EL EJÉRCITO ‘PIRATA’ DE CHINA

Mara Hvistendahl

El mito de una ciberguerra china monolítica está empezando a desmontarse. Eche un vistazo al mundo abarrotado y caótico de* hackers *patrióticos chinos.

La autobiografía del pirata informático (*hacker*) SharpWinner empieza con un grupo de jóvenes en un apartamento lleno de humo de cigarrillos, en una ciudad anónima de algún lugar de China. La piratería es un trabajo cansado, y este grupo concreto, uno de los centenares que hay por todo el país, lleva horas dedicado a ello. Pero el líder del grupo, un “joven guapo e inteligente” -en todo el relato de *The Turbulent Times of the Red Hackers* [La turbulenta época de los piratas rojos], SharpWinner se refiere a sí mismo en tercera persona-, es imperturbable. Después de introducirse de tapadillo en una web japonesa, hace una pausa para responder a mensajes de texto de admiradoras.

AFP/Getty Images

Sería fácil considerar que SharpWinner, que ha promovido su libro en la televisión nacional y asegura que está negociando un contrato de derechos cinematográficos, no es más que un hombre que recurre a los golpes de efecto para llamar la atención. Y la noticia de que Google y docenas de otras empresas habían sufrido este invierno un gigantesco ataque procedente de China hizo pensar en el brazo fuerte del Gobierno chino, no en el mundo amorfo de piratas informáticos de SharpWinner. El gigante de Internet dijo que la decisión de hacer pública la

información sobre Operación Aurora, nombre que se ha dado a la acción pirata, estaba relacionada “con un debate mundial, mucho más amplio, sobre la libertad de expresión”. El espionaje por parte del Gobierno chino de las cuentas de correo electrónico de activistas de los derechos humanos, insinuó Google, fue uno de los motivos por los que amenazó con retirarse del *gigante asiático* (una amenaza que todavía está por cumplir).

Sin embargo, un informe hecho público recientemente por la empresa de seguridad de Atlanta Damballa dice que el ataque de Aurora parece ser obra de aficionados que trabajan con herramientas poco sofisticadas. Esa revelación, unida a una información de *The Financial Times* de que el código Aurora está escrito por alguien que trabaja por su cuenta, ha hecho que se preste más atención a la red de piratas informáticos independientes de China. Y SharpWinner -jefe de una coalición de entre 50.000 y 100.000 miembros y, antes de desaparecer de la vida pública en 2007, un participante habitual en los conflictos cibernéticos internacionales, entre ellos la guerra de *piratas* informáticos de 2001 que se extendió desde China hasta la Casa Blanca- no es más que el comienzo.

Los ataques de Aurora fueron un intento, por parte de piratas aparentemente establecidos en China, de robar información valiosa de grandes compañías estadounidenses. (Hasta ahora, la lista de víctimas incluye Adobe Systems y Dow Chemical, además de Google*. Durante el fin de semana, un investigador especializado en seguridad declaró a *Computerworld* que es posible que Aurora haya penetrado en más de 100 empresas.) Los investigadores están todavía tratando de comprender de dónde surgió Aurora y qué significa, pero ya han aparecido algunas pistas sorprendentes. El reportaje de *The Financial Times* apareció justo después de una información de *The New York Times* según la cual los investigadores han descubierto que los ataques se originaron en dos universidades chinas, una de las cuales es, desde hace mucho tiempo, un campo de entrenamiento para *hackers* independientes o *patrióticos*. Una de las cosas que se deduce de estas informaciones es que el conocimiento que tiene Estados Unidos sobre la piratería china está muy anticuado.

Las noticias aparecidas en los medios de comunicación occidentales suelen pasar por alto a los independientes y, en cambio, hacen mucho ruido sobre el Gobierno chino. Algunos conjugan relatos entrecortados de ciberguerra con imágenes extraídas de la propaganda del Ejército Popular de Liberación en los 60, como si quisieran sugerir que China posee una oficina cibernética centralizada que alberga un ejército de piratas informáticos profesionales. Hace dos años, un reportaje de portada del *National Journal* afirmó que los *hackers* habían sido responsables del apagón que dejó sin luz en 2003 a gran parte del nordeste de Estados Unidos, un suceso que repetidas investigaciones han atribuido a la negligencia local.

