Capítulo quinto

El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato

Manuel R. Torres Soriano

Resumen

El propósito de este capítulo es analizar cómo el hacktivismo ha sido empleado por individuos y organizaciones como una eficaz estrategia de comunicación. Se presta una especial atención a dos manifestaciones particulares: el hacktivismo yihadista y el antisistema. El propósito de ambos estudios de caso es analizar las dinámicas organizativas de estos movimientos. Se parte de la tesis de que el principal reto al que tiene que enfrentarse el hacktivismo (particularmente el de carácter delictivo) no es tanto la viabilidad de sus operaciones sino cómo conciliar su vertiente colectiva con la individualidad de sus miembros.

Palabras clave

Internet, ciberseguridad, medios de comunicación, privacidad, propaganda.

Abstract

The purpose of this chapter is to analyze how hacktivism has been used by individuals and organizations as an effective communication strategy. Particular attention is paid to two particular manifestations: Jihadist and anti-system hacktivism. The purpose of both case studies is to analyze the organizational

dynamics of these movements. The starting point is the thesis that the main challenge facing hacktivism (particularly that of a criminal nature) is not so much the viability of its operations, but how to reconcile its collective side with the individuality of its members.

Keywords

Internet, cybersecurity, media, privacy, propaganda.

Introducción

A comienzos de 2010, la secretaria de Estado norteamericana Hillary Clinton presentó la *Internet Freedom*[1] como uno de los ejes de la política exterior de su país. En un entusiasta discurso atribuyó a las nuevas tecnologías de la información la capacidad de reescribir las reglas del activismo político y empujar a la humanidad hacia un proceso irreversible de liberalización política y democratización. Esta visión era consecuente con una tradición previa de utopismo tecnológico[2] que atribuía a esta herramienta una naturaleza intrínsecamente beneficiosa. Según esto, las nuevas tecnologías fomentan la circulación de la información y la participación de los ciudadanos en las cuestiones políticas, los cuales gozan de un poderoso instrumento para obtener una mayor transparencia y responsabilidad en la actuación de sus gobernantes. Siguiendo esta lógica, algunos autores llegaron a sugerir que los creadores de la red social Twitter deberían recibir el Premio Nobel de la Paz por haber hecho posible el instrumento que galvanizó las protestas de 2009 en Irán contra el fraude electoral[3].

Esta visión sobre Internet como una fuerza en pro del conocimiento y la libertad recibió un nuevo respaldo durante los primeros compases de las llamadas Primaveras Árabes. Internet era el elemento diferencial que había hecho posible en ese momento histórico el proceso de transformación política en el mundo árabe y musulmán. El futuro estaría protagonizado por una masa de ciudadanos empoderados por las nuevas tecnologías, frente a unas autócratas que habían perdido el monopolio sobre los flujos de información.

Este optimismo se vio pronto afectado por el insatisfactorio (y en algunos casos, trágico) desenlace de los distintos escenarios donde se produjeron las protestas. Empezó así a ganar fuerza una visión antagónica sobre la naturaleza de Internet, una perspectiva que atribuía efectos deterministas a un instrumento que era capaz de erosionar la libertad y privacidad de los ciudadanos en los países democráticos, al tiempo que cimentaba el autoritarismo político en el resto del mundo, potenciando hasta límites insospechados los aparatos de control y represión. Esta visión pesimista se vio reforzada por el desembarco en el territorio virtual de todo tipo de depravados, criminales y grupos terroristas. Una presencia inquietante que alimentaba los miedos y fobias de una sociedad que contemplaba con desconcierto cómo

---

[1] Clinton, Hillary. «Remarks on Internet Freedom» [en línea], en *The Newseum*. Washington DC. 21 enero 2010. Disponible en web: https://2009-2017.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm

[2] Torres, Manuel R. «Internet como motor del cambio político: ciberoptimistas y ciberpesimistas» [en línea], en *Revista del Instituto Español de Estudios Estratégicos*, n.º 1. 2013. pp. 127- 148. Disponible en web: http://revista.ieee.es/index.php/ieee/article/view/40/36.

[3] Aday, Sean et al. «Blogs and Bullets. New Media in Contentious Politics» [en línea], en *United States Institute of Peace*. Washington DC. 2010. Disponible en web: https://www.usip.org/publications/2010/09/blogs-and-bullets-new-media-contentious-politics.

la herramienta que presuntamente iba a universalizar el conocimiento y la libertad, otorgaba una visibilidad inédita a la superstición, la intolerancia y el fanatismo.

Más allá de las lecturas maniqueas que ignoran la naturaleza neutra de esta herramienta, existe un terreno intermedio donde se ha producido la eclosión de un nuevo tipo de activismo político que no solo emplea Internet como una plataforma para promover sus objetivos, sino que también emplea esta tecnología para llevar a cabo, desde un punto de vista instrumental, actividades ilícitas o delictivas que contribuyen a aumentar la resonancia de su ideario. Es el llamado *hacktivismo*, un término que apunta hacia la confluencia entre al activismo político y el uso de técnicas de *hacking*. Se trata de un fenómeno de gran interés que se mueve en una incómoda intersección entre el crimen y el activismo político. Supone, al mismo tiempo, la confirmación de las dos visiones deterministas sobre la naturaleza de Internet: aquella que lo contemplaba como un proceso de empoderamiento de los individuos, y aquella otra que lo contempla como una ventana abierta a los aspectos más sórdidos de la naturaleza humana. Esta naturaleza ambivalente ha generado que no exista unanimidad sobre su conceptualización y elementos definitorios. Las aproximaciones a este fenómeno oscilan entre aquellas visiones que lo entienden como una nueva forma de participación política no convencional, que aprovecha las potenciales que ofrece el ciberespacio, a aquellas otras que lo entienden como una táctica delictiva para avanzar en los objetivos de grupos de carácter ilegítimo.

El propósito de este capítulo es analizar cómo el hacktivismo ha sido empleado por individuos y organizaciones como una eficaz estrategia de comunicación. Todo lo relacionado con el ciberespacio se encuentra rodeado de una aureola de misterio y sofisticación que lo convierte en irresistible ante la perspectiva de los medios de comunicación. Esta atracción es aún más intensa cuando ese ámbito se fusiona con otro tipo de factores de alto impacto informativo como el escándalo político y social, el crimen o el terrorismo. El hacktivismo es contemplado por algunos actores como una carta ganadora que proporciona una visibilidad que difícilmente podrían alcanzar con otro tipo de tácticas.

El universo del hacktivismo es muy heterogéneo, y en él podemos encontrar actores que, a pesar de su praxis delictiva, gozan de una amplia legitimidad por el tipo de objetivos que persiguen o por el antagonismo que originan las víctimas de sus acciones. Este trabajo va a centrar su atención en dos manifestaciones particulares, cuyos objetivos son rechazados por una gran mayoría social: el hacktivismo yihadista y el antisistema. El propósito de ambos estudios de caso es analizar las dinámicas grupales e individuales en las cuales se basan estos movimientos, así como las ventajas y debilidades que posee este tipo de activismo como estrategia de comunicación.

Una breve historia del hacktivismo

Hacktivismo es un término cuyo origen suele atribuirse a un grupo de *hackers* estadounidense que en 1984 adoptaron el nombre de La Secta de la Vaca Muerta, en referencia al matadero texano donde el grupo realiza sus reuniones. Entre su ideario se encontraba la proclama de que el acceso a la información online era un derecho humano universal, lo que les llevó a poner en marcha un proyecto llamado *hacktivismo*, destinado a luchar contra la censura de Internet y a la prestación de apoyo técnico a los internautas que vivían bajo Gobiernos opresivos. Sus acciones características incluían toda una serie de prácticas exclusivamente virtuales, las cuales, a pesar de su carácter no violento, planteaban problemas en cuanto a su legalidad.

A principios de la década de los noventa, cuando los primeros grupos de hacktivismo hicieron su aparición, fue frecuente que desde el ámbito académico se interpretara el fenómeno como una expresión natural del activismo político protagonizado por redes de ciudadanos. Según esta visión, el fenómeno era el resultado de la intersección entre la disponibilidad del ciberespacio, las sociedades de la información y los modernos movimientos sociales de protesta y resistencia. Para algunos observadores, constituían el vínculo entre Internet y la globalización de la democracia participativa[4].

Aquellos que contemplaban con simpatía estos nuevos actores establecían una clara distinción entre este uso poco ortodoxo del activismo político a través del ciberespacio y aquellas otras actividades catalogadas como *cracking*, las cuales no dejaban de ser usos meramente delictivos de las nuevas herramientas informáticas.

