vida&artes

sociedad

Holanda planea pagar por abusos prescritos del clero

Nadie está a salvo de esta ciberguerra

- Ataques a favor y en contra de Wikileaks desestabilizan la Red
- En nombre de la libertad se puede caer en la censura masiva

ROSA JIMÉNEZ CANO

El término parece propio de la ciencia ficción: ciberguerra. Pero los bandos están muy definidos. Por un lado, Wikileaks, la web que ha difundido las filtraciones de documentos secretos de EE UU, ha recibido constantes ataques que le han obligado a trasladar el servicio a nuevos servidores; por el otro, las empresas que han roto con la web sufren las iras de los numerosos partidarios de Julian Assange, el líder de Wikileaks. Como paradoja en esta guerra, los adalides de la libertad de expresión, que dicen luchar contra la censura, a su vez hacen lo posible para silenciar las páginas de empresas como Visa y MasterCard. Muchos contienen la respiración porque nadie está a salvo de las presiones políticas, pero tampoco de sufrir la ira de los internautas, que no requieren ya grandes conocimientos para participar en las refriegas.

Las declaraciones de John Perry Barlo, cofundador de la Electronic Frontier Foundation, una organización sin ánimo de lucro que trabaja para proteger los derechos civiles y la libertad de expresión en el mundo digital, han prendido la mecha: "La primera guerra informática ya ha empezado. El campo de batalla es Wikileaks", escribió en Twitter.

¿Es posible que se dé esta circunstancia? Miguel Suárez, experto en seguridad informática de Symantec, cree que ya estamos inmersos en ella: "Y va a ser mucho más común en los próximos años. De hecho, cada vez es más normal que no solo compañías, sino también los Gobiernos recurran a consultores a la hora de definir los planes de protección de infraestructuras críticas".

"Si se diese una ciberguerra la forma sería diferente y se nos haría entender que la Red es global pero causa efecto local. La estrategia ya no es con un ejército, un mapa y una brújula", indica Antonio Miguel Fumero, investigador de la Universidad Politécnica de Madrid. Opina que todo esto servirá para que los políticos tomen conciencia del nuevo mundo en que viven, aprendan de ello y entiendan que los flujos de la información han cambiado.

Chema Alonso, que se presenta como "un informático en el lado del mal", opina que los Gobiernos se preocupan cada vez más por este factor. Conocido por sus demostraciones públicas, en las que es capaz de entrar en sistemas de seguridad de servicios financieros o cuentas de correo de asistentes al *show,* cree que la Red es un nuevo campo de batalla: "Tendríamos que tener un ejército de Internet, igual que lo hay de tierra, mar y aire".

Tanto Estados Unidos como Israel gastan grandes cantidades de dinero no solo en reclutar expertos sino en adquirir programas para defenderse de agresiones. Como es el caso de los programas "día cero" (*0 days* en inglés), cuyos precios pueden superar el millón de euros. Este *software* se introduce en el sistema de la misma manera que lo hacen los troyanos (programas que no parecen nocivos pero lo son), sin que el usuario lo perciba. Su valor reside en que son capaces de entrar en ordenadores con fuerte protección y con los últimos parches de seguridad actualizados.

EE UU ha designado un responsable, el *ciberzar,* cargo que desde la llegada de Barack Obama a la Casa Blanca ostenta Howard Schmidt. Su aterrizaje no es una novedad, pues ya trabajaba como asesor del presidente Bush.

En España existe el Centro Nacional de Protección de Infraestructuras Críticas (CNPIC), que depende del Ministerio del Interior. En opinión de Alonso, aunque el esfuerzo que se hace es loable, falta mucho para llegar al nivel deseable. "En los próximos años los ataques van a ser más frecuentes. No es el mejor momento para pedir inversiones en investigación y tecnología pero lo podemos pagar muy caro. Puede haber, por ejemplo, un pucherazo electrónico en las elecciones, inutilizar autopistas, trenes, aviones...", aventura.

