ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

122/2013 10 diciembre de 2013

*Manuel R. Torres Soriano**

SIETE LECCIONES NO APRENDIDAS SOBRE ANONYMOUS

SIETE LECCIONES NO APRENDIDAS SOBRE ANONYMOUS

Resumen:

El propósito de este trabajo es abordar las siete principales lecciones que pueden extraerse de la aparición, desarrollo y decadencia del movimiento de *hacktivismo* llamado Anonymous. La breve historia de este grupo es de gran interés para entender algunas dinámicas de poder y movilización social en la era de la información. Este legado no ha sido siempre bien entendido, siendo habitual que se asuman como ciertas, determinadas imágenes distorsionadas sobre su funcionamiento y capacidades. Se analiza el papel secundario que puede tener la ideología, frente a una estética atrayente; la importancia de las organizaciones formales para coordinar e imprimir eficacia a las aportaciones de un amplio colectivo de personas; y el peligro de la sobre-reacción frente a este tipo de amenazas.

Abstract:

The purpose of this paper is to address the seven key lessons to be drawn about the origin, development and decay of hacktivism movement called Anonymous. The brief history of this group is of great interest to understand some of the dynamics of power and social mobilization in the information era. This legacy has not always been well understood, it being usual to assume as true, certain images distorted on its operation and capabilities. This article analyzes the role it may have ideology vs. an attractive appearance, the importance of formal organizations to support and coordinate a broad group of people, and the danger of over-reaction to this type of threats.

Palabras clave:

Ciberseguridad, hacktivismo, internet, actores no estatales.

Keywords:

Cybersecurity, hacktivism, internet, non-state actors.

Anonymous es el principal referente de una nueva forma de participación política no convencional conocida como *hacktivismo*: el recurso a los ataques, sabotajes y robo de información en el ciberespacio como instrumento de presión e influencia. Sus actividades han sido interpretadas como una premonición del poder que puede alcanzar una nueva generación de actores políticos generados exclusivamente a través de Internet. A la altura de 2011, tan solo tres años después de sus primeras acciones, el grupo ya era percibido como una ciber-amenaza de primer nivel debido a la magnitud y frecuencia de sus operaciones de *hackeo*. El nombre de Anonymous empezó a ser una palabra familiar en los informativos y en las declaraciones de políticos y responsables de las agencias de seguridad e inteligencia de medio mundo. Su estructura sin liderazgo y su lógica de funcionamiento basada en la espontaneidad y el voluntarismo de sus miembros, parecían una combinación invencible frente a la cual poco podían hacer las estructuras de poder clásicas[1]. Sin embargo, en un corto espacio de tiempo, tuvo lugar una sucesión de operaciones policiales contra sus miembros más destacados, lo que provocó una rápida decadencia operativa del movimiento, y la pérdida de su protagonismo mediático.

La breve historia de Anonymous es de gran interés para entender algunas dinámicas de poder y movilización social en plena era de la información. Sin embargo, este legado no ha sido siempre bien entendido, siendo habitual que se asuman como ciertas determinadas imágenes distorsionadas sobre su funcionamiento y capacidades.

El propósito de este artículo es enumerar las siete principales lecciones que pueden extraerse de la aparición, desarrollo y decadencia de Anonymous, las cuales nos permiten intuir algunas tendencias sobre el activismo político y social en Internet, así como el impacto de este tipo de grupos sobre la seguridad en el ciberespacio.

1- EL AZAR PUEDE CREAR LAS MARCAS MÁS EXITOSAS

El principal activo de Anonymous es precisamente su atractivo como marca. Su nombre, y una estética propia de los comics de superhéroes, funcionaron como reclamo para que miles de internautas se sintiesen atraídos por una identidad alternativa que prometía misterio, secretismo y la oportunidad de cambiar el mundo desde tu propio ordenador.

Una de las realidades más sorprendentes de este "éxito comercial", es que su origen no es el sesudo trabajo de un equipo de expertos en marketing y comunicación, sino el resultado del azar y la creatividad espontánea de la subcultura de Internet.