El contexto sociopolítico que desencadenó el movimiento antiglobalización de mediados de la década de los noventa[5] sirvió también como germen de los primeros grupos hacktivistas. Puede apreciarse una confluencia entre ambos fenómenos (malestar antiglobalización y nuevas tecnologías de la información) en el protagonismo mundial que alcanzaría el movimiento zapatista de Chiapas (México)[6].

Al amparo de esta nueva ventana tecnológica se congregaron un tipo de activistas políticos revestidos de tres cualidades propias[7]: a) La apuesta por acciones simples, pero de gran impacto social y mediático; b) Una elevada

---

[4] Jordan, Tim. *Activism! Direct Action, Hacktivism and the Future of Society*. London: Reaktion Books, 2002; Hill, Kevin & Hughes, John E. *Cyberpolitics: Citizen Activism in the Age of the Internet*. Lanham (Md): Rowman & Littlefield, 1998.

[5] Auty, Caroline. «Political hacktivism: tool of the underdog or scourge of cyberspace?», *Aslib Proceedings*, vol. 56, n.º 4, 2004, pp. 212-221.

[6] Harvey, Neil. *The Chiapas Rebellion: The Struggle for Land and Democracy*. London: Duke University Press, 1998.

[7] Jordan, Tim; Taylor, Paul A. *Hacktivism and cyberwars: Rebels with a cause?* London: Routledge, 2004.

cualificación técnica que les permitía dominar las nuevas tecnologías de la información, y c) Su desprecio hacia las normas establecidas.

A pesar de que las primeras aproximaciones académicas al fenómeno partían de una valoración positiva sobre los integrantes y objetivos de estos grupos, los medios de comunicación de masas tardaron poco tiempo en enfatizar aquellas otras características que más suspicacia generaban entre la ciudadanía. El carácter anónimo de sus acciones sirvió de base para el tratamiento sensacionalista de la información procedente sobre estos grupos. La predilección que sus miembros mostraron por adoptar nombres inquietantes como The Legion of Doom, Bad Ass Mother Fuckers, Toxic Shock, etc., tampoco ayudó a mejorar este enfoque.

Esta tendencia se vio reforzada por el clima de inseguridad generado por los atentados del 11 de septiembre de 2001 en Washington y Nueva York. La figura del *hacker* empezó a identificarse con la de criminal, y por extensión con la del ciberterrorista[8]. Empezaron a ganar peso los análisis que lo identifican básicamente como una nueva forma de participación política ilegítima, centrada básicamente en el recurso a los ciberataques, sabotajes y robo de información en el ciberespacio como instrumento de presión e influencia.

La trayectoria de grupos de hacktivismo como Anonymous fue interpretada como una premonición del preocupante poder que podía alcanzar una nueva generación de actores virtuales motivados únicamente por el nihilismo. A la altura de 2011, tan solo tres años después de sus primeras acciones, el grupo ya era percibido como una ciberamenaza de primer nivel debido a la magnitud y frecuencia de sus operaciones de hackeo.

Entre lo individual y lo colectivo

A la hora de entender las causas que han provocado la eclosión del activismo político a través del *hacking* ha sido habitual centrar la atención en su utilidad instrumental. Suele incidirse[9] en factores como:

a) Su accesibilidad, incluso para gente que carece de conocimientos técnicos.

b) El reducido riesgo personal de este tipo de activismo si lo ponemos en relación con otro tipo de prácticas como las protestas o sabotajes callejeros.

---

[8] Vegh, Sandor. «The media's portrayal of hacking, hackers, and hacktivism before and after September 11» [en línea], en *First Monday*. 2005. Disponible en web: http://uncommonculture.org/ojs/index.php/fm/article/view/1206/1126.

[9] Denning, Dorothy. «The Rise of Hacktivism» [en línea], en *Georgetown Journal of International Affairs*. 2015. Disponible en web: https://www.georgetownjournalofinternationalaffairs.org/online-edition/the-rise-of-hacktivism.

c) Permite sumarse de manera efectiva a todo tipo de causas, sin importar la distancia o las diferencias culturales o idiomáticas.

d) Sus acciones tienen un alto impacto en la opinión pública y los medios de comunicación.

Los patrones organizativos en este tipo de movimientos varían en términos de formalización y apertura, pero todos ellos normalmente comparten estas características:

e) Suelen constituirse entre grupos de iguales y rechazan jerarquías y mecanismos de representación, aunque es posible encontrar algún tipo de estructuras basadas en un reparto consensuado de tareas para garantizar su sostenibilidad.

f) La confianza y la lealtad suelen ser los principales mecanismos de reclutamiento, lo que produce organizaciones de tamaño reducido, pero también movimientos más amplios que se basan en la existencia de pequeños clústeres de individuos comprometidos con un objetivo específico.

g) La división de trabajo se realiza en base a la reputación individual y a la existencia de un alto grado de motivación de sus miembros.

h) El proceso de toma de decisiones suele producir tensiones entre lo colectivo y lo individual. Mientras que el hacktivismo es un proceso predominante grupal, gran parte de su éxito depende de las habilidades individuales de unos pocos de sus miembros, lo que puede producir conflictos entre sus participantes más valiosos y aquellos que desean disipar las individuales dentro de una personalidad colectiva.

Para entender las dinámicas de gestión de la identidad de los miembros de estos grupos, resulta útil realizar un paralelismo con el mundo de la criminalidad común en Internet. Puede observarse, por ejemplo, que para los ciberdelincuentes el anonimato es tanto un beneficio como un problema: es útil porque los hace menos detectables para las agencias policiales y para otros competidores que desean atacarlos, pero es una limitación porque sin reputación es muy complicado hacer negocios o establecer relaciones de cooperación con otros delincuentes. Sin alguna forma de verificar la identidad, no se puede establecer la confianza. El objetivo es por tanto conjugar objetivos que *a priori* parecen incompatibles: anonimato y reputación.

Existen diferentes procedimientos que permiten establecer relaciones de confianza en un entorno hostil[10]. Así, por ejemplo, los ciberdelincuentes recurren a múltiples indicadores para establecer si un posible colaborador es un agente del orden público, un impostor sin credenciales reales o un mero

[10] Lusthaus, Jonathan. «Trust in the world of cybercrime», en *Global crime,* vol. 13, n.º 2, 2012, pp. 71-94.

espectador «en el lugar equivocado, en el momento equivocado». Como en cualquier otra subcultura, los criminales cibernéticos exhiben sus propios patrones de comportamiento y lenguaje. Estos pueden ser una mezcla de elementos idiomáticos, los temas de los que hablan, actitud, conocimiento y capacidad. La participación permanente en este tipo de subculturas virtuales proporciona un tipo de conocimiento intuitivo muy similar al que se desarrolla en las interacciones cara a cara dentro de los entornos delincuenciales, el cual constituye un importante patrón para establecer la confianza hacia un desconocido. No obstante, este sistema de identificación no es perfecto y necesita ser complementado con otra serie de procedimientos, como la creación de espacios virtuales excluyentes, en los cuales es muy difícil que se produzca un encuentro accidental con alguien que no tiene una voluntad clara de frecuentar esos espacios. Así, por ejemplo, uno de los elementos clave que discrimina un ciberdelincuente genuino de otro tipo de internauta es el conocimiento de dónde se hallan los diversos canales y foros *online* donde localizar a este tipo de individuos. De esa forma, si en el mundo «físico» es plausible que un no criminal pueda acceder de manera accidental a un bar con conexiones criminales, es muy improbable que un internauta común pueda acceder a un foro de venta de narcóticos oculto dentro del anonimato de la *dark web*. Este tipo de espacios no solo están excluidos de manera deliberada de los motores de búsqueda e indexación, sino que su ubicación está en continua migración para eludir el bloqueo de las empresas prestatarias de servicios. Sin una considerable inversión de tiempo para mantener actualizados los contactos y el conocimiento de los lugares de encuentro, resulta muy difícil acceder a estos espacios y contar con la reputación suficiente para poder interactuar con sus miembros.

No suele prestarse tanta atención[11] a los incentivos psicológicos que aporta este tipo de activismo. Se trata de un aspecto que ayuda a entender cómo el hacktivismo no es solo un instrumento útil para el logro de un objetivo político, sino que, para algunos, puede ser un fin en sí mismo debido a su capacidad de aportar una experiencia gratificante.