En realidad, el mundillo de la piratería informática en China consiste más bien, probablemente, en unos cuantos agentes de los servicios secretos que supervisan a un grupo de *hackers* patrióticos, llenos de talento y a veces incontrolables. Desde los 90, Pekín cuenta con un programa de sus servicios de inteligencia encargado de la tecnología extranjera, dice James A. Lewis, investigador de seguridad cibernética y política de Internet en el Centro de Estudios Estratégicos e Internacionales. Ahora bien, más allá de eso, las cosas se complican. “El mundo de la piratería informática puede ser caótico”, dice. “Hay muchos actores, algunos dirigidos por el Gobierno y otros tolerados por él. Entre ellos puede haber organismos civiles, empresas e individuos”.

Para cualquiera que hable chino, ese caos es evidente. Si se buscan en Google los caracteres de *heike* -una transliteración de *hacker* que significa literalmente “invitado negro”-, se obtienen páginas y páginas de resultados. Webs como www.chinahacker.com, www.cnhacker.com y www.hackbase.com contienen instrucciones detalladas, anuncios de seminarios en los que aprender –“¡hágase pirata informático en unas semanas!”- y fotos de víctimas extranjeras. Pero está claro que no son obra del Gobierno central. Si se sigue leyendo (más vale no hacerlo, las páginas están llenas de virus y los usuarios corren peligro si entran en ellas), se encuentran hilos de discusión llenos de luchas enconadas, comentarios groseros y fotos de mujeres escasas de ropa.

“Existen centenares de páginas de ésas”, dice Scout Henderson, un especialista en inteligencia y antiguo lingüista del Ejército estadounidense que ha escrito un libro sobre los *piratas* chinos. “Todos tienen sus propias agendas y su propio personal. No está coordinado, no están todos juntos en una sala con alguien que dice ‘Tú escribe este código, tú, este otro’”.

Más bien, los *hackers* en China surgen de manera orgánica. Si a eso se unen el extenso nacionalismo juvenil y el gran porcentaje de población que utiliza la Red -China presume de tener el mayor número de usuarios de Internet en el mundo, 384 millones de personas conectadas-, el resultado es la piratería patriótica. Los autodenominados “piratas rojos” son producto de que “vivimos en una época en la que nuestro país avanza hacia la prosperidad”, dijo una vez SharpWinner, con bastante razón. La prosperidad garantiza asimismo un mercado en el que comercializar numerosos artículos relacionados con la piratería: revistas, camisetas y libros reveladores como el de SharpWinner. En una ocasión, de viaje por la China rural, encontré en una tienda de un pueblo unas latas de caramelos de marca Pirata.

Cada mes de agosto, los *hackers* más destacados se reúnen en Pekín y celebran una conferencia en teoría sobre seguridad informática pero, según un participante, llena de seminarios sobre técnicas de ataque y consejos. La élite de los piratas informáticos chinos

Ahora bien, el hecho de que los intereses de estos piratas se superpongan con la política china no significa que actúen en nombre de Pekín

incluye a divos extravagantes como SharpWinner, Sunwear, un veinteañero menudo y con aspecto travieso que incluye en sus ataques a páginas con la inocua posdata “¡lo hago por divertirme!”, y Xiao Tian, la inalcanzable *femme fatale* que dirige el Equipo de Seguridad Femenino de China. Muchas de las causas que adoptan se solapan con los intereses del Gobierno chino. Por ejemplo, uno de los acontecimientos que impulsó el desarrollo de la cultura *hacker* en el Imperio del Centro fue el bombardeo de la embajada china en Belgrado por parte de la OTAN en 1999. En represalia, los piratas invadieron la web de la embajada estadounidense en Pekín con la exclamación “¡Abajo los bárbaros!” Otro ejemplo: el ataque contra cuentas de correo de la Save Darfur Coalition, que se opone a la intervención del *gigante asiático* en Sudán, en 2008. Otro: GhostNet, la operación de *ciberespionaje* surgida de China que, según se reveló el año pasado, infectó 1.295 ordenadores de 103 países, entre ellos la red del Dalai Lama en Dharamsala, India. Los investigadores de la Universidad de Toronto que descubrieron el ataque no han identificado aún a sus organizadores, pero en un informe dijeron que la operación podía muy bien ser obra de *hackers* patrióticos que hubieran utilizado “inteligencia de señales casera”.

Ahora bien, el hecho de que los intereses de estos piratas se superpongan con la política china no significa que actúen en nombre de Pekín, y muchas de sus actividades sugieren que no hay ninguna interferencia oficial. “Los Gobiernos no se apoderan de *botnets* de ordenadores infectados para realizar ataques de denegación de servicio”, dice Dorothy Denning, profesora de análisis de defensa en la Escuela Naval de Postgraduados de Monterey, California. Sí ayuda que Pekín haga la vista gorda. Existe una norma no escrita que dicta que los *hackers* independientes pueden campar a sus anchas mientras ataquen páginas y empresas extranjeras. Cuando se dirigen contra webs chinas, el Gobierno los reprime. Para un pirata interesado en sobrevivir, la elección está clara.