El germen de Anonymous es un foro de internet llamado *4chan*, creado originariamente como un lugar para el intercambio de archivos de imagen entre los aficionados al *anime* japonés. Desde su aparición en 2003, fue evolucionado dando cabida a otro tipo de

[1] OLSON Parmy. "5 Things Every Organization Can Learn From Anonymous", *Forbes* (6.5.2012), disponible en: http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/. Fecha de la consulta 05.11.2013.

contenidos, los cuales siempre tuvieron como rasgo común el uso de un lenguaje deliberadamente ofensivo y la búsqueda de "Lulz" (una corrupción del acrónico en inglés LOL: "laugh out loud": "reír a carcajadas"). La plataforma estaba compuesta por varios directorios temáticos, dentro de los cuales destacaba el llamado "/b/ board", el más inclasificable de todos. En él era posible encontrar desde la pornografía más bizarra (cuyo único límite era los contenidos pedófilos) a las fotografías de gatitos, todo ello aderezado con un humor muy particular basado en la subcultura hacker. La búsqueda de diversión a toda costa, sin importar sus consecuencias, dio lugar a bromas que traspasaran el ámbito virtual como, por ejemplo, el envío masivo de pizzas o pornografía a personas, grupos o instituciones elegidas únicamente por la expectativa de que sintiesen especialmente molestas u ofendidas.

El foro *4chan*, a diferencia de otras plataformas de Internet, no exigía un registro previo para participar o acceder a sus contenidos. Aquellos que optaban por ingresar sin nombre de usuario, eran etiquetados automáticamente por el foro como usuario "anónimo". En el caso del directorio "/b/ board", el lugar más activo y proclive a los excesos verbales, el porcentaje de usuarios que decidían no hacerlo alcanzaba el 90%[2], lo que les llevó a conocerse entre sí como los "anonymous".

2- EL ACTIVISMO POLÍTICO PUEDE SER DIVERTIDO

Dentro de los habituales del foro *4chan* empezó a ganar fuerza un sector al que los usuarios bautizaron como "moralfags", los cuales querían añadir algún sentido trascendente o utilidad a las bromas pesadas que periódicamente se organizaban desde esta plataforma. Su propuesta era dirigir estas acciones hacia objetivos a los que consideraban perniciosos para la libertad en internet o para la propia sociedad.

A principios de 2008 tuvo lugar un acontecimiento que supuso la consolidación de Anonymous como movimiento de *hacktivismo*. En enero se filtró en internet un video[3] protagonizado por el actor Tom Cruise donde reflexionaba sobre su experiencia como adepto a la cienciología. Se trataba de una producción de consumo interno, elaborada con la intención de ser proyectada dentro las reuniones de los seguidores de esta creencia. El intérprete estadounidense no salía especialmente bien parado en esa entrevista: sus respuestas improvisadas carecían de sentido y parecía un desequilibrado que gesticulaba de manera incoherente. El video fue motivo de todo tipo de bromas y sátiras dentro de la comunidad de internautas.

---

[2] BERNSTEIN Michael S., MONROY-HERNANDEZ A., HARRY D., ANDRE P., PANOVICH K. y VARGAS G. "4chan and /b/: An Analysis of Anonymity and Ephemerality in a Large Online Community", *Association for the Advancement of Artificial Intelligence*, 2011, disponible en: http://projects.csail.mit.edu/chanthropology/4chan.pdf. Fecha de la consulta 05.11.2013.

[3] Puede encontrarse una copia de este video en: http://www.youtube.com/watch?v=XHzfwFj2NdY. Fecha de la consulta 05.11.2013.

Tras la difusión no autorizada de esta grabación, la Iglesia de la Cienciología, como ya había sido habitual en el pasado, empezó a demandar judicialmente a cualquier web o servicio que alojase en sus páginas este video, o aprovechase su difusión para realizar comentarios críticos contra la cienciología.