Algunos de los principales movimientos hacktivistas han tenido su origen en comunidades virtuales cuyo principal nexo de unión era el deseo de sus miembros de transgredir las convenciones sociales desde una perspectiva lúdica. Así, por ejemplo, las raíces de Anonymous pueden detectarse en un foro japonés denominado 2chan dedicado a compartir todo tipo de contenidos aberrantes relacionados con el anime, el porno y las bromas pesadas[12]. En 2003 se crea el equivalente en lengua inglesa de esta página,

[11] Cheng, Justin; Danescu-Niculescu-Mizil, Cristian; Leskovec, Jure. «Antisocial Behavior in Online Discussion Communities» [en línea], en *Proceedings of the Ninth International AAAI Conference on Web and Social Media*. 2015. pp. 61-70. Disponible en web: https://www.aaai.org/ocs/index.php/ICWSM/ICWSM15/paper/viewFile/10469/10489.

[12] Bartlett, Jamie. *The dark net: Inside the digital underworld*. London: Melville House, 2015.

4chan, el cual copió con éxito este modelo y fue capaz de congregar a una amplia comunidad dedicada al «lulz» (una corrupción del acrónico en inglés LOL: *laugh out loud*; reír a carcajadas). Este germen prepolítico originó las primeras tensiones internas en este colectivo cuando algunos de sus usuarios propusieron enfocar sus actividades hacia causas más trascendentes, como la lucha contra la censura en Internet. Algunos usuarios se opusieron a esta reorientación, que contemplaban como una amenaza existencial al único propósito del foro: divertirse sin importar las consecuencias. A pesar de ello, un buen número entendió como conciliables ambos propósitos, y no renunció a la vertiente lúdica del logro de objetivos «morales».

Para entender esta predisposición a la transgresión de las normas sociales resulta útil recurrir a la psicología social. Alguna de sus aportaciones permite entender el atractivo de algunos comportamientos que rompen con lo que se considera socialmente aceptable, pero también cómo este tipo de actitudes pueden verse reforzadas y ampliadas cuando se producen en el ámbito de Internet.

Una de las contribuciones más populares a este ámbito de estudio ha sido la de John Suler, el cual desarrolló el concepto de *efecto de desinhibición online*[13], según el cual los individuos tienen una mayor propensión a romper las normas sociales cuando se encuentran en un entorno *online* que en uno *offline*. Esto se produce como consecuencia de que algunos sujetos «disocian» su realidad física de su realidad virtual. En esta última puede proyectar una identidad ficticia que no tiene por qué atener a las restricciones sociales o a la idea de asumir las consecuencias de su comportamiento. La percepción de anonimato (tanto propio como ajeno) y la sensación de irrealidad les lleva a entender que sus infracciones son impunes al carecer de consecuencias en el mundo «real». El sentido de pertenencia a un colectivo que aprueba y alienta este tipo de actitudes difumina en la responsabilidad grupal determinadas prácticas que serían más difíciles de racionalizar desde un punto de vista individual. Así, por ejemplo, uno de los eslóganes más desafiantes de Anonymous era precisamente: «porque ninguno de nosotros es tan cruel como todos nosotros»[14].

Este tipo de percepciones se ven reforzadas en espacios como, por ejemplo, 4chan, donde el anonimato constituye un principio organizativo[15]. Ante

---

13 Suler, John. «The online disinhibition effect», en *Cyberpsychology & Behavior*, vol. 7, n.º 3, 2004, pp. 321-326.

14 Mitchell, Liam. «Because none of us are as cruel as all of us: Anonymity and Subjectivation» [en línea], en *Theory Beyond the Codes*. 2013. Disponible en web: http://ctheory.net/ctheory_wp/because-none-of-us-are-as-cruel-as-all-of-us-anonymity-and-subjectivation/.

15 Bernstein, Michael S., et al. «4chan and/b: An Analysis of Anonymity and Ephemerality in a Large Online Community» [en línea], en *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media*. 2011. pp. 50-57. Disponible en web: http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/download/2873/4398/.

la ausencia de un sistema que permita verificar la identidad y credibilidad de sus participantes, estas comunidades adoptan otro tipo de estrategias de identificación como el uso compartido de determinadas imágenes, una jerga propia o determinadas pautas de comportamiento que distinguen a los miembros del grupo del resto de internautas. En el caso de la comunidad que dio origen a Anonymous, se optó por cualquier manifestación transgresora: la misoginia, el racismo, la burla contra las minusvalías, las extravagancias sexuales, etc.

Otro factor que facilita las dinámicas que hacen posible el hacktivismo es lo que se ha denominado *sindicación online*[16], la cual hace referencia a cómo Internet ha permitido agregar a individuos que comparten determinadas conductas o intereses, que son minoritarios y habitualmente rechazables por el conjunto de la sociedad. En un contexto previo a Internet, era el azar y la cercanía física lo que determinaba las oportunidades de que estos sujetos pudiesen socializar, normalizar y promover sus intereses comunes. Así, por ejemplo, la probabilidad de que alguien interesado en una parafilia sexual minoritaria pudiese entrar en contacto con otras personas que compartan sus mismas aficiones era muy reducida si este residía en una pequeña localidad alejada de los grandes núcleos urbanos. Sin embargo, Internet crea los espacios de encuentro necesarios para conectar y promover desde un punto de vista colectivo actitudes que antaño habían sido relegadas por la improbabilidad de que se produjese esta conexión física.

La eclosión del hacktivismo antisistema: Anonymous[17]

La marca Anonymous y el hacktivismo se han convertido en sinónimos como consecuencia del enorme éxito mediático alcanzado por este movimiento de base virtual. 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[18]. Sin embargo, en un corto espacio de tiempo, tuvo lugar una sucesión de operaciones policia-

[16] Aiken, Mary. *The Cyber Effect: A Pioneering Cyberpsychologist Explains How Human Behavior Changes Online*. New York: Random House Publishing Group, 2017.

[17] Este epígrafe se basa de manera extensa en un artículo previo del autor: Torres, Manuel R. «Lecciones aprendidas de la lucha contra el yihadismo en Internet» [en línea], en *IEEE Documento de Opinión*. Abril 2017. Disponible en web: http://www.ieee.es/Galerias/fichero/docs_opinion/2017/DIEEEO04-2017_Lucha_Yihadismo_Internet_MRTorres.pdf.

[18] Olson, Parmy. «5 Things Every Organization Can Learn From Anonymous» [en línea], en *Forbes*. 6 mayo 2012. Disponible en web: http://www.forbes.com/sites/parmyolson/2012/06/05/5-things-every-organization-can-learn-from-anonymous/.

les 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. 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 la comodidad de un 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. Como se ha mencionado con anterioridad, 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 evolucionando dando cabida a otro tipo de contenidos, los cuales siempre tuvieron como rasgo común el uso de un lenguaje deliberadamente ofensivo y una finalidad lúdica. La plataforma estaba compuesta por varios directorios temáticos, dentro de los cuales destacaba el llamado */b/ board*, el más inclasificable de todos. 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%, lo que les llevó a conocerse entre sí como los *anonymous*.

Entre los habituales del foro 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 vídeo protagonizado por el actor Tom Cruise donde reflexionaba sobre su experiencia como adepto a la cienciología. Se trataba de una producción de consumo interno, donde el intérprete estadounidense no salía

especialmente bien parado. El vídeo fue motivo de todo tipo de bromas y sátiras dentro de la comunidad de internautas. 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 vídeo o aprovechase su difusión para realizar comentarios críticos contra este grupo.

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[19]. Además de sabotear algunas de sus webs 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. 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.

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*[sic]* [...] perpetrando crímenes de odio religioso»[20]. 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.

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 era bien distinta. En la génesis del grupo y su evolución posterior encontramos apenas cinco *hackers* sobre los cuales orbitó no solo 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

[19] Anderson, Nate. «Who Was That Masked Man?» [en línea], en *Foreign Policy*. 31 enero 2012. Disponible en web: http://www.foreignpolicy.com/articles/2012/01/31/who_was_that_masked_man.

[20] Smith, Stevie. «Scientologists accuse protestors of cyber terrorism» [en línea], en *The Tech Herald*. 11 febrero 2008. Disponible en web: http://www.thetechherald.com/articles/Scientologists-accuse-protestors-of-cyber-terrorism.

han frecuentado los chats, foros y redes sociales administradas o inspiradas por Anonymous, la realidad es que solo un pequeño grupo de ellos han sido verdaderos *hackers* con las habilidades necesarias para implementar ciberataques[21].

