUE OPERAN EN LA RED

FÉLIX BREZO Y YAIZA RUBIO

RESUMEN

Las soluciones tecnológicas disponibles en la red son utilizadas con éxito por grupos organizados para satisfacer sus estrategias de comunicación. Sin embargo, las necesidades de cada grupo y el contexto en el que operan son los que marcan los requisitos técnicos de estas aplicaciones. En algunos casos, las alternativas comerciales no son opciones válidas para estos grupos debido a la preocupación por los programas de vigilancia gubernamentales y a la presión que se pueda ejercer sobre las grandes corporaciones para lograr acceso a la información de sus usuarios. En este contexto, la elección de herramientas libres permite a las organizaciones un mayor control sobre su información con una capa adicional de anonimato a un coste razonable. En este artículo se identifican las aplicaciones utilizadas por diferentes grupos organizados para satisfacer sus necesidades de difusión de información, comunicación interna y financiación a través de la red.

Palabras clave: internet profundo, tor, internet de superficie, dinero electrónico.

ABSTRACT

Organized groups successfully use technological solutions available in the network in order to meet their communication strategies. However, each group's needs and the context in which they operate are the factors that determine the technical requirements of these applications. In some cases, commercial alternatives are not a valid option for these groups because of concerns regarding government surveillance programs and the pressure that may be exercised on major corporations to access information on their users. In this context, choosing free software tools enables organisations to have a major control over their information with a larger level of anonymity at a reasonable price. In this article we identify the applications used by different organized groups in order to meet their information dissemination, internal communication, and funding through the network.

Key words: dark internet, surface, deep web, tor, electronic money.

1. INTRODUCCIÓN

La utilización de las nuevas tecnologías no ha pasado desapercibida para los grupos organizados que encuentran en ellas herramientas que mejoran sus procesos de funcionamiento interno. Sin embargo, la preocupación por los programas de vigilancia en internet y por la presión que puedan ejercer los gobiernos sobre plataformas como Facebook y Google para que compartan información sobre sus usuarios ha reforzado

el interés de algunos grupos por proteger su anonimato. Algunos de ellos ya han desplegado infraestructuras tecnológicas que les permiten proteger la integridad de sus comunicaciones.

El objetivo de este artículo es identificar las herramientas utilizadas por diferentes grupos organizados en función de su actividad, desde la difusión de sus acciones y la captación de nuevos miembros, hasta los mecanismos de comunicación interna y las alternativas de financiación que ofrecen estas tecnologías.

En consecuencia, este documento está estructurado como sigue: la sección 2 recoge definiciones y conceptos generales. La sección 3 analiza la disposición de herramientas empleadas para dar soporte a las actividades de distintos grupos y organizaciones que operan en la red. Por último, en la sección 4 se recogen las conclusiones a extraer de este trabajo.

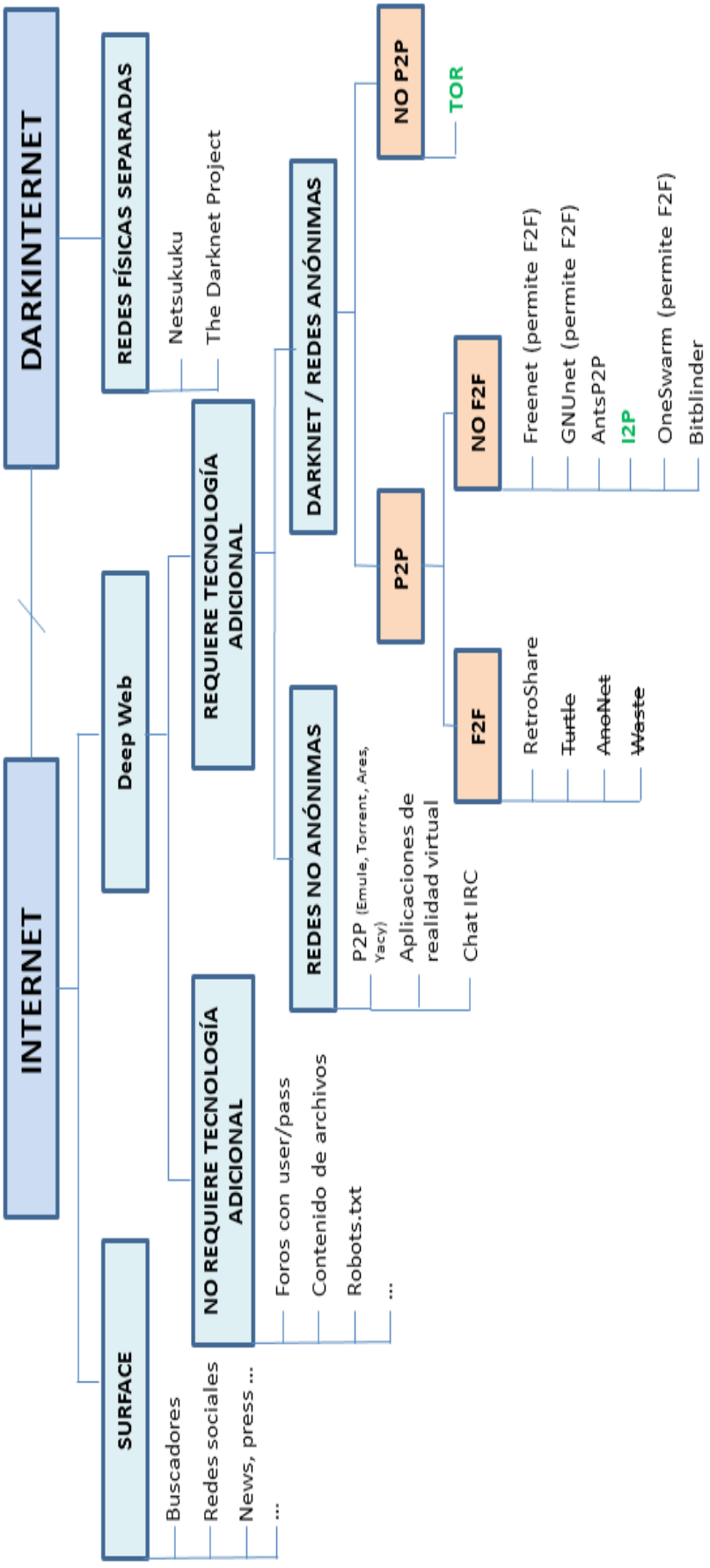
2. CONCEPTOS GENERALES

Las características propias de una investigación en el ámbito de internet y las comunicaciones obligan a la definición de los elementos que componen su arquitectura para afrontar con garantías el proceso de investigación. A continuación, se enumeran una serie de conceptos generales que, aplicados a las redes de ordenadores y a la evolución observada más recientemente de los mecanismos de financiación que proliferan en la red, servirán para comprender los casos de estudio recogidos en este documento.

2.1. CONCEPTOS GENERALES APLICADOS A REDES DE COMUNICACIÓN

En este apartado se va a proceder a detallar parte de la terminología relativa a la estructura de los contenidos de la red en función de la forma en que estos pueden ser consultados. En la Figura 1 se recoge la clasificación propuesta por los autores atendiendo a la naturaleza de las conexiones. En general, se puede hablar de la existencia de dos grandes familias:

- **Internet**. Es un conjunto de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, lo cual hace que las redes físicas heterogéneas que la componen funcionen como una red única.
- **Dark internet**. Se consideran dentro de esta categoría todas aquellas redes físicas separadas de internet que hacen uso de infraestructuras físicas al margen del internet convencional. Actualmente, este tipo de redes son utilizadas por distintos tipos de organizaciones para evitar el control gubernamental, como ocurre con la red Guifi (1), proyectos patrocinados por el Departamento de Estado de los EEUU (2) como Commotion Wireless (3) del Open Technology Institute o aplicaciones de comunicación que utilizan el *wireless* de los dispositivos móviles como Firechat (4). Tienen la particularidad de que su estudio requiere acceso físico a dichas redes, lo que dificulta su monitorización si estas están muy localizadas o son administradas por grupos muy reducidos de personas.