Los "anons" partidarios de conjugar la diversión y cierta conciencia política se organizaron fuera del foro y dirigieron su primera gran ofensiva coordinada ("Project Chanology") contra la Iglesia de la Cienciología, a la cual consideraban una peligrosa secta dedicada al lavado de cerebro de sus miembros[4]. Además de sabotear algunas de sus web oficiales, alentaron un boicot global que se trasladó al ámbito físico. Algunos miembros empezaron a protestar en frente de las dependencias de esta iglesia, pero al hacerlo decidieron ocultar sus rostros para no ser identificados y demandados por los cienciólogos[5]. Acordaron utilizar la máscara de Guy Fawkes, un conspirador inglés del siglo XVI, el cual sirvió de inspiración para un comic y una película con un claro mensaje antisistema llamada *V de Vendetta*. De ese modo nació una estética que se convertiría en el núcleo central de la identidad de Anonymous por encima de cualquier elemento ideológico u objetivo común.

Miembros de Anonymous protestando en frente de las dependencias de la Iglesia de la Cienciología

La expresión procedente del argot de Internet "no alimentes al troll" encierra una importante lección que explica en buena medida en auge y popularidad de este movimiento. Los "troll" son aquellos internautas que se dedican a molestar deliberadamente a otros usuarios, a través de provocaciones o comentarios ofensivos, con la intención de

[4] ANDERSON Nate, "Who Was That Masked Man?", *Foreign Policy* (31.01.2012), disponible en: http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man. Fecha de la consulta 05.11.2013.

[5] Grupo S21sec, "Anonymous", *S21sec Ecrime* (2009).

desencadenar una respuesta desmedida. En la subcultura de Internet existe la certeza de que la peor forma de encarar la acción de estos vándalos virtuales es responderles de manera emocional. Al hacerlo sólo se contribuye a "alimentar al troll", reafirmando su postura y animando a otros usuarios a seguir los pasos del provocador.

Uno de los más poderosos potenciadores de la actividad de Anonymous fue precisamente la reacción de sus víctimas. Cuando la Iglesia de la Cienciología empezó a ser hostigada, respondió de manera desproporcionada declarando públicamente que eran víctimas de "un grupo de ciber-terroristas…perpetrando crímenes de odio religioso[6]". Estas declaraciones divirtieron profundamente a los atacantes, animándoles a seguir por el mismo camino, e incitando a otros unirse a esta ofensiva contra lo que consideraban eran una secta detestable que empezaba a perder los nervios.

3- EN INTERNET NO NECESITAS UNA LEGIÓN DE SEGUIDORES

Uno de los eslóganes más célebres de Anonymous es "Somos legión", una expresión que pretende trasladar a la opinión pública la idea de que sus miembros son innumerables. El propio grupo se encargó de afirmar que no había líderes detrás del movimiento, y por tanto la detención de algunos de sus activistas no podía neutralizarles. La realidad es bien distinta. El germen del grupo y su evolución posterior es obra de apenas cinco hackers sobre los cuales orbitó, no sólo la actividad comunicativa de la organización, sino la ejecución de sus ataques más destacados a lo largo de 2011. El arresto de este núcleo duro supuso el inicio de un periodo de decadencia operativa y de irrelevancia mediática. Aunque son miles los internautas que han frecuentado los chats, foros y redes sociales administradas o inspiradas por Anonymous, la realidad es que sólo un pequeño grupo de ellos han sido verdaderos hackers con las habilidades necesarias para implementar ciberataques.

La gran mayoría han sido simpatizantes, que han consumido y retroalimentado el discurso del grupo a través de Internet, siendo muy heterogéneo su grado de identificación, compromiso e implicación. Algunos frecuentaron estos espacios por curiosidad, otros buscaron una vía de "bajo coste" en términos de esfuerzo y riesgo para dar salida a su frustración o voluntad de transformar la realidad. Para otros, era simplemente la oportunidad de sentirse miembros de un proyecto colectivo, sin importar excesivamente su contenido. Sin embargo, en todos esos casos, la importancia de sus contribuciones fue totalmente secundaria para el éxito de las "operaciones" de Anonymous. No obstante, algunos de los ciber-ataques más exitosos fueron presentados como el resultado del esfuerzo colaborativo de decenas de miles de internautas que ponían a disposición de las "operaciones" sus habilidades y potencial informático. Para ello habrían recurrido a herramientas descargadas de los foros del movimiento y ejecutadas de manera coordinada en sus equipos para tumbar la web atacada (DDoS: ataques de denegación de servicio). La