Antonio Miguel Fumero, también socio fundador de la consultora Win Win, cree que la ciberguerra es un término que no viene al caso. "La mitología de los *hackers,* con muchos adeptos en Estados Unidos, con toda su literatura, tiene mucho de romántico pero poco sentido. El problema es cuando se mezclan los mitos con las conspiraciones", explica.

En la última década se han sucedido las guerrillas informáticas entre países. En 2003, Taiwán recibió un supuesto ataque del que siempre culpó a China, sin pruebas, que dejó sin servicio varias infraestructuras básicas como hospitales, la Bolsa y hasta los semáforos. Un caos, ordenado y organizado, que no se limitó a un ataque de denegación de servicio, sino que incluyó virus y troyanos. En 2007, Estonia acusó a Rusia de diversas embestidas que alteraron la normalidad de medios, bancos y estamentos gubernamentales. A finales de septiembre, Irán también registró un intento de agresión a su programa nuclear. El programa que se infiltró recibió el nombre de Stunex. Sin un origen claro, el régimen siempre ha acusado a Estados Unidos de su autoría.

Esta vez los simpatizantes de Wikileaks y defensores a ultranza de Julian Assange decidieron tomar la justicia por su mano. La denominada Operación PayBack, venganza, en inglés, ha decidido atacar en primer lugar a la fiscalía sueca, pero también a MasterCard, Visa y Paypal en primer término. Las tres se negaron a seguir teniendo como cliente la página de filtraciones.

La diferencia entre los *hackers* iniciales y estos activistas es muy clara. En los ochenta y noventa se pretendía alertar a la sociedad de los fallos de seguridad y problemas de privacidad que generaban estos nuevos sistemas informáticos. En la actualidad, los que actúan contra estas máquinas son precisamente los que ponen en peligro la privacidad de la sociedad. Esas causas movieron acciones como los ataques contra los servidores de propaganda serbios en 1998 porque "justificaban crímenes de guerra y decidimos entrar en los servidores y cambiar las imágenes" dice David de Ugarte, miembro entonces del colectivo Cyberpunk.

La ofensiva contra la compañía financiera es similar a la que sufrió la SGAE recientemente: un ataque de denegación de servicio, que consiste en el envío masivo y simultáneo de peticiones a las páginas para bloquear los servidores que las hospedan y sirven.

Luis Corrons, director técnico de PandaLabs, no ve una gran sofisticación en esta forma de actuar. "Casi a diario vemos intentos como estos pero no consiguen su objetivo. Suelen actuar como los gánsteres: chantajean a las empresas a cambio de protección", expone. "La diferencia estriba en que a este colectivo no le motiva el dinero sino sus ideales y eso sí desconcierta a las autoridades".

El grupo activista que promueve la acción es exactamente el mismo: Anonymous. Se organizan a través de un popular foro de entusiastas de la seguridad informática, 4Chan (www.4chan.org). Allí se reúnen varios millones de usuarios y, con un lenguaje propio e incluso un peculiar sentido del humor, debaten cuál será la siguiente víctima.

En su web (http://anonops.net/anonops/Main_Page), que está sufriendo caídas frecuentes, han explicado los motivos y muestran su objetivo en cada momento. El miércoles era MasterCard.

Las claves del duelo en Internet

¿QUIÉNES SON?

▶ **'Hackers'.** Entusiastas de la informática y la seguridad con capacidad para crear programas y entrar en sistemas protegidos. Lo hacen para demostrar conocimientos y vulnerabilidades, pero no tienen ánimo de lucro.

▶ **'Crackers'.** A diferencia de los *hackers* buscan el daño o el lucro a través de sus acciones.

▶ **'Lammers'.** Los que se suman a los ataques masivos. Son los más numerosos y se consideran aprendices. Suelen descargarse programas de otros para dañar sistemas.