INTERNET
SURFACE
Buscadores
Redes sociales
News, press ...
...
Deep Web
NO REQUIERE TECNOLOGÍA ADICIONAL
Foros con user/pass
Contenido de archivos
Robots.txt
...
REQUIERE TECNOLOGÍA ADICIONAL
REDES NO ANÓNIMAS
P2P (Emule, Torrent, Ares, Yacy)
Aplicaciones de realidad virtual
Chat IRC
DARKNET / REDES ANÓNIMAS
P2P
F2F
RetroShare
Turtle
AneNet
Waste
NO F2F
Freenet (permite F2F)
GNUnet (permite F2F)
AntsP2P
I2P
OneSwarm (permite F2F)
Bitblinder
NO P2P
TOR
DARKINTERNET
REDES FÍSICAS SEPARADAS
Netsukuku
The Darknet Project

En cualquier caso, en este trabajo se va a hacer referencia a diversas fuentes de internet. Es habitual diferenciar entre internet de superficie (o *surface*) e internet profunda (o *deep*).

- ***Surface.*** Se considera *surface* a aquel contenido indexado por los buscadores convencionales, por lo que se encuentran en esta categoría las redes sociales (exceptuando los perfiles privados), los foros (exceptuando aquellas partes que establezcan mecanismos de protección como usuario y contraseña) y las plataformas de *pastes* (exceptuando aquellos que se hayan borrado previamente a la indexación por parte de los buscadores)[1].

- ***Deep.*** Es aquel contenido al que no se puede acceder a través de un buscador convencional. La ausencia de contenidos indexados en dichos buscadores puede venir motivada por la necesidad de autenticar el acceso mediante un usuario y contraseña o por el uso de una tecnología adicional entre otras razones. En esta última categoría se encuentran las redes no anónimas y las redes anónimas.

Las redes anónimas se utilizan para compartir información y contenidos digitales entre distintos nodos. En ellas se toman medidas para preservar el anonimato de las identidades de quienes intercambian información. Este tipo de redes pueden dividirse en redes P2P, aquellas en las que las relaciones entre todos sus miembros son de igual a igual, y no P2P.

El caso de Tor (5) es el de una red de comunicaciones distribuida de baja latencia y superpuesta sobre internet en la que el encaminamiento de los mensajes que viajan por ella está concebido para proteger la identidad de los usuarios, la integridad de la información y la confidencialidad de la misma. En la red Tor se cifra la información en los nodos de entrada y se descifra en los nodos de salida, momento en el que un atacante podría acceder a la información que circula por ellos si no se emplea un protocolo de cifrado a nivel de aplicación como SSL.

Por su parte, las redes P2P se pueden dividir en *friend-to-friend* (F2F), aquellas redes P2P anónimas en donde los nodos tienen la capacidad de conectarse únicamente con nodos *amigos* conocidos, limitando la exposición de los mismos, y redes no *friend-to-friend* (no F2F). Las primeras presentan grandes inconvenientes para su monitorización, dada la necesidad de que ambos nodos consensuen la comunicación. A continuación se enumeran algunos ejemplos existentes de este tipo de redes.

- **Retroshare** (6). Por su arquitectura, es una red P2P que únicamente funciona como F2F. Se trata de un tipo de red en el que la gente se conecta directamente con sus amigos, por lo que se necesitarían otro tipo de capacidades no técnicas para tener acceso al contenido.

- **I2P** (Invisible Internet Project) (7). Es una red de capa anónima pensada para el envío de mensajes punto a punto preservando el anonimato. Está concebida para alojar cualquier servicio de internet tradicional como servidores de correo, canales de chat IRC, servidores HTTP, así como otras aplicaciones distribuidas. Sin embargo, a diferencia de Tor, no está concebida para acceder a la *surface* de forma anónima.

1 Las excepciones señaladas se encuentran dentro de la categoría de deep web como contenido que no requiere una tecnología adicional para acceder.

- **Freenet**. Es una red P2P destinada a la distribución de información anónimamente entre los usuarios que la conforman (8) y que ponen a disposición de la red parte de su ancho de banda y de su capacidad de almacenamiento. Tiene la característica de que se puede configurar para funcionar como una red F2F.

Además, existen otras tecnologías que ofrecen diferentes soluciones de conectividad como las plataformas de compartición de archivos GNUnet (9), OneSwarm (10), Bitblinder (11) y AntsP2P (12) o los proyectos ya descontinuados Turtle, Anonet (13) y Waste (14).

2.2. CONCEPTOS GENERALES DE LA ECONOMÍA EN LA RED

El dinero convencional y los métodos de pago han encontrado diferentes formas de evolucionar y adaptarse a las nuevas tecnologías. El efectivo ha dado paso al dinero electrónico y este a la aparición de métodos de pago alternativos cuyo control escapa a organismos centralizados. En este sentido, tomaremos como referencia la definición de dinero electrónico procedente de la Directiva 2009/110/CE (15) sobre el acceso a la actividad de las entidades de dinero electrónico cuyo proceso de trasposición en España se culminó con la Ley 21/2011 sobre dinero electrónico (16):

- **Dinero electrónico.** «Todo valor monetario almacenado por medios electrónicos o magnéticos que representa un crédito sobre el emisor, se emite al recibo de fondos con el propósito de efectuar operaciones de pago, según se definen en el artículo 4, punto 5, de la Directiva 2007/64/CE, y que es aceptado por una persona física o jurídica distinta del emisor de dinero electrónico».

Otro punto de vista es el sostenido por un informe del Departamento del Tesoro de los EEUU enfocado al análisis de las monedas virtuales convertibles (17), es decir, aquellas que tienen un valor equivalente en divisas virtuales. Los conceptos de divisa convencional y divisa virtual son definidos como sigue:

- **Divisa convencional**. «La moneda o papel moneda de los EEUU o de cualquier otro país que ha sido designada como de curso legal y que circula y es utilizada y aceptada como medio de intercambio en el país emisor».
- **Divisa virtual**. «La divisa utilizada como medio de intercambio que funciona como tal en determinados entornos, pero que no posee todos los atributos de las monedas convencionales. En particular, las divisas virtuales no tienen estatus de curso legal en ninguna jurisdicción».

En base a estas definiciones y a la tipología de las entidades de gestión de las divisas virtuales, estas se pueden clasificar de dos formas:

- **Centralizadas**. Se entiende por divisas centralizadas todas aquellas cuya gestión corre a cargo de un organismo central, que las expide y se hace responsable de ellas. Ejemplos de este tipo de plataformas son Paypal (18), Skrill (19), Webmoney (20), CashU o Ven (21). En otro ámbito, existen plataformas virtuales que también permiten la compraventa de bienes digitales dentro de las distintas comunidades virtuales que las utilizan, como los Linden Dollars de Second Life (22) o las divisas utilizadas en plataformas de compraventa de

exploits[2] y servicios de *hacking* y *cracking* como 1337day.com[3] (23). Estas divisas no necesariamente han sido concebidas originalmente para el comercio electrónico pero sí entran en la definición de *convertibles* del Financial Crimes Enforcement Network (17) que recogíamos en la definición de divisas virtuales.

- **P2P**. A semejanza del funcionamiento de las redes P2P en otros ámbitos, esta arquitectura también funciona para la gestión de los pagos realizados con *criptodivisas* de forma que son los nodos de la red los que mantienen la integridad de las transacciones de la moneda. La *criptodivisa* más utilizada es Bitcoin, que acapara el 84% de la capitalización total del mercado (24). Se trata de un protocolo público que implementa una divisa virtual basada en una arquitectura *peer-to-peer* (P2P) en la que no existen servidores centrales (25). Su mantenimiento recae en la capacidad computacional de la red de usuarios en sí misma aplicando un modelo de *proof-of-work*[4] para la validación de las monedas. El hecho de que se trate de un proyecto de *software* libre ha permitido la proliferación de monedas derivadas como Litecoin, Peercoin y Namecoin. Pese a la hegemonía de las *criptodivisas* basadas en Bitcoin, Ripple, Nxt y BitSharesX son ejemplo que, aun no compartiendo el código fuente, heredan su filosofía.