[6] SMITH Stevie, "Scientologists accuse protestors of cyber terrorism", *The Tech Herald* (11.02.2008), disponible en: http://www.thetechherald.com/articles/Scientologists-accuse-protestors-of-cyber-terrorism. Fecha de la consulta 06.11.2013

realidad es que esta participación masiva sólo era útil contra webs muy modestas, siendo totalmente ineficaz contra las páginas de grandes compañías concienciadas sobre la necesidad de proteger sus redes. A pesar de ello este tipo de llamamientos al *hackeo* colectivo se mantuvo, no por necesidades logísticas, sino como un instrumento para lograr la implicación de los seguidores y como recurso propagandístico.

Las principales operaciones de hostigamiento, como las que se llevaron a cabo contra compañías de pagos online como *Paypal, Visa y Mastercard* fue llevadas a cabo gracias a la potencia cientos de miles de *botnets*, u ordenadores sobre los que se había tomado de manera fraudulenta el control para coordinar ataques en fuerza contra objetivos en el ciberespacio[7]. Esta acción hacía innecesaria la participación voluntaria de los "anons", bastando con la intervención de un único controlador o "botmasters". Paradójicamente los ordenadores más importantes en las operaciones de Anonymous procedían de millones de internautas que de manera involuntaria e inconsciente pasaron a engrosar las capacidades del grupo cuando descargaron accidentalmente software infectado, o visitaron una web inapropiada que instaló malware en sus equipos. Anonymous, no sólo creó sus propias redes de ordenadores "cautivos", sino que también acudió al mercado negro para alquiler puntualmente algunos de estos botnets a un precio irrisorio[8].

4- PARA ACTUAR COMO UN HACKER NO HACE FALTA SABER INFORMÁTICA

La imagen de sofisticación técnica proyectada por Anonymous no se corresponde necesariamente con las habilidades de sus miembros. Aunque su núcleo duro poseía unos conocimientos técnicos por encima del internauta medio, sus ciberataques más populares no implicaron ningún salto cualitativo con respecto a las técnicas e instrumentos usados hasta el momento por otros grupos de *hacktivismo*, ni mucho menos se acercaban a las empleadas por las organizaciones de ciber-delincuencia más importantes. Muchos de sus ataques se implementaron llevando a cabo herramientas genéricas de *hackeo* disponibles en manera abierta en Internet, como por ejemplo el llamado "Low Orbit Ion Cannon", una aplicación que envía múltiples solicitudes de acceso al servidor de una página web. Un programador puede utilizar de manera legítima este test para asegurar que una página web puede soportar un tráfico intenso. En cambio, si se quiere utilizar como una herramienta de ataque, basta con que un grupo de personas se coordine para ejecutar desde sus ordenadores esta aplicación sobre una misma web, con el objetivo de que el servidor se sature y deje de estar operativo[9].

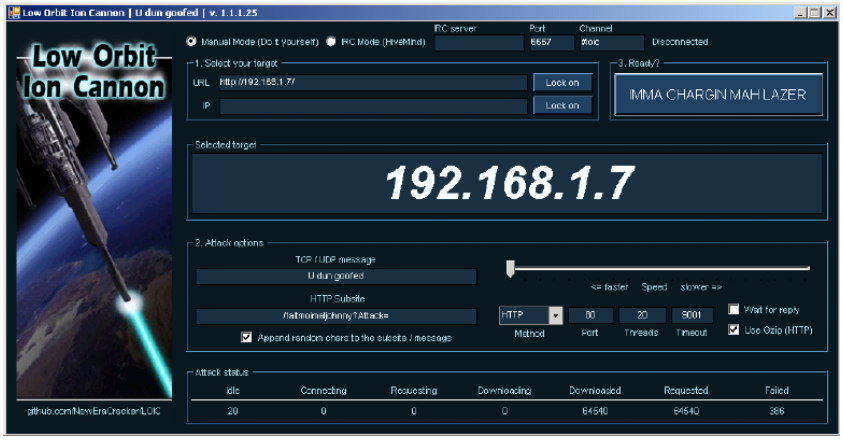
---

[7] OLSON Parmy, *We are Anonymous: inside the hacker world of Lulzsec, Anonymous, and the global cyber insurgency* , London, Little, Brown and Company, 2012.