TIPOS DE ATAQUE

▶ **'Gusanos'.** Virus que tienen la capacidad de duplicarse a sí mismos y hacer que las máquinas que los hospedan sean cada vez más lentas. Utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

▶ **'Troyanos'.** Como el caballo de Troya, entran sin que se perciba. Aprovechan una puerta trasera para ejecutar programas sin permiso o la entrada remota de intrusos.

▶ **'Ddos'.** Consiste en saturar los servidores que hospedan las páginas webs. Se hacen más peticiones de las que puede soportar. Al desbordarse su capacidad se queda sin servicio.

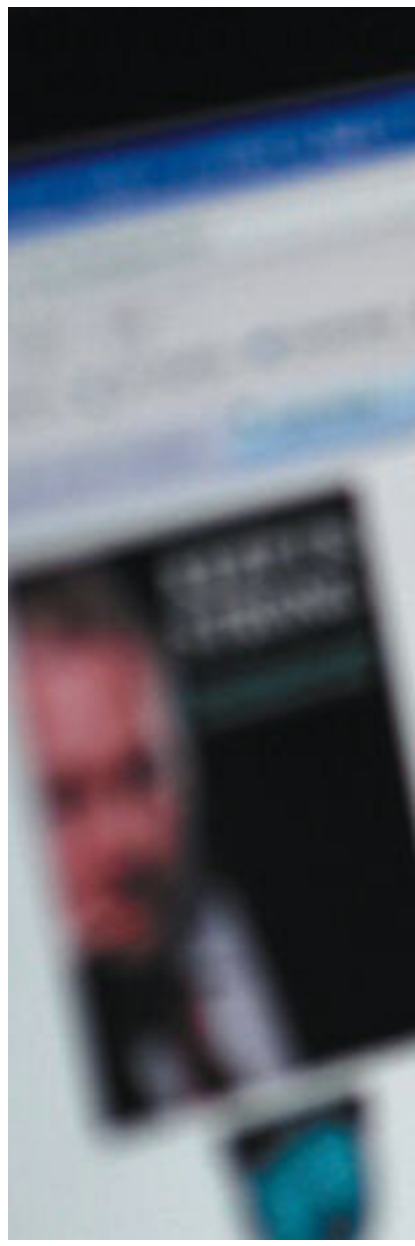
ATAQUES MÁS RELEVANTES

▶ **Septiembre de 2003, en Taiwán.** El Gobierno detectó que varios troyanos procedentes de provincias chinas habían contaminado las redes de 10 compañías privadas.

▶ **Abril de 2007, en Estonia.** El ministro de Exteriores estonio, Urmas Paet, acusó al Kremlin de dejarles sin varios servicios: la Bolsa, hospitales, sitios webs estatales y periódicos.

▶ **Agosto de 2009, en Georgia.** Desde las mismas direcciones IP que se usaron contra Estonia se sabotearon oleoductos.

▶ **Enero de 2010.** Google denuncia el espionaje por China a través de cuentas de correo de periodistas y disidentes.