3. HERRAMIENTAS UTILIZADAS POR LOS GRUPOS ORGANIZADOS EN LA RED

Los grupos organizados se sirven de soluciones existentes en la red para mejorar la efectividad de sus campañas de difusión, agilizar los procesos de toma de decisiones mejorando sus estructuras de comunicación interna y explotar nuevas vías de financiación al margen de los sistemas convencionales. En consecuencia, en esta sección se recogen las opciones que tienen a su alcance cuatro tipos de entidades de diferente naturaleza que comparten la utilización de la red para como instrumento organizativo.

3.1. ORGANIZACIONES ACTIVISTAS Y MOVIMIENTOS SOCIALES

Tanto las organizaciones internacionales como los movimientos sociales que defienden causas sectoriales hacen uso de las nuevas tecnologías para multiplicar su capacidad de convocatoria, aumentar la presión sobre los organismos e instituciones con poder de decisión o eludir las limitaciones interpuestas por los gobiernos para materializar sus objetivos.

2 Un exploit es un fragmento de software utilizado con el objetivo de explotar una vulnerabilidad de seguridad dentro de un sistema informático para conseguir que este se comporte de una forma en la que no fue concebido siendo explotado por el atacante.

3 En 1337day.com, la moneda de intercambio es el Gold (1 Gold = 1USD al cambio) y permiten el depósito y el retiro empleando criptodivisas o Webmoney entre otros. Cuenta con un modelo de negocio que acapara un 20% de comisión en las retiradas de dinero.

4 Estos sistemas se caracterizan por hacer que los nodos de una red resuelvan una serie de operaciones matemáticas (a menudo hashes) antes de poder ejecutar una acción sobre la misma (en el caso de Bitcoin, añadir un nuevo bloque) de modo que se previenen ataques de denegación de servicio o abusos contra ella dado que se puede ir ajustando la dificultad de los problemas matemáticos solicitados. En el caso de Bitcoin, estos modelos hacen que la posibilidad de recibir la autorización de la red para añadir un nuevo bloque sea directamente proporcional al porcentaje de la capacidad de cómputo total que representa un nodo con respecto al resto de la red.

3.1.1. Mecanismos de difusión

Una parte importante de las acciones activistas es la promoción de sus actividades para la difusión del mensaje. Una de las estrategias de comunicación consiste en aparecer en los medios de comunicación convencionales con protestas mediáticas como las llevadas a cabo por colectivos como Femen (26) (27) (28) o Greenpeace (29). Antes de la democratización del uso de internet, estas prácticas constituían el eje central de sus campañas para alcanzar a un público más amplio.

Hoy en día, estos grupos también encuentran en la red un medio propicio para la difusión de sus acciones y motivaciones, así como para la publicación de decálogos que ya venían siendo difundidos en el pasado mediante cadenas de correo o sitios Web 1.0. En este sentido, las redes sociales y las plataformas de recogidas de firmas se conforman como medios de difusión que permiten poner a disposición de cualquiera vídeos y materiales de manera inmediata e independiente a grupos de presión y con mayor capacidad de viralización para la identificación de perfiles afines.

3.1.2. Mecanismos de comunicación interna

Históricamente, las salas de chat IRC y las listas de correo han sido utilizadas como mecanismos de comunicación interna. De hecho, la plataforma activista Riseup todavía mantiene una colección de listas de correo en la que se alojan más de 17 000 agrupadas por temáticas (30). Sin embargo, este tipo de soluciones presentan problemas para clasificar contenidos, realizar el seguimiento de una determinada temática y abrir hilos en paralelo dada la gran cantidad de conversaciones simultáneas existentes.

Actualmente, se utilizan herramientas de edición colaborativa de documentos como Google Docs, cuyo anonimato depende de la confianza depositada en la compañía que ofrece el servicio. Existen alternativas libres como Loomio[5] (31) o Etherpad-lite[6] (32) que permiten su despliegue en servidores privados o, si el objetivo es reforzar el anonimato, en los *hidden services* de Tor o de Freenet. En este sentido, plataformas como Riseup ofrecen a los diferentes grupos activistas la posibilidad de utilizar la solución de Etherpad a través de una versión pública desplegada en sus propios servidores (33).

El uso de herramientas para evadir el control que ejercen sobre internet los gobiernos en los que se limita la libertad de expresión o de reunión es de gran utilidad para los grupos activistas. Existen soluciones que apuestan por evitar la utilización de la infraestructura cableada de los proveedores de servicios de Internet y que se apoyan en arquitecturas físicas creadas *ex professo* por los activistas para mantener la conectividad interna. Por ejemplo, Firechat, que fue utilizada con éxito por los manifestantes en las protestas de Hong Kong de otoño de 2014 (34) (35) (36), explota el concepto de topologías de red en malla o *mesh networks*[7] para crear redes P2P interconectadas

5 Loomio es un proyecto de software libre distribuido bajo licencia AGPL que permite la toma de decisiones, el trabajo colaborativo y la votación de propuestas a través de una interfaz web. El código fuente del proyecto está disponible en Github (83).

6 Etherpad es un proyecto de The Etherpad Foundation que mantiene una solución para la edición de documentos de forma colaborativa y en tiempo real liberada bajo la licencia Apache 2.0. El código fuente del proyecto está disponible en Github (90).

7 Las topologías de red en malla no requieren de un nodo central que las gestione permitiendo que

haciendo uso de la conexión Wifi de los dispositivos y eludir la presión que pudiera aplicarse sobre los proveedores de servicio.

Para agilizar el proceso de toma de decisiones, existen aplicaciones para la administración de los procesos de votación[8]:

- Appgree (37) es una plataforma centrada en la formulación de procesos de votación multipropuesta de forma ágil mediante la creación de tantos subgrupos de población elegidos al azar como propuestas iniciales se hayan planteado en las que cada uno de estos subgrupos será consultado sobre un número limitado de propuestas de forma representativa.
- Agora Voting (38) es un proyecto de Wadobo Labs que presenta una plataforma web distribuida bajo licencia AGPL[9] concebida para la administración de procesos de votación basados en el concepto de democracia líquida, es decir, procesos en los que el participante puede optar por delegar el voto en personas de su confianza.

3.1.3. Mecanismos de financiación

Pese a que tradicionalmente la financiación de las actividades de organizaciones activistas se ha mantenido a costa de las cuotas de sus abonados y suscriptores, la red ofrece hoy en día otras soluciones complementarias:

- Donaciones voluntarias enviadas a través de plataformas como Paypal, Google Wallet o similares.
- Proyectos específicos financiados a través de sitios como Kickstarter (39), Peerbackers (40) y Goteo (41). Se trata de plataformas en las que organizaciones y particulares proponen proyectos que son financiados por la comunidad a cambio de determinados beneficios y que se llevan a cabo cuando una determinada cifra es alcanzada.
- *Merchandising* y venta de productos por internet que incluyan lemas o mensajes asociados al movimiento como camisetas, tazas, llaveros y otros productos similares (42).

En cualquier caso, no es habitual que estas plataformas empleen *banners* de publicidad de productos de terceros para aumentar sus ingresos, ya que predomina el interés por mantener su independencia.

3.2. GRUPOS *HACKTIVISTAS*

La actividad de los grupos *hacktivistas* se ha incrementado en las últimas décadas aprovechando el descontento social para identificarse con otras causas activistas (43).

los mensajes circulen por los nodos que pertenecen a la red y agregando tolerancia a fallos en el caso de que un nodo se desconecte o falle.