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 buscaban una vía de «bajo coste» en términos de esfuerzo y riesgo para dar salida a su frustración o voluntad de transformar la realidad, mientras que tampoco escaseaban los que identificaron una oportunidad para 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 ciberataques 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» las webs atacadas. La realidad es que esta participación masiva solo era útil contra objetivos modestos, 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.

La imagen de sofisticación técnica proyectada por Anonymous no se corresponde necesariamente con las habilidades de sus miembros. Muchos de sus ataques se implementaron llevando a cabo herramientas genéricas de hackeo disponibles en manera abierta en Internet. 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[22].

El verdadero poder de Anonymous residió en la falta de diligencia de sus víctimas, las cuales no habían mantenido medidas de ciberseguridad básicas para evitar ser víctimas de estos sabotajes y robos de datos. Esta deficiente protección era común incluso en grandes empresas cuya principal línea de negocio tenía una base tecnológica. Así, por ejemplo, la compañía japonesa Sony

---

21 Olson, Parmy. *We Are Anonymous: Inside the Hacker World of Lulzsec, Anonymous, and the Global Cyber Insurgency*. London: Little, Brown and Company, 2012.

22 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.

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*, algo que obligó a la firma japonesa a suspender el servicio durante semanas. La deficiente ciberseguridad de algunas de estas empresas no era un dato de acceso público, algo que permitió a Anonymous seguir cultivando una imagen de supremacía técnica. Sin embargo, sus miembros, lejos de dedicarse a desarrollar procedimientos creativos e individualizados para sobrepasar las defensas de sus objetivos, se limitaron a la búsqueda indiscriminada de víctimas que pudiesen ser vulnerables al *software* de hackeo disponible en la red.

A pesar de sus proclamas, los «anons» tampoco eran 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[23]. Desde diciembre de 2010 hasta abril de 2012 fueron identificadas, interrogadas o detenidas más de doscientas diez personas relacionadas con Anonymous en doce países distintos[24].

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»[25] cuyas acciones generaban mucho «ruido», pero escasas consecuencias.

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*» 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.

---

[23] Alandete, David. «*Hacker*, líder, insurgente y... topo del FBI» [en línea], en *El País*. 10 marzo 2012. Disponible en web: http://internacional.elpais.com/internacional/2012/03/10/actualidad/1331404002_864490.html; Fishman, Steve. «Hello, I Am Sabu...» [en línea], en *New York Magazine*. 3 junio 2012. Disponible en web: http://nymag.com/news/features/lulzsec-sabu-2012-6/.

[24] Paget, François. «Hacktivism. Cyberspace has become the new medium for political voices» [en línea], en *White Paper – McAfee Labs*. 2012. Disponible en web: http://www.mcafee.com/us/resources/white-papers/wp-hacktivism.pdf.

[25] Goldman, David. «Hacker group Anonymous is a nuisance, not a threat» [en línea], en *CNN Money*. 20 enero 2012. Disponible en web: http://money.cnn.com/2012/01/20/technology/anonymous_hack/.

Algunos autores[26] han creído detectar en su ideario múltiples matices que coexisten al mismo tiempo y que podrían ser calificados de libertarismo, colectivismo, idealismo, nihilismo, utopismo, distopismo, etc. Sin embargo, por encima de la existencia de una compleja producción doctrinal que requiere interpretación, la realidad es que 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 quién se decidiese a hablar en cada momento en nombre del grupo.

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 cuáles eran las prioridades o cómo sus acciones contribuirían al logro de sus fines. Esta confusión les llevó a dirigir sus ataques contra objetivos tan heterogéneos e inconexos como el grupo mexicano de narcos Los Zetas[27], los pedófilos de Internet[28], las asociaciones de gestión de derechos de autor[29], el Gobierno de Israel[30] o el Opus Dei.

El ejemplo de Anonymous nos muestra cómo 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 cómic: la oportunidad de formar parte de un grupo invisible, omnipotente y omnipresente. Los comunicados en vídeo 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.

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

---

26 Goode, Luke. «Anonymous and the political ethos of hacktivism», en *Popular Communication*, vol. 13, n.º 1, 2015, pp. 74-86.

27 Rexton Kan, Paul. «Cyber War in the Underworld: Anonymous vs Los Zetas in Mexico» [en línea], en *Yale Journal of International Affairs*. 2013. pp. 40-51. Disponible en web: http://yalejournal.org/wp-content/uploads/2013/03/Kan.pdf.

28 Steadman, Ian. «Anonymous launches #OpPedoChat, targets paedophiles» [en línea], en *Wired*. 10 julio 2012. Disponible en web: http://www.wired.co.uk/news/archive/2012-07/10/anonymous-targets-paedophiles.

29 Romero, Pablo. «Así actuó la Policía para identificar a los supuestos 'líderes' de Anonymous» [en línea], en *El Mundo*. 27 junio 2011. Disponible en web: http://www.elmundo.es/elmundo/2011/06/24/navegante/1308937468.html.

30 ASSOCIATED PRESS. «'Anonymous' hackers launch cyberattack on Israeli sites» [en línea], en *Fox News*. 7 abril 2013. Disponible en web: http://www.foxnews.com/tech/2013/04/07/anonymous-hackers-launch-cyberattack-on-israeli-sites/.

e individuos con agendas contradictorias. Bajo la bandera de Anonymous se congregaron personas que sinceramente creían que debían apoyar los procesos de democratización en cualquier lugar del planeta; otros cuya única inspiración era un destrucción nihilista del mundo tal y como lo conocían. Algunos grupos de ciberdelincuentes 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.

Anonymous ha sido definido de varias formas: como la quintaesencia de una marca «antimarcas»[31] o como la «marca de acceso abierto»[32] 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[33] no tenía capacidad para 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, ya que poco tiempo después anunció públicamente que rompía su acuerdo de colaboración con Wikileaks afirmando: «no podemos

31 Coleman, Gabriella. *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*. London: Verso Books, 2014.

32 Paget, Francois. «The Future of Hacktivism and Anonymous» [en línea], en *McAfee Blog Central*. 18 enero 2013. Disponible en web: http://blogs.mcafee.com/mcafee-labs/the-future-of-hacktivism-and-anonymous.

33 Durden, Tyler. «Intelligence Service Stratfor Suffered a Devastating Hacking Attack Last Night» [en línea], en *Business Insider*. 25 noviembre 2011. Disponible en web: http://www.businessinsider.com/stratfor-hacked-anonymous-2011-12.

apoyar más en lo que se ha convertido Wikileaks: en el espectáculo de un solo hombre, Julian Assange»[34].

Frustrados por la decreciente atención pública de sus acciones, en 2012 algunos miembros del colectivo pusieron en marcha una iniciativa llamada Par:AnoIA (Potentially Alarming Research: Anonymous Intelligence Agency)[35]. Se trataba de su propio portal de filtraciones que trataba de cubrir el hueco que había dejado su ruptura con Wikileaks. La plataforma pretendía ampliar el impacto de sus publicaciones masivas de datos, las cuales tenían un impacto mediático fugaz debido a la incapacidad de los medios de comunicación convencionales para explotar un elevado volumen de información. Los creadores de esta iniciativa pretendían explotar el potencial de la *inteligencia colectiva* que reside en el ciberespacio, ofreciendo a los internautas una plataforma para trabajar de manera desestructurada en el análisis de estas filtraciones. Sin embargo, este experimento de *crowdsourcing* no funcionó. La comunidad de internautas que respaldaba las acciones de Anonymous no se mostró muy dispuesta a implicarse en el tedioso trabajo de análisis de los datos, los cuales, en muchos casos, requerían de una elevada cualificación y experiencia para hacer inteligibles dichos documentos. Otro problema añadido era la necesidad de contar con estructuras permanentes de coordinación que fuesen capaces de explotar un conocimiento multidisciplinar que se encontraba disperso. Se trataba, por tanto, de un tipo de organización que chocaba con la propia filosofía antijerarquías del movimiento y que ponía en peligro el anonimato de sus miembros.

Bajo la estela de Anonymous

El principal legado de Anonymous ha sido el haber convertido al hacktivismo en una práctica popular que trasciende el ámbito *hacker.* El *expertise* técnico fue perdiendo relevancia en este tipo de movimientos[36] a medida que hizo su aparición un tipo de *software* que permitía llevar a cabo acciones disruptivas sin necesidad de conocer lenguaje de programación.