Otra parte del trato parece ser que permanezcan a disposición de las peticiones del Gobierno. Si las informaciones de *The Financial Times* son ciertas, la Operación Aurora se llevó a cabo con un código desarrollado por un asesor de seguridad de Internet, un treintañero independiente, sin que el Gobierno le dijera nada. Según la fuente del periódico, que dicen que es un investigador del Ejecutivo estadounidense, el pirata se limitó a colgar un trozo del código en un foro de piratas desde el que se abrió paso hasta caer en manos del Gobierno chino. “Prefiere no tener a unos tipos de uniforme mirando todo lo que hace, pero es imposible que alguien con su talento pueda evitar una cosa así”, dice el investigador.

El resto de la historia se aclarará probablemente en los próximos meses. Pero otras informaciones dicen que los ataques se originaron en servidores de la Escuela de Ingeniería de Seguridad Informática de la Universidad Jiao Tong de Shanghai, una de las principales

facultades de informática chinas y un semillero de *hackers*. Desde hace años, sus estudiantes son libres de organizar grupos de piratas e intercambiar historias en foros albergados por la web de la facultad. En 2001, el graduado de Jiao Tong y veterano *hacker* Peng Yinan organizó una reunión informativa titulada “El pirata informático en pocas palabras” en una sala de conferencias de la escuela. La presentación de PowerPoint con la que habló -que, hasta hace poco, podía descargarse de la web de su grupo, aunque ahora la han retirado- glorificaba la cultura *hacker* y explicaba una serie de técnicas que pueden intentarse en casa; asimismo destacaba que unos periodistas de *The Chicago Tribune* revelaron en una ocasión los datos de contacto de miles de agentes de la CIA utilizando un servicio *on line* básico. Un folleto que anunciaba el acto decía que Peng era asesor de la Oficina de Seguridad Pública de Shanghai. Otro estudiante cuyo apodo aparece en los ataques piratas de Peng -pero que me dijo que no había participado- fue luego a trabajar a Google.

¿Puede ser que la Operación Aurora la diseñara un pirata independiente y luego un funcionario la adoptara y la reasignara a otro independiente vinculado a Google? Por lo menos, es una posibilidad digna de tenerse en cuenta. Algunos dicen que el Gobierno chino debería tener unos medios de adquisición de inteligencia más eficaces que unos estudiantes y unos *frikis*. Pero otros explican que la estrategia descentralizada le va muy bien a Pekín. “Son evidentes las ventajas de que haya unos límites borrosos”, dice Lewis. “Los rusos lo hacen todo el tiempo con Estonia: ‘Por supuesto que no fuimos nosotros. ¿Pueden demostrar que fuimos nosotros?’”

Al final, que haya una vaga conexión entre los servicios de inteligencia de Pekín y los piratas patrióticos es más inquietante que si la relación fuera mayor. Los Gobiernos están sujetos a restricciones. Unas bandas de jóvenes -como ha aprendido Estados Unidos a su pesar-, no. “Desde luego, si es una guerra cibernética patrocinada por el Gobierno, tengo alguien a quien puedo disuadir”, explica Henderson. “Si se trata de una destrucción mutua *on line*, por lo menos puedo elaborar una teoría al respecto. Pero cuando son internautas descontrolados, es muy difícil. Pueden ser muy peligrosos”.

La idea halagaría a SharpWinner. En su aparición televisiva, contó su preocupación por la cultura *hacker* en China. Había sido testigo de la desintegración de varios grupos importantes y le inquietaba que muchos patriotas sólo se apunten cuando estalla algún incidente internacional pero luego dejen en paz a las empresas extranjeras cuando la situación se enfría. Sin embargo, con un poco de esfuerzo, concluyó, era posible superar esas dificultades, y dijo que le animaba ver un reciente despertar del interés por la piratería informática. Luego se dirigió a los espectadores. “Hermanos”, dijo, “¡venid conmigo! ¡El futuro de la piratería roja es brillante!”

**La versión original de este artículo citaba unas informaciones de que RAND Corporation había sufrido un ataque de Aurora. Un portavoz de RAND escribió para decir que "RAND no ha sufrido ningún ataque; no tenemos pruebas de ataques ni de que Aurora nos haya agredido".*

Fecha de creación
10 marzo, 2010