8 Organizaciones como la Electronic Frontier Foundation (89) o GNU (87) e incluso activistas del software libre como Richard Stallman (92) ya han manifestado en el pasado dudas en relación a los problemas que entraña para la privacidad de los votantes la utilización de dispositivos electrónicos.

9 El código fuente del proyecto está disponible en Github (95).

Se erigen como defensores de la libertad de expresión y de los derechos humanos y denuncian de la actividad de los gobiernos y corporaciones a partir de la utilización de herramientas digitales para la filtración de documentos, la ejecución de DDoS[10], la ingeniería social[11] o la realización de otros ataques más sofisticados técnicamente como inyecciones SQL[12] o ataques de *cross-site-scripting*[13] entre otros.

3.2.1. Mecanismos de difusión

Los grupos *hacktivistas*, al igual que las organizaciones activistas, tienen su propia estrategia de comunicación, esencialmente a través de internet. Utilizan las redes sociales para difundir tanto sus próximas actuaciones, denominadas *operaciones*, como la información obtenida a partir de sus ataques. Por este motivo, muchos de estos grupos han visto cancelados en algún momento sus perfiles en distintas plataformas, como ocurriera con Anonymous en Facebook (44) o Youtube (45) por publicar información «privada y confidencial de otras personas». Para asegurarse de que dicha información no desaparezca de internet y sea visible desde cualquier buscador, suelen utilizar plataformas con términos y condiciones menos restrictivas en cuanto al tipo de información publicada como Pastebin (46).

Asimismo, es habitual que las identidades que colaboran con estos grupos reivindiquen la atribución de sus actos. Suelen utilizar páginas como Zone-H (47) en las que los atacantes dan a conocer las vulnerabilidades que han descubierto o publicar su logo o lema en aquellos *sites* que han sido objetivo de sus ataques. Sus actividades suelen tener consecuencias legales y, es por ello que en ocasiones utilizan pseudónimos para evitar ser relacionados con otras de sus identidades en la red o, por el contrario, que se refugien bajo otros movimientos *hacktivistas* como los de Anonymous, Lulzsec o Turkish Ajan.

3.2.2. Mecanismos de comunicación interna

La organización de los grupos *hacktivistas* es anárquica y a menudo difusa (48). Se caracterizan por tener una estructura flexible y por funcionar como redes P2P en las que la desaparición de una identidad no implica la pérdida de una funcionalidad estructural significativa. En cualquier caso, no es imprescindible que sus miembros posean altos conocimientos informáticos para colaborar en la ejecución de ataques ya que pueden utilizar programas denominados LOIC[14] (del inglés, Low Orbit Ion Cannon),

10 Un ataque de denegación de servicio distribuido tiene como objetivo la paralización intencional de una red informática inundándolo con datos enviados simultáneamente desde varios ordenadores.

11 La ingeniería social se define como el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros.

12 Una inyección SQL es un método de infiltración de código que se vale de una vulnerabilidad informática presente en el nivel de validación de entradas de una aplicación que realiza consultas a una base de datos.

13 Los ataques de cross-site-scripting o XSS son un tipo de inyección en el que el atacante se sirve de una vulnerabilidad en una aplicación web para enviar código malicioso al usuario final. Como el navegador del usuario no tiene forma de comprobar si es de confianza, ejecutará la secuencia maliciosa de comandos.

14 Low Orbit Ion Cannon (LOIC) es una herramienta de inundación utilizada para generar una gran cantidad de tráfico de red. Esta alta tasa de resultados de tráfico tiene el objetivo de degradar la disponibilidad de una plataforma y, potencialmente, provocar una interrupción del servicio.

diseñados para realizar denegaciones de servicio de forma sencilla y sin necesidad de compartir una localización geográfica.

Las vías de comunicación entre expertos de seguridad informática tienen en común la dificultad del rastreo de sus miembros y de la información que estos publican. Aún hoy en día, uno de los principales mecanismos de comunicación son las listas de distribución a partir del correo electrónico.

Este tipo de listas dieron paso a mecanismos de comunicación más interactivos. Los chats IRC[15] y las zonas privadas de los foros de seguridad son utilizados por los grupos *hacktivistas* para coordinar sus ofensivas contra objetivos planificados. En cambio, los foros habitualmente presentan dos zonas, una pública, que es utilizada a modo de agregador de noticias y consultas técnicas generales, y otra privada para la planificación de operaciones. A menudo, se utilizan medidas de seguridad adicionales para dificultar el acceso a las plataformas por parte de programas de monitorización automatizados. Las más utilizadas son las siguientes:

- Verificación del User-Agent del navegador para evitar el acceso de *crawlers* y recolectores de enlaces o correos.
- Ejecución de javascript que solicita *feedback* al usuario y que complica las tareas de automatización.
- Obligación de contar con una cuenta registrada y la necesidad de contar con permisos de acceso al recurso.
- Resolución de captchas[16] visuales o auditivos, así como de operaciones matemáticas u otras preguntas de verificación que dificultan accesos no deseados a la plataforma.
- Obligación de publicar un comentario para poder acceder a cierta información.

Por otra parte, las redes sociales funcionan de manera similar. Los grupos *hacktivistas* tienen la posibilidad de comunicarse a través de grupos privados con la salvedad de que la administración de la página es ajena a la organización. Esta circunstancia hace que sea susceptible de ser utilizada por las fuerzas de seguridad aprovechando las exigencias que se pueden requerir a los administradores de sitios como *Facebook*.

Con respecto a los correos electrónicos como herramienta de comunicación, se cuenta con la posibilidad de emplear servidores anonimizados a través de la red Tor como Mailtor (49) o el ahora desactivado Tormail (50). También se utilizan técnicas de cifrado PGP (51) en los proveedores de servicio convencionales para evitar que se pudiera acceder al contenido del correo electrónico, en el caso de que la información fuera requerida a los administradores del servicio de correo electrónico por mediación de una autorización judicial. Estas técnicas sólo pueden ser vulneradas cuando se

15 Algunos de los chats IRC más utilizados por grupos como Anonymous son los servidores irc.cyberguerrilla.org, irc.anonops.com, irc.anonibero.com e irc.anonnet.org.

16 Un captcha (del inglés, Completely Automated Public Turing test to tell Computers and Humans Apart) es un test automático controlado por una máquina conformado por una prueba en la que se pretende determinar si un usuario es un humano o un bot. Se utilizan desafíos que supuestamente solo sabrían solventar los usuarios humanos como la lectura de una imagen distorsionada o la respuesta concreta a preguntas complejas o enunciados de problemas sencillos.

carezca tanto de protección física del punto en el que se encuentra la clave privada utilizada como de protección lógica de las claves que dan acceso a ella.

3.3. GRUPOS DEDICADOS A ACTIVIDADES CRIMINALES EN INTERNET

La capa adicional de anonimato que ofrece operar detrás de un ordenador ha dado pie a la proliferación de grupos criminales que operan en la red. La existencia de dichos grupos depende del mantenimiento de un ecosistema que les permita continuar con sus actividades delictivas. Este caso de estudio tiene el objetivo de conocer el modo en el que los grupos dedicados al crimen en la red se organizan de tanto para la venta de contenidos (robo de credenciales o de tarjetas bancarias) o el ofrecimiento de servicios ilegales (alquiler de *botnets*, servicios de *hacking* y *exploits*) como para la compartición o distribución de contenido de pornografía infantil.

3.3.1. Mecanismos de difusión

Estos grupos evitan su exposición en la web de superficie. Suelen utilizar foros[17] con medidas de seguridad basadas en relaciones de confianza o en la publicación de *posts* para acceder a la información robada como mecanismo de prevención frente a *bots*. Asimismo, las salas de chat IRC también permiten poner en contacto a los interesados para concertar el formato de entrega de contenidos. Estos dos tipos de fuentes no garantizan, por definición, la anonimización de los delincuentes a no ser que hagan uso de VPN que protejan su identidad o realicen las conexiones a través de *proxies* alojados en distintos países para conectarse a dichas plataformas y dificultar el rastreo.