[8] Las cantidades pueden oscilar en función del número de ordenadores vinculados en el botnet. Uno de tamaño medio puede ser alquilado 24 horas por menos de 100$. Para ataques de mayor entidad se necesita una red de muchos más equipos la cual puede contratarse durante una hora por unos 200$. Véase: Ibid.

[9] NORTON Quinn, "How Anonymous Picks Targets, Launches Attacks, and Takes Powerful Organizations Down", *Threat Level -Wired* (7.03.2012), disponible en http://www.wired.com/threatlevel/2012/07/ff_anonymous/.

Las operaciones destinadas al robo de información, aparentemente más complejas, también fueron llevadas a cabo a través de procedimientos simples como las llamadas "inyecciones SQL" las cuales pueden ser ejecutadas a través de aplicaciones automatizadas gratuitas, como "Havij" que no exigían ningún tipo de programación o conocimiento especializado[10].



Consola del programa LOIC para la realización de ataques DDoS (Versión 1.1.1.25)

El verdadero poder de Anonymous residió en la falta de diligencia de sus víctimas, las cuales no habían mantenido medidas de ciber-seguridad básicas para evitar ser víctimas de estos sabotajes y robos de datos. Esta deficiente protección era común incluso en grandes compañías cuya principal línea de negocio tenía una base tecnológica. Así, por ejemplo, la japonesa Sony no nombró a un responsable de ciberseguridad, hasta haber sufrido a manos de Anonymous el robo de los datos de los 77 millones de clientes que accedían a su red de juegos online[11], algo que obligó a la firma japonesa a suspender el servicio durante semanas. La deficiente seguridad de estas compañías no era un dato de acceso público, algo que permitió a Anonymous seguir cultivando una imagen de supremacía técnica. Sin embargo, sus miembros no se habían dedicado a desarrollar procedimientos creativos e individualizados para sobrepasar las defensas de sus objetivos, simplemente se limitaron a la búsqueda indiscriminada de víctimas que pudiesen ser vulnerables al software de *hackeo* disponible en la red.

Fecha de la consulta 05.11.2013.

[10] OLSON Parmy, "Now Anyone Can Hack a Website Thanks To Clever, Free Programs", *Forbes* (25.04.2012), disponible en: http://www.forbes.com/sites/parmyolson/2012/04/25/now-anyone-can-hack-a-website-thanks-to-clever-free-programs/ Fecha de la consulta 05.11.2013.

[11] POULSEN Kevin, "PlayStation Network Hack: Who Did It?", *Threat Level -Wired* (27.04.2011), disponible en http://www.wired.com/threatlevel/2011/04/playstation_hack/. Fecha de la consulta 05.11.2013.

A pesar de sus proclamas, los "anons" tampoco era indetectables ni impunes. El núcleo duro del movimiento fue identificado y detenido en un corto espacio de tiempo a través de medios de investigación convencionales, los cuales se vieron facilitados por la traición de uno de sus miembros más importantes: Hector Xavier Monsegur, alias "Sabu," el cual actuó como "agente provocador" para el FBI[12]. Desde diciembre de 2010 hasta abril de 2012, fueron identificados, interrogados o detenidos más de 210 personas relacionadas con Anonymous en 12 países distintos[13].

Esta realidad llevó a algunos analistas a matizar las valoraciones más alarmistas sobre el peligro que suponía esta colectivo. Sus miembros no dejaban de ser unos "grafiteros de Internet"[14], cuyas acciones generaban mucho "ruido", pero escasas consecuencias.