Por otro lado, la información volvió a situarse en el centro de la estrategia hacktivista: mientras que el saboteo de las redes y sistemas de sus objetivos eran acciones de gran visibilidad, no dejaban de ser meras contingen-

[34] ASSOCIATED PRESS. «Anonymous rompe relaciones con Assange y WikiLeaks» [en línea], en *La Voz*. 12 octubre 2012. Disponible en web: http://www.lavoz.com.ar/noticias/tecnologia/anonymous-rompe-relaciones-con-assange-wikileaks.

[35] Norton, Quinn. «Par:AnoIA: Anonymous Launches WikiLeaks-esque Site for Data Dumps» [en línea], en *Wired*. 3 julio 2012. Disponible en web: https://www.wired.com/2012/07/paranoia-anonymous/.

[36] Holt, Thomas J.; Freilich, Joshua D.; Chermak, Steven M. «Exploring the subculture of ideologically motivated cyber-attackers», en *Journal of Contemporary Criminal Justice*, vol. 33, n.º 3, pp. 212-233.

cias temporales. 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. Para algunas incluso suponía una amenaza existencial debido a los graves perjuicios económicos o personales que estas filtraciones podían causarle por la pérdida de contratos o posibles demandas judiciales por parte de los afectados.

Anonymous puso en evidencia alguna de las contradicciones de la actual sociedad de la información, donde la sobreabundancia informativa y las demandas de transparencia pública, no han anulado la necesidad que tienen las organizaciones de custodiar y mantener alejados del conocimiento público sus datos más sensibles. La acción de un grupo poco sofisticado demostró lo frágil que puede ser la posición de fuerza que ocupan algunas grandes corporaciones e instituciones públicas. La pérdida de control sobre su propia información, bien por filtraciones originadas desde dentro o por incursiones externas, puede destruir de manera instantánea 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 de Anonymous que han sido replicadas por otros grupos hacktivistas: la apropiación ilícita y divulgación de información sensible puede convertirse en una vía principal de activismo político.

Durante los últimos años, uno de los principales exponentes de este modelo de hacktivismo antisistema ha sido un actor que opera aparentemente a título individual y que ha ganado un elevado prestigio dentro de la subcultura antisistema debido a su pericia técnica y la cuidada selección de sus víctimas.

Es el caso de Phineas Fhiser, el cual adquiriría fama internacional tras el filtrado masivo de los datos privados de dos controvertidas compañías: Gamma Group[37] y Hacking Team[38]. Con esta acción pretendía desvelar los oscuros negocios de unas empresas de *software* que proporcionaban herramientas de monitorización de las comunicaciones a todo tipo de clientes, incluyendo regímenes dictatoriales que emplean estos recursos para reprimir a disidentes y periodistas críticos. Phineas, que se definía asimismo como «un anarquista revolucionario» que vivía de la ciberdelincuencia porque no tenía «demasiadas opciones para vivir con dignidad dentro del

[37] Cox, Joseph. «A Hacker Claims to Have Leaked 40GB of Docs on Government Spy Tool FinFisher» [en línea], en *Motherboard*. 7 agosto 2014. Disponible en web: https://motherboard.vice.com/en_us/article/z4mzze/a-hacker-claims-to-have-leaked-40gb-of-docs-on-government-spy-tool-finfisher.

[38] Franceschi-Bicchierai, Lorenzo. «The Vigilante Who Hacked Hacking Team Explains How He Did It» [en línea], en *Motherboard*. 15 abril 2016. Disponible en web: https://motherboard.vice.com/en_us/article/3dad3n/the-vigilante-who-hacked-hacking-team-explains-how-he-did-it.

sistema»[39], optó por un modelo más selectivo a la hora de orientar sus ataques. Sus objetivos no solo debían tener un elevado perfil mediático, sino también debían ser fácilmente culpabilizados desde la óptica de este movimiento. Esto le llevó también a publicar trescientos mil correos electrónicos del partido político AKP del presidente de Turquía Tayyip Erdogan,[40] en represalia por los ataques del Gobierno turco a algunas organizaciones kurdas de ideología anticapitalista. También filtraría la identidad de 5540 miembros de la policía autonómica catalana alojados en los servidores del sindicato policial SME como una forma de represalia contra los supuestos abusos policiales y la represión del cuerpo de Mossos d'Escuadra contra el movimiento antisistema en Cataluña[41].

Desde el comienzo de sus actividades, mantuvo una notable actividad comunicativa a través de la administración de perfiles propios en redes sociales, la publicación de un vídeo reivindicativo donde registra de manera didáctica cómo había logrado vulnerar la seguridad de sus objetivos y la concesión de entrevistas a periodistas. Sin embargo, su principal contribución a la promoción del hactivismo antisistema fue la publicación de dos manuales[42] con instrucciones detalladas para que cualquier activista pudiese imitar sus acciones de hackeo contra otros objetivos.

El carácter quirúrgico de sus acciones, junto a una mayor sofisticación ideológica y seriedad sobre las causas de su activismo[43], le otorgaron una autoridad entre la subcultura *hacker* mucho más elevada que la que fue capaz de cosechar Anonymous.

Sin embargo, la aparición de Phineas en el universo hacktivista fue tan repentina como su desaparición. A comienzos de 2017 tuvo lugar una operación policial en España contra tres individuos a los que se atribuía la respon-

---

39 Franceschi-Bicchierai, Lorenzo. «Hacking Team Hacker Phineas Fisher Is Taking a Break Because of Stress» [en línea], en *Motherboard*. 9 febrero 2017. Disponible en web: https://motherboard.vice.com/en_us/article/xy5enw/hacking-teams-phineas-fisher-will-return-but-only-after-a-break-at-the-beach.

40 Franceschi-Bicchierai, Lorenzo. «Notorious Hacker 'Phineas Fisher' Says He Hacked The Turkish Government» [en línea], en *Motherboard*. 21 julio 2016. Disponible en web: https://motherboard.vice.com/en_us/article/yp3n55/phineas-fisher-turkish-government-hack.

41 Cox, Joseph. «A Notorious Hacker Just Released a How-To Vídeo Targeting Police» [en línea], en *Motherboard*. 19 julio 2016. Disponible en web: https://motherboard.vice.com/en_us/article/vv77y9/phineas-fisher-sme.

42 «Hack Back! A DIY Guide». Disponible en web: https://pastebin.com/0SNSvyjJ; «A DIY Guide for those without the patience to wait for whistleblowers». Disponible en web: https://pastebin.com/BMb543G9.

43 Franceschi-Bicchierai, Lorenzo. «A Notorious Hacker Is Trying to Start a 'Hack Back' Political Movement» [en línea], en *Motherboard*. 23 mayo 2016. Disponible en web: https://motherboard.vice.com/en_us/article/qkjjnb/notorious-hacker-phineas-fishers-is-trying-to-start-a-hack-back-political-movement.

sabilidad de la filtración de los afiliados al sindicato de Mossos[44]. Aunque se especuló con la posibilidad de que entre los detenidos se encontrase el misterioso Phineas Fhiser, este reaparecería en Internet para negar que hubiese sido apresado. A pesar de ello, eliminaría repentinamente sus perfiles en redes sociales e interrumpiría su actividad de hackeo para tomarse un «descanso», como declararía a un periodista. Según esto, su elevado perfil público y, por motivos de seguridad, la necesidad de mantener una doble vida, le habían causado algún tipo de depresión/estrés de la cual esperaba recuperarse. Ante la pregunta del periodista sobre si podía considerarse que Phineas Fhiser había muerto, el respondió: «No. Las palabras viven para siempre. Mientras que alguien lea los manuales y se sienta inspirado, seguirá vivo»[45].

Hacktivismo yihadista

Entre el heterogéneo catálogo de usos que el terrorismo yihadista hace de Internet también podemos encontrar el recurso del hacktivismo. Un amplio elenco de siglas y actores individuales han recurrido al *hacking* para apoyar los objetivos y tácticas de estas organizaciones.

Este ha sido el principal fruto de su llamamiento para que sus seguidores saquen partido a las potencialidades del ciberespacio en beneficio de la yihad. Así, por ejemplo, en un vídeo de 2011 elaborado por Al Qaeda con el título *No confíes en otros, toma la responsabilidad por ti mismo*[46], se incitaba a que cualquier musulmán con conocimientos especializados llevase a cabo «en armonía con el plan general de los muyahidín [...] ataques contra los *websites* y las redes electrónicas de las grandes empresas y las administraciones públicas de los países que atacan a musulmanes [...]».