El romanticismo de los primeros 'hackers' ha quedado atrás

"Falta un ejército de la Red como de tierra, mar o aire", dice un experto

sociedad

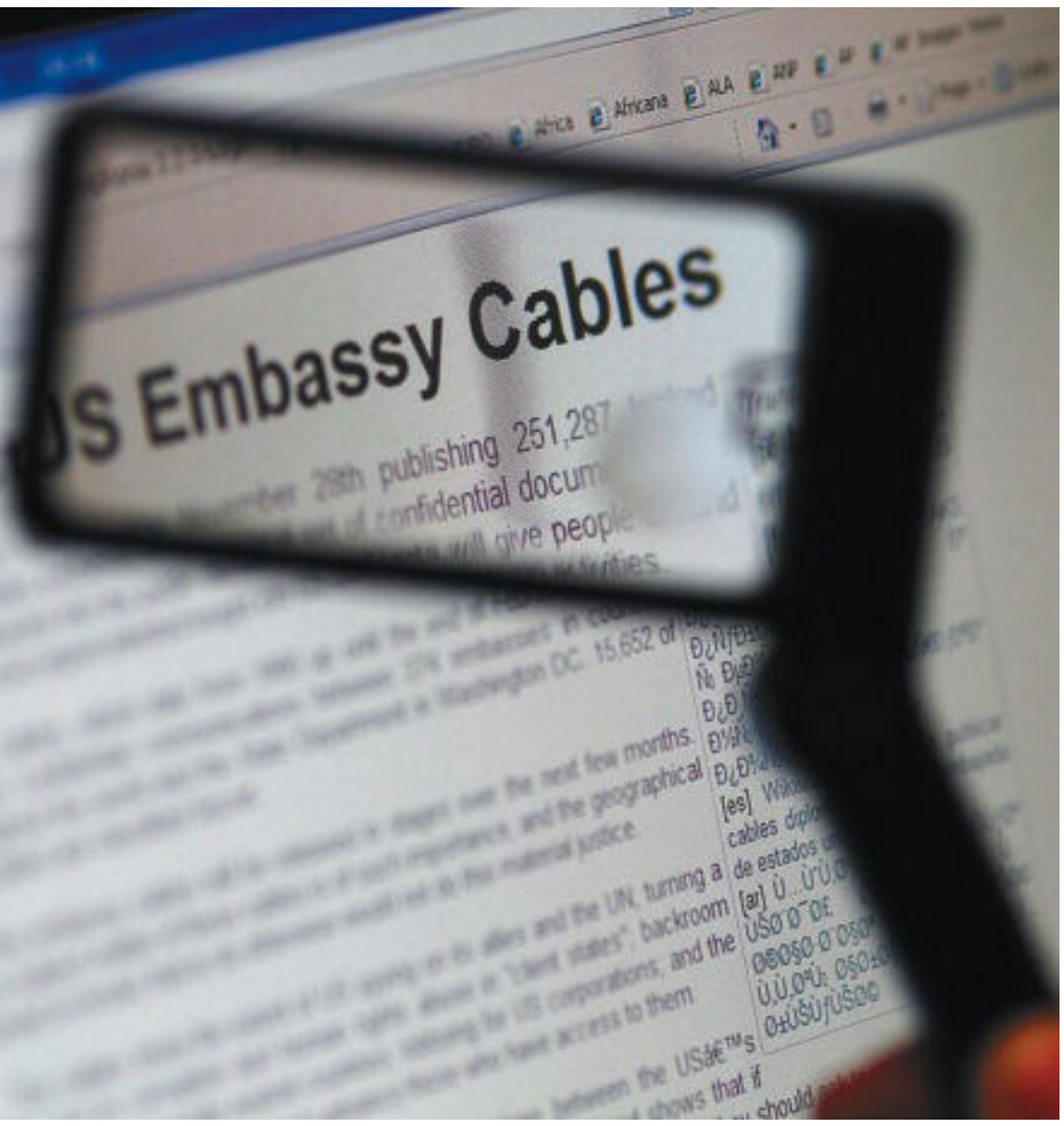
La menor lista de espera quirúrgica: 61 días

cultura

Documenta, las olimpiadas del arte sin concepto

cine

La secuela de la fracasada 'Tron' aspira al taquillazo



La información secreta difundida por Wikileaks y los ataques que sufrió después han agitado la Red. / GETTY

Esa misma noche consiguieron hacer que cayese la página web de Visa. Se quedó varias horas sin página web y muchas más con intermitencias. La compañía ha emitido un comunicado en el que reconoce que "algunos sitios webs de Visa están experimentando un tráfico mayor del habitual, lo que ha dificultado el acceso a los mismos de forma intermitente. Estamos trabajando para solucionarlo y esperamos que el servicio esté restaurado en breve".