En cambio, uno de los grandes desafíos que se plantea a los organismos policiales es el seguimiento de grupos criminales a través de redes anónimas. El grado de anonimato que les otorgan estas redes ha conseguido que los delitos tradicionales del tráfico de drogas, órganos y armas hayan puesto especial interés sobre estos servicios ocultos. En concreto, a partir de Tor, la red anónima por excelencia, podemos encontrar mercados negros como Silk Road (52) (53) o Agora (54), servicios de email como los ya mencionados Tormail (50) o Mailtor (49) e, incluso, distintos tipos de redes sociales en las que poder ponerse en contacto con más usuarios como Torchat (55) y la extinta Torbook (56).

3.3.2. Mecanismos de comunicación interna

Los ciberdelincuentes son conscientes de que uno de los tipos de comunicación existentes en internet y que garantizan una mayor complejidad de rastreo es el proporcionado por aquellas redes P2P anónimas en donde sus nodos se conectan únicamente con sus «amigos». En este punto, se hace inviable una monitorización automatizada del contenido que circula por ellas y, llegado el caso, sería necesario otro tipo de capacidades como la infiltración en dicha red para tener acceso al contenido.

Adicionalmente, un informe del European Cybercrime Centre (57) reconoce que la dificultad de identificar la ubicación del material ilegal, especialmente cuando este es

17 Por ejemplo, los foros de leakforums.org (97) y lampeduza.so (98) están especializados en la venta de credenciales y tarjetas bancarias sustraídas.

borrado tras su visualización, y la de averiguar el momento exacto en el que se está reproduciendo un recurso en *streaming* son los principales retos a los que deben hacer frente los organismos policiales en relación con la detección de delitos asociados a los abusos contra la población infantil en internet.

3.3.3. Mecanismos de financiación

A continuación, se recogen algunas de las principales líneas de acción que pueden ser utilizadas por grupos dedicados al cibercrimen para monetizar sus actividades.

- Administración de *botnets*. Symantec (58) identifica diversas formas de monetizar una *botnet*. Pueden variar desde el ofrecimiento de servicios de denegación de servicio bajo demanda utilizando los nodos infectados, hasta el envío de *spam*, el ofrecimiento de servicios de *proxies* a través de los equipos comprometidos, el *click-frauding*[18], la venta de credenciales o incluso la minería encubierta de bitcoins en dichos equipos.
- Compra de seguidores. El auge de las redes sociales y la importancia de la imagen de marca en la red han motivado que algunas compañías opten por la compra de seguidores para ganar reputación con mayor rapidez, dando pie al desarrollo de un mercado *underground* de venta de seguidores y *likes* (59).
- Contratación de servicios ofensivos. En algunas plataformas como 1337day.com se ofrecen servicios de *hacking* bajo demanda. De hecho, la dirección de Bitcoin asociada a 1337day.com a finales de 2014 había aparecido en casi 150 transacciones habiendo recibido más de 234 bitcoins (60) (65 000 € al cambio[19]).
- *Ransomware*. Se trata de un tipo de aplicación maliciosa que extorsiona a los usuarios mediante el secuestro de documentos (habitualmente ofimáticos) de los equipos infectados cifrando dichos documentos con una clave aleatoria para solicitar posteriormente el pago de un rescate que permita a la víctima recuperar los ficheros. Aunque en el caso de algunas filtraciones de bases de datos corporativas se han solicitado rescates de gran importe (61), es habitual que se apueste por rescates de tamaño medio o bajo, pero siempre en órdenes de magnitud que el usuario infectado esté dispuesto a abonar (62).
- *Phishing*. Utilizando técnicas de ingeniería social, los delincuentes pueden obtener credenciales bancarias y nombres de usuario y contraseñas de acceso a servicios sensibles para venderlos posteriormente.
- Contratación de servicios no autorizados. La proliferación de los *smartphones* da paso a la difusión de aplicaciones que pueden formalizar la contratación de servicios Premium sin conocimiento del usuario.

Además, las características propias de las *criptodivisas* dificultan la atribución de las transacciones y la identificación de los responsables frente a la monitorización de las divisas convencionales. Esta realidad, propicia un escenario en el que la sustracción

18 El click-frauding es un tipo de abuso perpetrado contra las plataformas de anunciantes que se basa en la realización de peticiones automáticas para visualizar anuncios controlados por el atacante generando tráfico artificial no humano.

19 Tasa de cambio estimada por blockchain.info a fecha 11 de diciembre de 2014 (88).

de monederos virtuales acapare un interés creciente para los grupos dedicados al cibercrimen ya que en ellos se almacenan monedas virtuales de más fácil sustracción que el dinero electrónico convencional.

3.4. GRUPOS TERRORISTAS

Las redes terroristas utilizan internet para satisfacer tres objetivos estratégicos de comunicación que, según Corman y Schiefelbein (63), son la legitimización de su causa, la propagación de su movimiento y la intimidación de sus oponentes. Dependiendo del propósito que deseen satisfacer, se situarán en una zona de internet u otra.

3.4.1. Mecanismos de difusión

Grupos terroristas como el Ejército Islámico de Irak y el Levante (ISIS) han desarrollado una sofisticada estrategia a través de redes sociales como medida de promoción de sus acciones ante el mundo. Por medio de estos canales, publican todo hecho en el que se destaque su fuerza militar y sus avances territoriales, llegando a realizar vídeos promocionales como la *Campaña de los mil millones* en la que se instaba la población musulmana a que colgara vídeos en Youtube e Instagram apoyando la causa (64). Con el objetivo de inundar las redes, crearon la aplicación The Dawn of Glad Tidings que publicaba *tweets* automáticamente en las cuentas de aquellos que se la hubieran descargado (65).

En vista de que la estrategia de comunicación de ISIS está siendo muy efectiva de cara al reclutamiento de combatientes extranjeros, el gobierno iraquí bloqueó el 13 de junio de 2014 el acceso a Facebook y a Twitter, lo que motivó la utilización de la aplicación Whisper (66) que permite la publicación de comentarios de forma anónima y que ha cobrado protagonismo en Iraq incluso entre militares desplegados en la zona (67) (68). Asimismo, también se ha incrementado el uso de Tor y de Psiphon que da la posibilidad a los usuarios de utilizar su dispositivo como *proxy* para permitir que terceros puedan acceder a internet a través de ellos (69).

3.4.2. Mecanismos de comunicación interna

Hace tiempo que los grupos terroristas son conscientes de las implicaciones que tendrían para su organización las fugas de información derivadas de la incautación de sus equipos. La banda terrorista ETA ya utilizaba como medida de protección de su información en el año 2003 el sistema de cifrado PGP (70) y en 2010 el proyecto de TrueCrypt[20] (71).

Por su parte, Al-Qaeda utiliza desde 2007 (72) una aplicación de cifrado para Windows denominada Asrar Al-Mujahideen (*secretos muyahidines* en español) que permite el intercambio de mensajes y archivos cifrados ya sea a través de foros o de buzones de correo electrónico. Adaptándose a los nuevos tiempos, en 2013, The Global Islamic Media Front hizo público el desarrollo de una aplicación de cifrado

20 El proyecto de Truecrypt fue descontinuado repentinamente por sus desarrolladores en mayo de 2014 (76) pese a sus funcionalidades multiplataforma y a que la propia comunidad había patrocinado un análisis forense de su código para verificar su robustez (77).

para dispositivos Android y Symbian que permite el cifrado de SMS, archivos y correo electrónico con criptografía asimétrica (73).

En el caso de aquellos grupos con una estructura localizada, las alternativas que crean una infraestructura de red paralela a la infraestructura telefónica convencional aportan una capa adicional de seguridad al resto de elementos de seguridad de la red, dado que las comunicaciones tienen lugar al margen de la red instalada por los proveedores de servicios de comunicaciones. Este es el caso de The Darknet Project, una red que habría permitido a Los Zetas mantener su estructura de comunicación sin depender de la red telefónica convencional (74).