5 - UNA ESTÉTICA ATRACTIVA PUEDE SER SUFICIENTE PARA LOGRAR LA MOVILIZACIÓN POLÍTICA

Anonymous pasó en un corto espacio de tiempo, de ser un pequeño grupúsculo de hackers con inquietudes políticas, a un verdadero movimiento con miles de seguidores repartidos por toda la geografía del planeta. Sin embargo, el atractivo de lo que algunos catalogaron como "el primer movimiento de conciencia online"[15] no residía en un relato ideológico persuasivo, o en un plan de acción coherente. Más allá de sus poses antisistema que le llevaron a denunciar la manipulación y el sometimiento ciudadano ejercido por parte de gobiernos y grandes empresas, el ideario de Anonymous era imposible de concretar en propuestas específicas sobre cómo debía organizarse la política, la sociedad o la economía. Los diferentes activistas que ejercieron de portavoces o redactaron sus escritos, plasmaban sus propios planteamientos y fobias personales, haciendo que el discurso de Anonymous fuese oscilando en función de quien se decidiese a hablar en cada momento en nombre del grupo.

[12] ALANDETE David, "'Hacker', líder, insurgente y... topo del FBI", *El País*, (10.03.2012), disponible en http://internacional.elpais.com/internacional/2012/03/10/actualidad/1331404002_864490.html. Fecha de la consulta 05.11.2013.; FISHMAN Steve, "Hello, I Am Sabu ... ", *New York Magazine* (3.06.2012), disponible en http://nymag.com/news/features/lulzsec-sabu-2012-6/. Fecha de la consulta 05.11.2013

[13] PAGET François, "Hacktivism. Cyberspace has become the new medium for political voices", *White Paper – McAfee Labs* (2012), 16, disponible en: http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf Fecha de la consulta 06.11.2013

[14] GOLDMAN David, "Hacker group Anonymous is a nuisance, not a threat", *CNN Money* (20.01.2012), disponible en: http://money.cnn.com/2012/01/20/technology/anonymous_hack/. Fecha de la consulta 05.11.2013

[15] Grupo S21sec op. cit.

Poster publicitario de la película *V for Vendetta* (2005)

Ni siquiera su lema más importante: "Somos legión. No olvidamos. No perdonamos. Espéranos" permitía intuir algo diferente a que eran muchos los que tenían ganas de venganza, pero ni una palabra sobre la razón de esa ira. No existía una estrategia elaborada sobre cual eran las prioridades, o cómo sus acciones contribuirían al logro de sus fines. Esta confusión les llevó a dirigir sus ataques de contra objetivos tan heterogéneos e inconexos como el grupo mexicano de narcos "Los Zetas"[16], los pedófilos de Internet[17], las asociaciones de gestión de derechos de autor[18], o el gobierno de Israel[19].

[16] REXTON KAN Paul, "Cyber War in the Underworld: Anonymous vs Los Zetas in Mexico", *Yale Journal of International Affairs*, Winter 2013, 40-51, disponible en: http://yalejournal.org/wp-content/uploads/2013/03/Kan.pdf. Fecha de la consulta 05.11.2013

[17] STEADMAN Ian, "Anonymous launches #OpPedoChat, targets paedophiles", Wired (10.07.2012), disponible en: http://www.wired.co.uk/news/archive/2012-07/10/anonymous-targets-paedophiles Fecha de la consulta 05.11.2013

[18] ROMERO Pablo. "Así actuó la Policía para identificar a los supuestos 'líderes' de Anonymous", *El Mundo* (27.06.2011), disponible en: http://www.elmundo.es/elmundo/2011/06/24/navegante/1308937468.html. Fecha de la consulta 06.11.2013

[19] Associated Press, "'Anonymous' hackers launch cyberattack on Israeli sites", *Fox News* (7.04.2013), disponible en: http://www.foxnews.com/tech/2013/04/07/anonymous-hackers-launch-cyberattack-on-israeli-sites/. Fecha de la consulta 06.11.2013

El ejemplo de Anonymous nos muestra como en plena era de la información, una iconografía atrayente, aunque carezca de un respaldo ideológico, puede ser un elemento suficiente para lograr una movilización masiva. Muchos de los que se sumaron a los planes de los "anons" lo hicieron atraídos por la estética de un grupo que se identifica con la mitología heroica propia de un comic: la oportunidad de formar parte de un grupo invisible, omnipotente y omnipresente. Los comunicados en video de los portavoces del grupo ataviados con la máscara de Guy Fawkes y una voz distorsionada a través de ordenador, era una imagen perturbadora, pero a la vez fascinante. Anonymous se presentaba como un rival situado a la altura de las elites que controlaban los resortes del poder mundial, y por tanto, alguien a cuyo lado merecía la pena pelear, aunque no se tuviese demasiado claro cuál era el objetivo de la lucha.