Los foros yihadistas de Internet han sido el principal espacio donde los partidarios de estos grupos han depositado sus esperanzas en que el ciberespacio se convirtiese en el arma definitiva que les permitiría alterar la balanza de fuerzas y vencer así a enemigos mucho más poderosos. Alguno de estos internautas llegó incluso a especular con la posibilidad de que un cibersa-

[44] Borràs, Enric. «Els Mossos arresten tres persones per la filtració de dades personals 5.540 policies» [en línea], en *ARA*. 1 febrero 2017. Disponible en web: https://www.ara.cat/societat/Arresten-persona-filtracio-mossos-desquadra_0_1733826703.html.

[45] Franceschi-Bicchierai, Lorenzo. «Hacking Team Hacker Phineas Fisher Is Taking a Break Because of Stress» [en línea], en *Motherboard*. 9 febrero 2017. Disponible en web: https://motherboard.vice.com/en_us/article/xy5enw/hacking-teams-phineas-fisher-will-return-but-only-after-a-break-at-the-beach.

[46] JIHADOLOGY. «As-Saḥāb Media presents a new vídeo message from al-Qā'idah: "For Incitement and Publishing: You Are Held Responsible Only for Yourself, Parts 1 and 2"» [en línea], 3 junio 2011. Disponible en web: http://jihadology.net/2011/06/03/as-sa%E1%B8%A5ab-presents-a-new-vídeo-message-from-al-qa%E2%80%99idah-thou-are-held-responsible-only-for-yourself-parts-1-2/.

botaje contra Estados Unidos diese como resultado el lanzamiento remoto de alguna de sus armas nucleares contra China o Rusia, y que esto fuese el inicio de una guerra que terminaría exterminando a los «enemigos del islam»[47]. A pesar de esas reflexiones en «voz alta», lo cierto es que estos llamamientos no han logrado que ningún partidario con las capacidades necesarias atendiese esta llamada y protagonizase algún acto de ciberterrorismo en sentido estricto. Sí que se ha producido, por el contrario, la activación de ese otro activismo que, aun siendo muy modesto desde el punto de vista técnico, ha generado unos cuantiosos resultados en términos de publicidad y generación de miedo entre sus víctimas.

Es muy significativo que el primer registro existente sobre el uso de Internet desde una perspectiva ofensiva por parte de un yihadista se pueda catalogar como un acto de hacktivismo. Este es el caso del juicio en Estados Unidos contra el mauritano Mohamedou Ould Slahi[48], un reclutador de Al Qaeda, con experiencia profesional como administrador de sistemas. Según relataría, la organización de Bin Laden llevó a cabo una serie de ciberataques contra redes informáticas gubernamentales en el año 2001. Sin embargo, dichas operaciones se limitaron al sabotaje temporal de páginas web públicas (como la del primer ministro israelí) a través de los llamados *ataques de denegación de servicio*.

A pesar de la existencia a lo largo del tiempo de numerosos incidentes de hacktivismo yihadista, el fenómeno no alcanza su eclosión hasta fechas más recientes. Se trata de un fenómeno tardío que obedece a dos factores principales: su inspiración en el exitoso modelo Anonymous, el cual sería el detonante de un considerable movimiento de hackitivismo pro-alestino en países de mayoría musulmana, y la capacidad del grupo terrorista Estado Islámico para conectar con una nueva generación de partidarios que se desenvuelven con mayor comodidad en el activismo virtual.

Algunos internautas que simpatizaban con el ideario y métodos del terrorismo yihadista extrajeron de la experiencia de Anonymous unas valiosas lecciones sobre cómo alcanzar una elevada notoriedad en los medios de comunicación, pero también cómo era posible importar ese modelo de compromiso de «baja intensidad» con una causa, lo que permitía extender el abanico de contribuciones a la yihad al ámbito del *hacking*.

Este tipo de conexiones entre la subcultura antisistema y la yihadista no solo se han producido en el plano del aprendizaje vicario, sino que también es

---

47 Torres, Manuel R. «Cómo contener a un califato virtual» [en línea], en Jordán, Javier. (coord.) *Estrategias para derrotar al Dáesh y la reestabilización regional*. Madrid: Ministerio de Defensa, 2016. Disponible en web: http://www.ieee.es/publicaciones-new/cuadernos-de-estrategia/2016/Cuaderno_180.html.

48 THE NEW YORK TIMES. «Mohamedou Ould Slahi» [en línea], en *The Guantánamo Docket*. Disponible en web: https://www.nytimes.com/interactive/projects/guantanamo/detainees/760-mohamedou-ould-slahi.

posible detectarlas en el perfil biográfico de algunos de sus protagonistas. El caso más destacado es el del británico de origen pakistaní Junaid Hussain. Siendo un adolescente creó junto a un amigo un grupo denominado Team Poison que tendría una clara orientación propalestina. A través de su apodo *Trick* se movería en la órbita de Anonymous, un colectivo con el cual compartiría varias ofensivas de *hacking* como Operation Free Palestine[49], que apuntó hacia el sistema financiero de Israel en 2011. Team Poison reivindicaría un buen número de acciones de un considerable impacto mediático, como la filtración de datos provenientes de políticos e instituciones gubernamentales. En 2012 sería condenado a seis meses de prisión por el hackeo de la agenda de contactos del asistente del primer ministro británico Tony Blair, así como por realizar más de cien bromas pesadas en la línea de teléfono habilitada por el Gobierno para recibir denuncias contra individuos relacionados con actividades terroristas.

Su paso por prisión intensificó la agresividad contra los que consideraba los responsables de un sistema opresivo que se cebaba especialmente contra los musulmanes. El 2014 reaparecería en los territorios dominados por Estado Islámico en Siria. Junaid había decidido sumarse a la causa de este grupo terrorista y marcó un punto de inflexión en su vida. Alteró su perfil en Twitter para adoptar un nuevo nombre de guerra, Abu Hussain al-Britani, y sustituyó una imagen donde podía verse un niño cubierto con una bandera palestina por una foto personal donde mostraba medio rostro cubierto por un pañuelo mientras apuntaba con un rifle a la cámara. Junaid puso a disposición del grupo sus conocimientos para formar a otros activistas y apoyar las actividades propagandísticas de la organización. Se convertiría asimismo en el operativo más reconocible del grupo más importante del hacktivismo yihadista, el Cibercalifato, el cual protagonizaría varias operaciones de gran resonancia como el hackeo del perfil en Twitter del Comando Central del Ejército de los Estados Unidos (CENTCOM). En paralelo, también lideró otra nueva denominación del hacktivismo yihadista bajo el nombre de Islamic State Hacking Division (ISHD)[50].

Junaid trató de potenciar las actividades de su nuevo grupo rentabilizando su antigua red de contactos entre el hacktivismo antisitema. Uno de los pocos activistas que aceptó su oferta fue el kosovar Ardit Ferizi[51], líder de un

[49] ANNONYMOUS. «A message from Anonymous to the Israeli government and the Zionist establishment» [en línea]. Disponible en web: https://www.anonymous-france.eu/anonymous-operation-free-palestine.html.

[50] Franceschi-Bicchierai, Lorenzo. «How a Teenage Hacker Became the Target of a US Drone Strike» [en línea], en *Motherboad*. 28 agosto 2015. Disponible en web: https://motherboard.vice.com/en_us/article/jp5wed/junaid-hussain-isis-hacker-drone.

[51] Varandani, Suman. «Who Is Ardit Ferizi? Malaysia Arrests Kosovo National For Hacking US Security Data For ISIS» [en línea], en *International Bussines Times*. 16 octubre 2015. Disponible en web: http://www.ibtimes.com/who-ardit-ferizi-malaysia-arrests-kosovo-national-hacking-us-security-data-isis-2143489.

grupúsculo denominado Kosova Hacker's Security. El yihadista le encargó la obtención de un listado con información personal de militares y funcionarios estadounidenses. El kosovar le facilitaría más de mil datos de contacto, los cuales fueron difundidos en Internet por Cyber Caliphate junto a un llamamiento público para que fuesen asesinados. La pobre diligencia técnica[52] de Ferizi facilitaría su detención poco tiempo después.

Abu Hussain al-Britani no solo sería conocido por su faceta virtual, sino que también protagonizaría una intensa actividad destinada a alentar la realización de atentados en Occidente por parte de musulmanes radicalizados con los que había entrado en contacto a través de Internet[53].

El 24 de agosto de 2015, el disparo de un dron militar de los Estados Unidos acabaría con su vida en la ciudad siria de Raqqa. Tras su muerte, varios colectivos de *hacker* opuestos a Estado Islámico (entre los que se encontraban antiguos camaradas de Junaid) se disputaron la responsabilidad de haber desvelado la localización del más famoso ciberactivista de Estado Islámico, haciendo así posible su muerte.