3.4.3. Mecanismos de financiación

Las *criptodivisas* ofrecen nuevas posibilidades de financiación complementarias a los métodos tradicionales. Sin embargo, los grupos terroristas tienen que enfrentarse al insuficiente número de pasarelas de intercambio que permitan la realización de transacciones de dinero en efectivo por bitcoins de una forma anónima. Solamente la proliferación de comercios que acepten esta *criptodivisa* como medio de pago o la utilización de cajeros automáticos que los expendan permitirían superar las barreras de seguridad interpuestas por estas plataformas.

Sin embargo, atendiendo a los datos recogidos en el proyecto de coinmap.org[21] (75), el número de establecimientos físicos que aceptan bitcoins o litecoins como medio de pago apenas supera los 6000 en todo el mundo. La realidad es que la adquisición de grandes cantidades de bitcoins es compleja si no se cuenta con una red de un tamaño suficiente como para asimilar el volumen de transacciones a realizar. En el caso particular de los grupos asociados al Estado Islámico, a las dificultades tecnológicas que conlleva la implantación de estos sistemas en puntos de venta físicos, se suma la inexistencia de comunidades activas en los países limítrofes lo que limita su margen de maniobra en esta región.

4. CONCLUSIONES

Las soluciones tecnológicas disponibles en la red están siendo utilizadas con éxito por grupos organizados para satisfacer sus objetivos de manera más eficiente, pero serán las necesidades concretas de cada grupo las que marquen el tipo de aplicaciones a utilizar. En este sentido, las organizaciones que centran sus esfuerzos en acciones de presión harán uso de la web de superficie (redes sociales, blogs, plataformas de recogida de firmas, etc.) para garantizar la difusión de su mensaje hacia un público más amplio. Por el contrario, aquellos grupos criminales o aquellas organizaciones que lleven a cabo actividades perseguidas por los estados optarán por soluciones que provean una capa de anonimato más robusta (Tor, I2P, Freenet, etc.) para dificultar las labores de investigación de las agencias de seguridad.

De la misma manera, las soluciones comerciales dedicadas a proteger los activos tecnológicos de empresas y organizaciones pueden ser percibidas como una amenaza para aquellos grupos que vean en ellas una puerta a intrusiones de los organismos

21 Su código fuente es distribuido como software libre bajo licencia AGPL (76).

de seguridad. Por ello, estos grupos suelen optar por soluciones de *software* libre y de código abierto que permitan mantener el control teórico sobre los sistemas ejecutados con unos costes de despliegue razonables. De todas formas, la elección de este tipo de soluciones no está exenta de riesgos de seguridad como puso de manifiesto la repentina clausura del proyecto de Truecrypt y los esfuerzos dedicados por su comunidad para auditar su código.

Por último, las *criptodivisas* ofrecen nuevas posibilidades de financiación complementarias a los métodos tradicionales. Las dificultades adicionales que conlleva el rastreo de las transacciones y el acceso a mercados de compraventa presentes en la *deep web* son elementos que podrían incentivar su uso de forma sumergida. Pese a ello, su utilización sistemática dependerá de la capacidad de los mercados para absorber el capital ingresado y de la preocupación de los actores involucrados para preservar su anonimato.

BIBLIOGRAFÍA

1. Lluis Dalmau. ¿Qué es guifi? | guifi.net. [En línea] 20 de marzo de 2009. [Citado el: 13 de diciembre de 2014.] https://guifi.net/es/trespasos.

2. Glanz, James. U.S. Underwrites Internet Detour Around Censors. [En línea] The New York Times, 12 de junio de 2011. [Citado el: 13 de diciembre de 2014.] http://www.nytimes.com/2011/06/12/world/12internet.html?_r=2&.

3. Open Technology Institute. About Commotion | Commotion Wireless. [En línea] 2012. [Citado el: 13 de diciembre de 2014.] https://commotionwireless.net/about/.

4. Open Garden. Open Garden | /firechat. opengarden.com. [En línea] [Citado el: 9 de octubre de 2014.] https://opengarden.com/firechat.

5. Tor Project: Anonymity Online. torproject.org. [En línea] [Citado el: 9 de octubre de 2014.]

6. RetroShare. sourceforge.net. [En línea] [Citado el: 9 de octubre de 2014.] http://retroshare.sourceforge.net/.

7. Red anónima I2P. geti2p.net. [En línea] [Citado el: 9 de octubre de 2014.] https://geti2p.net/es/.

8. The Freenet Project. freenetproject.org. [En línea] [Citado el: 9 de octubre de 2014.] https://freenetproject.org/?language=es.

9. GNUnet | GNU's Framework for Secure Peer-to-Peer Networking. gnunet.org. [En línea] [Citado el: 9 de octubre de 2014.] https://gnunet.org/.

10. OneSwarm - Private P2P Data Sharing. oneswarm.org. [En línea] [Citado el: 9 de octubre de 2014.] http://www.oneswarm.org/.

11. BitBlinder. uptodown.com. [En línea] [Citado el: 9 de octubre de 2014.] http://bitblinder.en.uptodown.com/.

12. ANts P2P. sourceforge.net. [En línea] [Citado el: 9 de octubre de 2014.] http://antsp2p.sourceforge.net/.

13. Anonet Wiki. anonet2.biz. [En línea] [Citado el: 9 de octubre de 2014.] http://anonet2.biz/.

14. Waste. sourceforge.net. [En línea] [Citado el: 9 de octubre de 2014.] http://waste.sourceforge.net/.

15. Diario Oficial de la Unión Europea. Directiva sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como la supervisión prudencial de dichas entidades. 2009.

16. Boletín Oficial del Estado. Ley 21/2011, de 26 de julio, de dinero electrónico. Núm. 179, Sec. I. Pág. 84235, Madrid : s.n., 2011.

17. Financial Crimes Enforcement Network. Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies . Washington : Department of the Treasury (USA), 2013. Guidance. FIN-2013-G001.

18. Paypal. Comprar, vender y transferir dinero por internet - Paypal España. paypal.com. [En línea] [Citado el: 09 de octubre de 2014.] https://www.paypal.com/.

19. Skrill. What is Skrill? | Skrill. skrill.com. [En línea] [Citado el: 10 de octubre de 2014.] https://www.skrill.com/en/about-us/.

20. Webmoney. Webmoney -- Universal Payment System. wmtransfer.com. [En línea] [Citado el: 10 de octubre de 2014.] http://www.wmtransfer.com/eng/information/short/index.shtml.

21. Hub Culture. Hub Culture | About us. hubculture.com. [En línea] [Citado el: 9 de octubre de 2014.] https://hubculture.com/groups/hub/projects/62/wiki/.

22. Second Life Community. Second Life Wiki. [En línea] [Citado el: 10 de octubre de 2014.] http://wiki.secondlife.com/wiki/Getting_Linden_Dollars_FAQ.

23. 1337day. FAQ | 1337day Inj3ct0r Base de datos de exploits : vulnerabilidades : 0day : Nuevos exploits : shellcode por equipo Inj3ct0r. 1337day.con. [En línea] [Citado el: 10 de octubre de 2014.] http://es.1337day.com/faq/buy_gold#buy_gold.

24. CoinMarketCup. Crypto-Currency Market Capitalizations. [En línea] 15 de diciembre de 2014. [Citado el: 15 de diciembre de 2014.] https://coinmarketcap.com/all/views/all/.

25. Nakamoto, Satoshi. Bitcoin: A Peer-to-Peer Electronic Cash System. [Documento] s.l. : Bitcoin.org, 2008.

26. FEMEN. FEMEN. femen.org. [En línea] [Citado el: 9 de noviembre de 2014.] http://femen.org/gallery?attempt=1.

27. Díez, Anabel. Activistas de Femen irrumpen en el Congreso: "El aborto es sagrado". elpais.com. [En línea] 9 de octubre de 2013. [Citado el: 9 de noviembre de 2014.] http://politica.elpais.com/politica/2013/10/09/actualidad/1381304240_913874.html.