6- LAS ORGANIZACIONES SIGUEN CONTANDO, INCLUSO EN INTERNET

Su estructura caótica permitió proyectar una imagen de ubicuidad, sin embargo, esta ausencia de control sobre aquellos que reivindicaban la pertenencia al movimiento, también provocó el solapamiento de múltiples grupos e individuos con agendas contradictorias. Bajo la bandera de Anonymous se congregaron personas que sinceramente creían que debían apoyar los procesos de democratización en el mundo, a otros cuya única inspiración era un destrucción nihilista del mundo tal y como lo conocían[20]. Algunos grupos de ciber-delincuentes sacaron partido de esta ausencia de control, para apropiarse de la marca Anonymous y llevar a cabo acciones de chantaje contra empresas. De manera paralela, otros utilizaban de manera ilimitada este nombre para lanzar una serie de amenazas que no se veían respaldadas por ninguna acción, y terminaban erosionando la credibilidad del colectivo[21].

Anonymous ha sido definido como "marca de acceso abierto"[22] que cualquiera podía adoptar y abandonar cuando estimase conveniente. Esta ausencia de responsabilidad sobre su reputación, ha generado la contradicción de que algunos miembros deban unir el nombre de Anonymous, a algo tan escasamente anónimo como sus respectivos pseudónimos en la red, los cuales sí tienen un historial previo y una posible verificación.

La falta de una mínima estructura organizativa capaz de coordinar el potencial y el trabajo de sus miembros, también ha supuesto al movimiento una limitación a la hora de llevar a cabo acciones distintas a las del sabotaje a través de Internet. Cuando Anonymous robó los archivos digitales de la empresa de análisis geopolítico Stratfor[23], no tenía capacidad para

[20] LEMOS Robert, "Anonymous Must Evolve or Break Down, Say Researchers", *Dark Reading* (19.04.2012), disponible en: http://www.darkreading.com/attacks-breaches/anonymous-must-evolve-or-break-down-say/232900561. Fecha de la consulta: 06.11.2013

[21] PAGET Francois, "The Future of Hacktivism and Anonymous", *McAfee Blog Central* (18.01.2013), disponible en: http://blogs.mcafee.com/mcafee-labs/the-future-of-hacktivism-and-anonymous. Fecha de la consulta: 06.11.2013.

[22] GOLDMAN op. cit.

[23] DURDEN Tyler, "Intelligence Service Stratfor Suffered A Devastating Hacking Attack Last Night", *Business*

sacar partido al contenido de 2,7 millones de correos electrónicos que habían conseguido extraer de sus servidores. Para llevar a cabo la lectura, interpretación y explotación mediática de los escándalos que supuestamente encerraban los intercambios de esta empresa con gobiernos y empresas de todo el mundo, Anonymous recurrió a los servicios del portal de filtraciones Wikileaks, que bautizó esta colaboración como "Global Intelligence Files". Sin embargo, la plataforma dirigida por Julian Assange, en buena medida, adolecía de las mismas limitaciones organizacionales, y tuvo a su vez que externalizar la labor de análisis con veinticinco medios de comunicación tradicionales. La experiencia no fue demasiado satisfactoria para Anonymous, puesto que poco tiempo después anunció públicamente que rompía su acuerdo de colaboración con Wikileaks afirmando "no podemos apoyar más en lo que se ha convertido Wikileaks: en el espectáculo de un solo hombre, Julian Assange"[24].