Su desaparición supone una nueva evidencia de la importancia del factor individual en los movimientos hacktivistas. Tras su muerte, Cyber Caliphate cambió su nombre por Islamic Cyber Army; sin embargo, en esta nueva fase se podía apreciar fácilmente una pérdida de capacidades en cuanto a sus procedimientos y selección de objetivos[54].

A pesar de ello, el yihadismo continúa siendo uno de los principales motores del hacktivismo. El elemento diferenciador se halla en su vinculación ideológica con los grupos e individuos que emplean la violencia terrorista, lo que otorga un nuevo sentido a muchas de sus actividades. Así, por ejemplo, el robo y difusión de información personal (o *doxxing*) no tiene como finalidad exclusiva atacar la intimidad de la víctima, sino el emplear esa información para crear *kill lists* donde se facilita la localización de personas a las que se presenta como candidatos propicios a ser asesinados. Este tipo de amenazas les otorga una enorme relevancia pública, teniendo en cuenta que se producen en un contexto de elevada ansiedad por la incidencia del terrorismo en todo el planeta. A pesar de que la gran mayoría de las siglas proyihadistas que han emergido en los últimos años carecen de vinculación

---

52 UNITED STATES DISTRICT COURT FOR THE EASTERN DISTRICT OF VIRGINIA. «Criminal Complaint United States of America v. Ardit Ferizi» [en línea]. Disponible en web: "https://www.justice.gov/opa/file/784501/download.

53 NEWSWEEK. «Junaid Hussain: How a Boy From Birmingham Became ISIS's Leading Hacker» [en línea], en *Newsweek*. 27 agosto 2015. Disponible en web: http://www.newsweek.com/janaid-hussain-isis-us-syriabritainisis-cybercyber-caliphateisis-hackermiddle-601034.

54 Murphy, Lorraine. «The Curious Case of the Jihadist Who Started Out as a Hacktivist» [en línea], en *Vanity Fair*. 15 diciembre 2015. Disponible en web: https://www.vanityfair.com/news/2015/12/isis-hacker-junaid-hussain.

efectiva con los grupos que emplean la violencia[55], su adhesión ideológica les ha permitido disfrutar de un acceso a la opinión pública que difícilmente se hubiese dado en otras causas que no estén respaldadas por las armas.

Un análisis detallado de estas «listas»[56] evidencia no solo la existencia de datos «fabricados», sino que en las que son genuinas también se aprecia un pobre bagaje técnico, así como un muy cuestionable criterio de selección de los objetivos. En unos casos, el acceso a este tipo de datos personales se ha logrado a través de simples métodos de ingeniería social a través de la impostación de identidades. En los casos más elaborados, se ha hecho uso de herramientas fácilmente accesibles como Havij u otro tipo de plataformas que automatizan las llamadas *inyecciones SQL*, las cuales permiten capturar los datos de acceso restringido de las webs que presentan graves deficiencias de seguridad[57]. Por otro lado, si en las primeras *kill list* se podía deducir cierta lógica en la culpabilización y en la selección de las víctimas (personal militar, policial, personal gubernamental, etc.), en aportaciones posteriores se incluyó de manera indiscriminada a residentes de cualquier ciudad occidental, por la única razón de que sus datos estaban disponibles de manera semipública en listines telefónicos a los que había tenido acceso estos grupos.

A pesar de este carácter *amateur*, las distintas organizaciones yihadistas no han estado especialmente interesadas en resolver la ambigüedad existente sobre sus posibles vínculos con los grupos de *hackers*. Estos grupos son conscientes de su capacidad para amplificar el terror entre sus enemigos, de ahí que, en vez de aclarar de manera explícita que estos actores no forman parte de su estructura organizativa, han preferido hacerlo de manera más sutil. Así, por ejemplo, Estado Islámico ha hecho varios llamamientos a sus seguidores para que solo atribuyan al grupo la información proveniente de fuentes oficiales y, acto seguido, han informado de cuáles eran esos canales oficiales, entre los cuales no se haya ninguno de los utilizados por estos grupos para divulgar sus mensajes.

El hacktivismo yihadista se mueve en los mismos parámetros culturales que otros grupos de ciberactivismo que recurren a técnicas delictivas, lo que le permite que se produzcan sinergias sorprendentes[58]. Así, por ejemplo,

---

55 King, Meg; Grayson, Clary. «Confronting Terror-affiliated Hacktivists» [en línea], en *Wilson Briefs*. 28 mayo 2015. Disponible en web: https://www.wilsoncenter.org/publication/confronting-terror-affiliated-hacktivists.

56 SITE INTELLIGENCE GROUP. «Kill Lists from Pro-ISIS Hacking Groups» [en línea], en *SITE,* 7 junio 2016. Disponible en web: http://sitemultimedia.org/docs/SITE_Analysis_of_Islamic_State_Kill_Lists.pdf.

57 Bernard, Rose. «These are not the terrorist groups you're looking for: an assessment of the cyber capabilities of Islamic State», en *Journal of Cyber Policy*, vol. 2, n.º 2, 2017, pp. 255-265.

58 Stalinsky, Steven; Sosnow, R. «Hacking In The Name Of The Islamic State (ISIS)» [en línea], en *MEMRI Inquiry & Analysis Series nº 1183*. 21 agosto 2015. Disponible en web: https://www.memri.org/reports/hacking-name-islamic-state-isis#_ednref7.

encontramos grupos que iniciaron su andanza como movimientos antiautoritarios o antisemitas en países de mayoría musulmana, que no poseían ningún objetivo de carácter religioso y que terminaron derivando hacia el hacktivismo yihadista. La estela del «caballo ganador» puede ser un movilizador mucho más importante,que la identificación ideológica o religiosa, especialmente cuando se comparte un mismo conjunto de odios y fobias hacia los que se consideran enemigos. En otros casos, encontramos actores que identifican el yihadismo (y particularmente el Estado Islámico) como una poderosa marca que garantiza impacto mediático y cierta respetabilidad y prestigio a sus acciones individuales de *hacking*. Esto explica, por ejemplo, cómo algunos individuos y grupúsculos de la escena *hacker* en América Latina terminasen orbitando hacia el hacktivismo proyihadista[59].

A pesar de la grandiosidad con la que describen sus capacidades técnicas y objetivos[60], el grueso de sus acciones se ha ceñido a simples ataques en fuerza contra algunas páginas web escasamente protegidas. En ocasiones, sus sabotajes contra aquellos contenidos virtuales que consideran ofensivos desde una perspectiva islámica se han implementado a través de procedimientos carentes de cualquier componente técnico, como la obtención de las contraseñas atacadas a través de ingeniería social o incluso el envío de mensajes amenazantes a las empresas que prestan servicios de alojamiento virtual, para forzarlas a descolgar estos contenidos del ciberespacio. En otros casos, se han limitado a escanear de manera automatizada vulnerabilidades en páginas web que les permitan tomar el control sobre ellas y llevar a cabo acciones de *defacement*, a través de las cuales publicitar las consignas de las diferentes organizaciones yihadistas. Sin embargo, que el principal criterio de selección de la víctima sea su accesibilidad ha llevado a muchos de estos actores a sabotear webs cuyo contenido difícilmente guarda alguna relación con esa supuesta pugna entre el Islam y sus enemigos. Así, por ejemplo, algunas de las víctimas de esta ofensiva han sido restaurantes, gimnasios, colegios o incluso asociaciones de taxistas[61].

Esta selección arbitraria de objetivos ha erosionado el poder coactivo de estos actores, así como su capacidad de concitar la atención de los medios de comunicación de masas. Si bien las primeras acciones obtuvieron un elevado eco mediático, el hacktivismo yihadista terminó agotando rápidamente

---

59 CCN-CERT. «Hacktivismo y Ciberyihadismo Informe Resumen 2016», en *Informe de Amenazas CCN-CERT IA-04/17*. Marzo de 2017.

60 Véase, por ejemplo: https://ia801309.us.archive.org/9/items/MessageToAmerica-MessageFromTheVirtualWorldandEuropeAustralia/Message%20to%20America%20Message%20From%20The%20Virtual%20World%20%28and%20Europe%2c%20Australia%29.mp4.

61 Cembrero, Ignacio. «Un ciberataque yihadista tumba las webs de tres liceos franceses en España» [en línea], en *El Confidencial*. 11 enero 2017. Disponible en web: https://www.elconfidencial.com/espana/2017-01-11/ciberataque-yihadista-liceos-webs-paginas_1314725/.

ese crédito cuando dejaron patente el carácter arbitrario y sin respaldo real de sus amenazas.