28. EFE. Activistas de Femen protestan ante Rouco por la reforma del aborto. elpais.com. [En línea] 3 de febrero de 2014. [Citado el: 9 de noviembre de 2014.] http://sociedad.elpais.com/sociedad/2014/02/02/actualidad/1391372833_430221.html.

29. EFE/AP. Ecologistas franceses entran a planta nuclear en paracaídas. terra.com. [En línea] 5 de febrero de 2012. [Citado el: 9 de noviembre de 2014.] http://noticias.terra.com/mundo/ecologistas-franceses-entran-a-planta-nuclear-en-paracaidas,6540c6cef6e07310VgnVCM5000009ccceb0aRCRD.html.

30. Colectivo Riseup. lists.riseup.net. riseup.net. [En línea] [Citado el: 9 de noviembre de 2014.] https://lists.riseup.net/www/.

31. Loomio. Loomio | Toma de decisiones colectiva. loomio.org. [En línea] [Citado el: 8 de diciembre de 2014.] https://www.loomio.org/?locale=es.

32. The Etherpad Foundation. Etherpad. [En línea] [Citado el: 8 de diciembre de 2014.] http://etherpad.org.

33. Riseup.net. pad.riseup.net. [En línea] [Citado el: 8 de diciembre de 2014.] https://pad.riseup.net/.

34. Cohen, Noam. Hong Kong Protests Propel FireChat Phone-to-Phone App. nytimes.com. [En línea] 5 de octubre de 2014. [Citado el: 9 de noviembre de 2014.] http://www.nytimes.com/2014/10/06/technology/hong-kong-protests-propel-a-phone-to-phone-app-.html?_r=0.

35. Shadbolt, Peter. FireChat in Hong Kong: How an app tapped its way into the protests. cnn.com. [En línea] 16 de octubre de 2014. [Citado el: 9 de noviembre de 2014.] http://edition.cnn.com/2014/10/16/tech/mobile/tomorrow-transformed-firechat/.

36. BBC Mundo. La app con la que los manifestantes de Hong Kong burlan la censura china. bbc.co.uk. [En línea] 30 de septiembre de 2014. [Citado el: 8 de diciembre de 2014.] http://www.bbc.co.uk/mundo/noticias/2014/09/140930_tecnologia_hong_kong_app_protestas_ig.

37. Appgree. Appgree: Now we are talking. appgree.com. [En línea] [Citado el: 8 de diciembre de 2014.] http://www.appgree.com/.

38. Wadobo Labs. Agora Voting. agoravoting.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://agora.agoravoting.com/.

39. Kickstarter Inc. Kickstarter. [En línea] [Citado el: 8 de diciembre de 2014.] https://www.kickstarter.com/.

40. Peerbackers llc. peerbackers - Your Path To Capital - Crowdfunding Consulting. peerbackers.com. [En línea] [Citado el: 8 de diciembre de 2014.] http://peerbackers.com/index.html.

41. Goteo.org. Goteo.org - Crowdfunding the commons. goteo.org. [En línea] Fundación Fuentes Abiertas. [Citado el: 9 de noviembre de 2014.] https://goteo.org.

42. FEMEN. FEMEN official store. femenshop.com. [En línea] [Citado el: 9 de noviembre de 2014.] http://femenshop.com/.

43. Paget, François. El ciberespacio: nuevo medio de difusión de ideas políticas. [En línea] [Citado el: 23 de octubre de 2014.] http://www.mcafee.com/es/resources/white-papers/wp-hacktivism.pdf.

44. El País. elpais.com. [En línea] 9 de diciembre de 2010. [Citado el: 2014 de di-

ciembre de 8.] http://internacional.elpais.com/internacional/2010/12/09/actualidad/1291849211_850215.html#EnlaceComentarios.

45. abc.es. abc.es. [En línea] 21 de diciembre de 2012. [Citado el: 8 de diciembre de 2014.] http://www.abc.es/medios-redes/20121219/abci-twitter-cierra-cuenta-anonymous-201212192044.html.

46. Pastebin. Privacy Policy for pastebin.com . [En línea] [Citado el: 8 de diciembre de 2014.] http://pastebin.com/privacy.

47. Zone-h. Zone-H.org - Unrestricted information. [En línea] [Citado el: 10 de diciembre de 2014.] http://www.zone-h.org/?zh=1.

48. Samuel, Alexandra. Hacktivism and the Future of Political Participation. Cambridge, Massachusetts : Harvard University, 2004.

49. Mailtor. Mailtor is a free anonymous email service provider. mailtor.net. [En línea] [Citado el: 8 de diciembre de 2014.] http://www.mailtor.net/.

50. Hawes, John. Freedom Hosting arrest and takedown linked to Tor privacy compromise. sophos.com. [En línea] 5 de agosto de 2014. [Citado el: 8 de diciembre de 2014.] https://nakedsecurity.sophos.com/2013/08/05/freedom-hosting-arrest-and-takedown-linked-to-tor-privacy-compromise/.

51. Callas, J., y otros, y otros. OpenPGP Message Format. IETF. [En línea] noviembre de 1998. [Citado el: 15 de diciembre de 2014.] https://www.ietf.org/rfc/rfc2440.txt.

52. Silk road: eBay for drugs. Barratt, Monica J. 3, s.l. : Addiction, 2012, Vol. 107.

53. Silk Road. Silk Road - We rise again. silkroad6ownowfk.onion. [En línea] [Citado el: 30 de septiembre de 2014.] http://silkroad6ownowfk.onion.

54. Agora Market. Agora Market. [En línea] 2014. [Citado el: 14 de diciembre de 2014.] https://agorahooawayyfoe.onion/.

55. 7bit@arcor.de. Decentralized anonymous instant messenger on top of Tor Hidden Services. github.com. [En línea] 28 de junio de 2012. [Citado el: 15 de diciembre de 2014.] https://github.com/prof7bit/TorChat.

56. TorBook. Torbook. [En línea] mayo de 2014. [Citado el: 15 de diciembre de 2014.] http://torbookdjwhjnju4.onion.

57. European Cybercrime Centre. The Internet Organized Crime Threat Assessment. s.l. : Europol, 2014.

58. G., Tim. Renting a Zombie Farm: Botnets and the Hacker Economy. [En línea] 8 de octubre de 2014. [Citado el: 11 de diciembre de 2014.] http://www.symantec.com/connect/blogs/renting-zombie-farm-botnets-and-hacker-economy.

59. Poultry markets: on the underground economy of twitter followers. Stringhini, Gianluca, y otros, y otros. [ed.] ACM. New York : s.n., 2012. Proceedings of the 2012 ACM workshop on Workshop on online social networks. ISBN: 978-1-4503-1480-0.

60. Blockchain.info. Dirección de Bitcoin 1AWqYR4CCP5j9GEqMNk8b3ZNPPfG5Jniu1. [En línea] [Citado el: 11 de diciembre de 2014.] https://blockchain.info/address/1

AWqYR4CCP5j9GEqMNk8b3ZNPPfG5Jniu1?currency=EUR.

61. Kumar, Mohit. Hacker threatens to sell data of 3.7 Million Israeli Bank Customers, demands extortion money in Bitcoin. thehackernews.com. [En línea] 21 de diciembre de 2013. [Citado el: 11 de noviembre de 2014.] http://thehackernews.com/2013/12/hacker-Israeli-Bank-botnet-malware-extortion-bitcoin.html.

62. Wei, Wang. CryptoLocker Ransomware demands $300 or Two Bitcoins to decrypt your files. thehackernews.com. [En línea] 13 de octubre de 2013. [Citado el: 11 de noviembre de 2014.] http://thehackernews.com/2013/10/cryptolocker-ransomware-demands-300-to.html.