Comunicado de Anonymous anunciando una operación de apoyo al fundador de Wikileaks Julian Assange

7- SI QUIERES DAÑAR UNA ORGANIZACIÓN, HAZ PÚBLICA SU INFORMACIÓN

Esta lección fue rápidamente asimilada por los miembros de Anonymous, los cuales comprendieron que el saboteo temporal de las webs de sus objetivos, aunque eran acciones de gran visibilidad, causaban una molestia menor. En cambio, la difusión pública de sus datos confidenciales: el contenido de sus correos electrónicos, listas de clientes, contraseñas, datos financieros, etc., podía erosionar gravemente la reputación de su víctima,

---

Insider (25.11.2011), disponible en: http://www.businessinsider.com/stratfor-hacked-anonymous-2011-12. Fecha de la consulta: 06.11.2013.

[24] Associated Press, "Anonymous rompe relaciones con Assange y WikiLeaks", *La Voz* (12.10.2012), disponible en http://www.lavoz.com.ar/noticias/tecnologia/anonymous-rompe-relaciones-con-assange-wikileaks. Fecha de la consulta: 06.11.2013.

llevándola incluso a la desaparición por los graves perjuicios económicos que estas filtraciones podían causarle por la pérdida de contratos, o por las demandas que debería soportar por no custodiar adecuadamente sus datos. Una de las víctimas más notables de este tipo de acciones fue Aaron Barr, el director de la consultora de ciber-seguridad HBGary Federal, el cual atrajo sobre sí el interés y los deseos de venganza de Anonymous, cuando declaró a un medio de comunicación que, como ejemplo del tipo de servicios que su empresa podía prestar, había sido capaz de establecer la verdadera identidad de los miembros clave del movimiento a través de inteligencia en redes sociales. Barr también hizo pública su intención de facilitar al FBI toda esa información. De manera inmediata, los servidores de HBGary fueron atacados y extraídas las claves de acceso a sus comunicaciones. Anonymous publicó más de 70.000 correos electrónicos de esta empresa. Su contenido era tan embarazoso[25] que Aaron Barr tuvo que dimitir tres semanas después, quedando herida de muerte la reputación de su compañía.

Anonymous puso en evidencia algunas de las contradicciones de la actual sociedad de la información, donde la sobreabundancia informativa y las demandas de transparencia pública, no ha anulado la necesidad que tienen las organizaciones de custodiar y mantener alejada del conocimiento público sus datos más sensibles. Las acciones de un grupo poco sofisticado han demostrado lo frágil que pueden ser algunas posiciones de fuerza ocupadas por grandes corporaciones e instituciones públicas. La pérdida de control sobre sus propia información, bien por filtraciones originadas desde dentro, o por incursiones externas, pueden destruir de manera instantánea de las expectativas de algunos de los actores más poderosos, e incluso provocar un cambio en las reglas del juego.

Esta es una de las principales aportaciones del polémico legado[26] de Anonymous que inevitable será replicada por otros grupos hacktivistas: la apropiación ilícita y divulgación de información sensible puede convertirse en una vía principal de activismo político. Según los datos publicados por una empresa de ciberseguridad: durante el año 2011, el *hacktivismo* sólo supuso entre el 2 y 3% del total de los ciberataques producidos en el mundo, sin embargo, estos ataques dieron lugar al 58% de todas las filtraciones ilícitas de datos que se produjeron en ese periodo[27].

*Manuel R. Torres Soriano**
Profesor Titular Ciencia Política. Universidad Pablo de Olavide de Sevilla

[25] Grupo S21sec, "Anonymous", *S21sec Ecrime* (2009).

[26] JACKSON HIGGINS Kelly, "'Anonymous' Legacy: Hacktivists Stole More Data Than Organized Crime In 2011 Breaches Worldwide", *Dark Reading*, (22.03.2012), disponible en: http://www.darkreading.com/vulnerability/anonymous-legacy-hacktivists-stole-more/232700065 Fecha de la consulta: 06.11.2013.

[27] Verizon RISK Team, "2012 Data BREACH Investigations Report", *Verizon* (3.2012), disponible en: http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf. Fecha de la consulta: 06.11.2013.