Diego Guerrero, autor del libro *Fraude en la Red*, relativiza el efecto de esta caída: "Es publicitario, para hacer ruido. Echan abajo la web de las tarjetas de crédito pero no el servicio en sí, que sería delito. Es decir, la gente puede seguir comprando. Ahora mismo solo generan perjuicio de imagen y económico". En medio de toda esta alarma colectiva este experto llama a la calma: "El nivel de dificultad para entrar en estos servidores es muy elevado. A veces se pueden escapar datos pero penetrar en su sistema es mucho más complejo".

A raíz de que Amazon se negase a hospedar a Wikileaks en sus servidores, la empresa de venta por Internet es el nuevo blanco. La solución a esta supuesta deficiencia se ha encontrado también en la propia Red, los sitios espejo que replican el contenido que no quieren que salga a la luz. Al igual que Paypal, la plataforma dominante en el pago virtual. Mientras que algunos críticos protestan dándose de baja de estos servicios, cada vez son más los que hacen una protesta más agresiva y toman el teclado como arma.

Los seguidores de Wikileaks más molestos con la detención de Julian Assange no cesan de dar enlaces en Twitter con herramientas para que más internautas se sumen a la acción.

José Alcántara, autor de *La sociedad de control* y *La neutralidad de la Red*, cree que estas acciones no las realizan profesionales sino *lammers*, personas sin gran preparación, en muchos casos adolescentes que no saben programar pero sí ejecutar un programa en lenguaje Javascript para hacer un ataque constante y descentralizado. "Crean turbas y, como todo el mundo sabe, con las turbas no se puede argumentar", lamenta.

> Panda denuncia que existen bandas de chantajeadores de empresas

> Adolescentes sin gran preparación pueden participar en sabotajes

En su opinión, las consecuencias de lo que denomina "gamberrada" va a costar muy caro: "Nos jugamos batallas como la neutralidad de la Red. Un uso irresponsable de su poder, como es el caso, no hace más que dar motivos para que se legisle en contra y se prime el control de Internet".

Lo que le está pasando factura a este grupo es, precisamente, la constante demostración de lo mucho que pueden hacer. En la mañana del miércoles celebraron en Twitter el bloqueo de la página de MasterCard. Las consecuencias llegaron poco tiempo después. El sistema de *microblogging* cerró la cuenta llamada @Anon_Operation. Los activistas crearon una nueva minutos después. Duró pocas horas en línea. Este cierre, junto con la acusación de censura, han convertido a Twitter en un nuevo blanco.

El sistema de Twitter no ha caído pero sí que ha sufrido varios intentos de denegación de servicio. Algo parecido ha ocurrido con Facebook tras cerrar la página de estos activistas.

El caos generado en la Red no está recibiendo mucha condena aunque no llega a los aplausos con que se recibe el que se tumbe la página de la SGAE. "A los canallas se los ve a veces con simpatía por su sentido de la justicia", indica Antoni Gutiérrez-Rubí. "Es como con los *okupas,* se genera un cierto placer con este cachete digital".

El nivel de las protestas de estos activistas espontáneos va en paralelo con el proceso contra Julian Assange. Gutiérrez-Rubí ve claramente una estrategia orquestada para deteriorar su imagen. "Ya están tocando su reputación, van a comenzar a cuestionar las motivaciones que le han llevado a crear un medio como Wikileaks, a sembrar dudas sobre la financiación de la página... Esto no ha hecho más que empezar", advierte.

Sin embargo, Julian Assange guarda un cartucho, el denominado seguro de vida en forma de archivo con filtraciones aún más relevantes. Nadie sabe lo que hay dentro pero se intuye que es de una relevancia superior a los cables aireados hasta ahora. Chema Alonso, reconocido además en varios encuentros de seguridad mundial, tiene una intuición con respecto al contenido del archivo encriptado: "Podría demostrar que Estados Unidos se encuentra detrás de Stunex, el ataque contra el núcleo del armamento nuclear iraní. Las consecuencias de esta revelación podrían generar una guerra no solo en Internet".