63. Corman, Steven R. y Schiefelbein, Jill S. Communication and Media Strategy in the Jihadi War of Ideas. Arizona State University. Arizona : Consortium for Strategic Communication, 2006. Report #0601 .

64. Mundo, BBC. bbc.co.uk. [En línea] 20 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://www.bbc.co.uk/mundo/noticias/2014/06/140620_internacional_irak_isis_redes_sociales_amv.

65. Report, ITV. itv.com. [En línea] 17 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://www.itv.com/news/2014-06-17/isiss-official-app-available-to-download-on-google-play/.

66. WhisperText LLC. Whisper - Comparte y Conoce. [En línea] 9 de diciembre de 2014. [Citado el: 13 de diciembre de 2014.] https://play.google.com/store/apps/details?id=sh.whisper.

67. Segall, Laurie. cnn.com. [En línea] 16 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://money.cnn.com/2014/06/16/technology/social/whisper-app-iraq/.

68. The Guardian. Whispers, regrets and re-deployment: 10 Iraq war veterans on the Isis effect. [En línea] 17 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://www.theguardian.com/commentisfree/2014/jun/17/iraq-war-veterans-isis-stories.

69. Makuch, Ben. vice.com. [En línea] 24 de junio de 2014. [Citado el: 13 de diciembre de 2014.] http://motherboard.vice.com/en_uk/read/iraqs-isis-targeting-internet-bans-have-caused-a-huge-surge-in-tor-usage.

70. El Confidencial. elconfidencialdigital.com. [En línea] 4 de abril de 2014. [Citado el: 13 de diciembre de 2014.] http://www.elconfidencialdigital.com/seguridad/Guardia-Civil-TrueCrypt-ETA-Seguridad_0_1372662745.html.

71. El confidencial digital. Así descifra la Guardia Civil el 'TrueCrypt', el nuevo sistema de encriptación de ETA: se ha pedido ayuda a la agencia de Seguridad de Obama. [En línea] 7 de abril de 2010. [Citado el: 13 de diciembre de 2014.] http://www.elconfidencialdigital.com/seguridad/Guardia-Civil-TrueCrypt-ETA-Seguridad_0_1372662745.html.

72. Qaeda Plot Leak Has Undermined U.S. Intelligence. [En línea] http://www.nytimes.com/2013/09/30/us/qaeda-plot-leak-has-undermined-us-intelligence.html?pagewanted=2&_r=0.

73. al-'Amil, Sheikh Abu Saad. Mobile Encryption for Android (V 1.1) and Symbian.

[En línea] 2013. [Citado el: 13 de diciembre de 2014.] http://gimfmedia.com/tech/en/download-mobile-encryption/.

74. Jusino, Eric. die-less. [En línea] 2012. [Citado el: 8 de octubre de 2014.] http://die-less.com/2012/01/06/zetas-offgrid-darknet/.

75. Coinmap.org. CoinMap. [En línea] 2014. [Citado el: 13 de diciembre de 2014.] http://coinmap.org/.

76. Prusnak. Coinmap: Map showing places where you can use Bitcoin and Litecoin. [En línea] 2014. [Citado el: 13 de diciembre de 2014.] https://github.com/prusnak/coin-map.

77. Larimer, Daniel, Hoskinson, Charles y Larimer, Stan. A Peer-to-Peer Polymorphic Digital Asset Exchange. [Digital] 2013.

78. Junestam, Andreas y Guigo, Nicolas. TrueCrypt: Security Assessment (Final Report). s.l. : iSEC Partners, Open Crypto Audit Project, 2014. Security Assessment.

79. Irrera, Anna. Q&A with LMAX CEO on Ven Virtual Currency. eFinancialNews Limited. Financial News.

80. Linden dollar and virtual monetary policy. Ernstenberger, P. s.l. : Macroeconomics, Departmen of Economics, Economics I, Bayreuth University, 2009.

81. Truecrypt Development Team. WARNING: Using TrueCrypt is not secure as it may contain unfixed security issues. [En línea] mayo de 2014. [Citado el: 13 de diciembre de 2014.] http://truecrypt.sourceforge.net/.

82. blockchain.info. Número de direcciones Bitcoin únicas utilizadas. [En línea] 17 de noviembre de 2014. [Citado el: 17 de noviembre de 2014.] https://blockchain.info/es/charts/n-unique-addresses?timespan=all&showDataPoints=false&daysAverageString=1&show_header=true&scale=0&address=.

83. Loomio. Loomio is an open-source web application that helps groups make better decisions together. github.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://github.com/loomio/loomio.

84. Boletín Oficial del Estado. Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. Núm. 103, Sec. I, Pág. 37458, Madrid : s.n., 2010.

85. Webmoney. Guarantors in the WebMoney Transfer System. wmtransfer.com. [En línea] [Citado el: 10 de octubre de 2014.] http://www.wmtransfer.com/eng/subjects/guarantors/index.shtml.

86. Free Software Foundation. GNU Affero General Public License - GNU Project. gnu.org. [En línea] 3, 19 de noviembre de 2007. [Citado el: 29 de septiembre de 2014.] https://www.gnu.org/licenses/agpl.html.

87. GNU.FREE project. FREE project policy change... gnu.net. [En línea] 25 de octubre de 2002. [Citado el: 8 de diciembre de 2014.] http://www.gnu.org/software/free/.

88. Blockchain.info. Exchange Rates API: Market Prices and exchanges rates api. [En línea] 2014. [Citado el: 11 de diciembre de 2014.] https://blockchain.info/es/ticker.

89. Electronic Frontier Foundation. E-Voting Rights. eff.org. [En línea] [Citado el: 8 de diciembre de 2014.] https://www.eff.org/es/issues/e-voting.

90. The Etherpad Foundation. Etherpad: Really real-time collaborative document editing. github.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://github.com/ether/etherpad-lite.

91. EMule-Project.net - Sitio Oficial de eMule. Descargas, ayudas, documentación, novedades, ... emule-project.net. [En línea] [Citado el: 9 de octubre de 2014.] http://www.emule-project.net/home/perl/general.cgi?l=17.

92. FSF France. Electronic voting and Free Software. fsffrance.org. [En línea] 17 de octubre de 2004. [Citado el: 8 de diciembre de 2014.] http://fsffrance.org/voting/voting.en.html.

93. Parlamento Europeo y el Consejo. Directiva 2009/110/CE del Parlamento Europeo y del Consejo, de 16 de septiembre de 2009 , sobre el acceso a la actividad de las entidades de dinero electrónico y su ejercicio, así como sobre la supervisión prudencial de dichas entidades, por la que se mod. DO L 267 de 10.10.2009, p. 7/17 , Directiva 2009/110/CE . s.l. : Diario Oficial de la Unión Europea, 2009.

94. Ares | Descarga gratis el mejor programa P2P. ares.com.es. [En línea] [Citado el: 9 de octubre de 2014.] http://www.ares.com.es/.

95. Wadobo Labs. A Liquid Voting system made with python and django. github.com. [En línea] [Citado el: 8 de diciembre de 2014.] https://github.com/agoravoting/agora-ciudadana.

96. Elistas. elistas.net. [En línea] [Citado el: 15 de diciembre de 2014.] http://www.elistas.net/grupos/Informatica/Seguridad.

97. LeakForums. LeakForums. [En línea] [Citado el: 15 de diciembre de 2014.] http://leakforums.org/?c=1.

98. The Republic of Lampeduza. The Republic of Lampeduza - Carding Forum, Dumps & Credit Cards Security. [En línea] [Citado el: 15 de diciembre de 2014.] http://lampeduza.so/.

99. Europol. The Internet Organized Crime Threat Assessment. s.l. : European Cybercrime Centre, 2014.

Fecha de recepción: 20/11/2014. Fecha de aceptación: 17/12/2014