Otro elemento que ha minado el crédito de este tipo de actores ha sido su escasa coherencia doctrinal e incluso estética. Su discurso y la simbología están plagados de elementos que entran en contradicción con los planteamientos doctrinales de los grupos a los que pretenden apoyar con sus acciones. En la subcultura del hacktivismo yihadista pesa mucho más la estética que terminaría popularizando Anonymous que el rigorismo de Estado Islámico, el cual cataloga gran parte de esas manifestaciones como influencias pecaminosas ajenas al verdadero islam. Es el caso, por ejemplo, del grupo tunecino denominado Al Fallaga Team, el cual, a pesar de estar alineado con los objetivos del Dáesh, siguió conservando en su emblema la bandera de Túnez. Este símbolo choca frontalmente con el rechazo del salafismo yihadista a la existencia de comunidades nacionales, a las cuales considera una creación de Occidente para dividir y enfrentar a los musulmanes, los cuales forman una única comunidad que debe ser regida bajo la forma del califato.

En las representaciones visuales de estos grupúsculos[62] e individuos no solo es recurrente la máscara del Guy Fawkes, sino otra serie de imágenes aún más problemáticas que la del *merchandaising* moderno de este conspirador católico del siglo XVI: podemos encontrar, por ejemplo, calaveras, fantasmas e incluso demonios. Al mismo tiempo, se obvia la pugna existente entre las organizaciones de Al Qaeda y Estado Islámico, cuyos nombres y símbolos han aparecido de manera indistinta en algunas de estas acciones de sabotaje de páginas web[63].

Otro elemento que ha restado eficacia a la acción comunicativa del hacktivismo yihadista es su carácter disperso: a pesar de compartir objetivos y metodología, los activistas de la yihad cibernética se han empeñado en agruparse en multitud de siglas y alianzas efímeras que dificultan en extremo el acto de catalogar y comprender a sus protagonistas. Para añadir más complejidad, algunos de estos grupos han utilizado de manera indistinta varias combinaciones de un mismo nombre; es el caso de Caliphate Cyber Army (CCA), que también se hacía llamar Islamic Cyber Army o Cyber Caliphate. Han creado nuevas marcas que supuestamente fusionaban grupos preexistentes, lo cual no implicaba que sus componentes no siguiesen existiendo y actuando a título individual. Es el caso de United Cyber Caliphate (UCC), presentado públicamente en abril de 2016 cómo la unión de tres grupos: Kalachnikv E-security Team, Sons Caliphate Army y Ghost Caliphate Section. Cuando se han agregado o escindido a título individual algunos de estos grupos, nunca ha quedado claro cuáles son los factores que motivaban estos

[62] Véase, por ejemplo: ICT Cyber-Desk. «Cyber-Terrorism Activities Report No. 15» [en línea]. 2015. Disponible en web: https://www.ict.org.il/UserFiles/ICT-Cyber-Review-15.pdf.

[63] Es el caso, por ejemplo, de un grupo autodenominado Al Qaeda Electronic Base, el cual empleaba como símbolo la bandera de Estado Islámico. Veáse: https://justpaste.it/qe_b2.

continuos movimientos de refundación, unión o separación. Desde la óptica de un observador externo, era inevitable percibir el hacktivismo yihadista como un ámbito dominado por las rivalidades individuales, la incapacidad de cooperar y la inmadurez de sus protagonistas.

Conclusiones

En el ámbito de la ciberseguridad estamos viviendo un momento de «cierre de etapa». Gran parte de las acciones de *hacking* que se han producido en los últimos años ha sido posible no tanto por la sofisticación técnica de sus autores, sino por la falta de preparación y las inadecuadas defensas de sus víctimas. Dicha ventana de oportunidad ha sido explotada con escasa discreción por parte de actores públicos y privados, lo que ha terminado generado entre sus víctimas una respuesta de adaptación que está limitando su efectividad. A medida que Internet se vaya «endureciendo» como objetivo, los grupos que recurren al hacktivismo tendrán que innovar en sus procedimientos para seguir obteniendo relevancia mediática.

Sin embargo, este cambio no supondrá el fin de las grandes filtraciones de datos ni de los sabotajes virtuales. Aunque estos resultados resulten más difíciles de alcanzar desde un punto de vista técnico, es previsible que se produzca una mayor implicación en términos de esfuerzo por parte de los protagonistas, sobre todo en la medida en que el activismo politico convencional parezca cada vez más ineficaz frente a otras modalidades transgresoras que obtiene un impacto mediático mucho más elevado.

El futuro del hacktivismo está intimamente vinculado al cambio tecnológico y a su recepción por parte de la sociedad. Si por un lado una mayor concienciación pública sobre la necesidad de la ciberseguridad hará obsoletos algunos de los procedimientos tradicionales, debe contemplarse la posibilidad de que la irrupción de nuevas tecnologías abra nuevas ventanas de oportunidad. Ese es el escenario que podría plantearse como consecuencia de la popularización de aplicaciones basadas en inteligencia artificial, las cuales pueden hacer viables determinados objetivos y procedimientos que hasta ahora no han sido asumibles por su elevado coste en términos de movilización de recursos humanos o por la necesidad de conocimiento especializado[64].

Es el caso, por ejemplo, de los engaños individualizados a través de la suplantación de identidad (*spear phishing attacks*) con el propósito de acceder a información confidencial. El éxito de estos ataques depende de una considerable inversion de tiempo y esfuerzo para poder identificar así el objetivo,

[64] Brundage, Miles et al. «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» [en línea], en *Future of Humanity Institute- Oxford University*. Febrero 2018. Disponible en web: https://maliciousaireport.com/.

su red social y el contexto en el cual la víctima daría credibilidad y estaría dispuesta a aceptar una petición que la sitúa en una situación de vulnerabilidad. La considerable inversión en tiempo y esfuerzo que debe realizarse para hacer viable este tipo de engaños explica que hasta el momento se haya reservado a objetivos de alto valor. Sin embargo, la inteligencia artificial puede hacer posible que las tareas de investigación del objetivo puedan ser automatizadas, lo que reducirá drásticamente el coste de este tipo de prácticas. Como resultado, se podrá lanzar de manera indiscriminada este tipo de ataques sin que por ello resulten menos eficaces.

Sin embargo, el principal reto al que tiene que enfrentarse el hacktivismo no es tanto la viabilidad de sus operaciones de hackeo, sino cómo conciliar su vertiente colectiva con la individualidad de sus miembros.

Uno de los principales activos propagandísticos de estos actores es el hecho de que sean percibidos por la sociedad como movimientos capaces de movilizar a un elevado número de activistas. Su discurso alcanza una resonancia distinta cuando su público interpreta que tras las palabras se encuentra una masa amorfa de entusiastas expertos informáticos a los que resulta imposible descabezar. Sin embargo, esta imagen no hace justicia a la realidad del hacktivismo, donde los números no solo son mucho más reducidos, sino donde las individualidades dificultan la capacidad de estos movimientos de actuar como un actor homogéneo. Muchos de los miembros que se suman a estas formaciones lo hacen desde una trayectoria previa, portando consigo una reputación individual de dominio técnico, osadía o compriso. Se trata de un patrimonio inmaterial del cual muchos no quieren desprenderse, sobre todo, si entiende que su militancia en estos proyectos es solo temporal. De ahí que cuando estos grupos reivindican sus acciones sea frecuente que, junto con el nombre del grupo, aparezcan también mencionados los seudónimos de sus activistas que han llevado a cabo la acción, los cuales no están dispuestos a perder la oportunidad de incrementar su reputación. Esto no solo es una contradiccion en los términos para movimientos que, como Anonymous, hacen bandera de cómo sus integrantes conforman una mentalidad colectiva, sino también para el hacktivismo yihadista, el cual tiene dificultades para presentarse como la vanguardia tecnológica de los muyahidín, sobre todo si el ego y el deseo de visibilidad de sus integrantes eclipsa al propio grupo.

En definitiva, la viabilidad futura del hacktivismo dependerá no tanto de su eficacia mediática, la cual ha quedado demostrada a lo largo de los últimos años, sino de la capacidad de sus protagonistas para superar los considerables desafios organizativos. En la medida en que movimientos de hacktivismo actuales y futuros consigan coordinar y dar coherencia a este heterogéneo colectivo, hablaremos de actores con capacidad real de influencia o de meras erupciones temporales sin impacto en la realidad.