Los actos de apoyo a Julian Assange comienzan a tener eco en el mundo real.

Más allá de la ciberguerra, este caso abre el debate sobre el derecho que tienen las compañías para escoger a sus clientes a partir de decisiones oficiales.

El nuevo ejército

ANÁLISIS

David de Ugarte

Lunes, 1 de septiembre de 2003. Taipei. El primer ministro taiwanés llamaba uno por uno a los responsables de las principales instituciones y empresas del país. La inteligencia nacional había reportado que un ejército de *hackers* con base en las provincias chinas de Hubei y Fujian había contaminado con éxito y mediante 23 *troyanos* las redes de 10 compañías privadas. Estas redes habían sido usadas como plataforma para asaltar al menos una treintena de agencias gubernamentales y 50 compañías particulares. Entre las dependencias gubernamentales asaltadas con éxito estaban la policía, el Ministerio de Defensa, la Junta Electoral y el Banco Central. En una decisión sin precedentes, el Gobierno taiwanés aprobó no solo hacer público el ataque, sino también sus detalles técnicos, recomendando de paso a las empresas locales que no compraran *software* desarrollado en China ni contratar desarrolladores en aquel país.

Era el primer caso documentado de ciberguerra. El Ministerio de Información de Milosevic ya había sufrido ataques organizados y estratégicos en los noventa, pero tras ellos no había Estados, sino grupos de ciberactivistas y voluntarios de todo el mundo empeñados en hacer visibles los crímenes de guerra y entorpecer la propaganda oficial.

Pero las fronteras de la ciberguerra siempre son borrosas. El 27 de abril de 2007 las principales instituciones estonas, desde el Parlamento a los periódicos pasando por los bancos, veían caer sus sitios webs ante un ataque masivo originado en Rusia. El apagón informativo virtual se acompasó con violentas protestas de la minoría prorrusa en la calle. Durante horas, la confusión y el miedo hicieron a muchos temer un verdadero golpe de Estado postmoderno. Al año siguiente, durante el conflicto ruso-georgiano, el estratégico gaseoducto entre Bakú, Tblisi y Ceyhan se veía paralizado por un ciberataque ruso. Lo sería por segunda vez en agosto de 2009. En esta ocasión se usaron las mismas IPs que en Estonia.

Estos ejemplos revelan el lugar de la ciberguerra en la relación entre Estados: paralizar infraestructuras y generar alarma para producir desestabilización política. La ciberguerra es el ciberterrorismo de los Estados.

Y entonces, ¿todos estos ataques contra servidores corporativos que reclaman *vengar* a un Assange perseguido por las revelaciones de Wikileaks serían también ciberguerra? Una de las características de nuestra época es, como enunciaba Jesús Pérez Triana en *Guerras posmodernas,* el "ascenso de un nuevo tipo de actor internacional de escala cada vez más pequeña". Los mismos cambios tecnológicos que dan la posibilidad a pequeñas firmas de convertir un producto en fenómeno global o a un periodista en celebridad planetaria permiten que comunidades de escala casi invisible "colapsen" sistemas vitales en la actual estructura de la globalización. La postmodernidad se parece cada vez más al mundo descrito por Bruce Sterling en *Islas en la Red,* y, como en aquella mítica novela, la ciberguerra es solo la telonera de las estrellas por llegar.

David de Ugarte es socio del Grupo Cooperativo de las Indias y autor de *Los futuros que vienen: la descomposición global y la importancia de la comunidad en el siglo XXI.*

+EL PAÍS.com

▶ **Participe**

¿Justifica los ciberataques en respuesta al acoso a Wikileaks?

sociedad

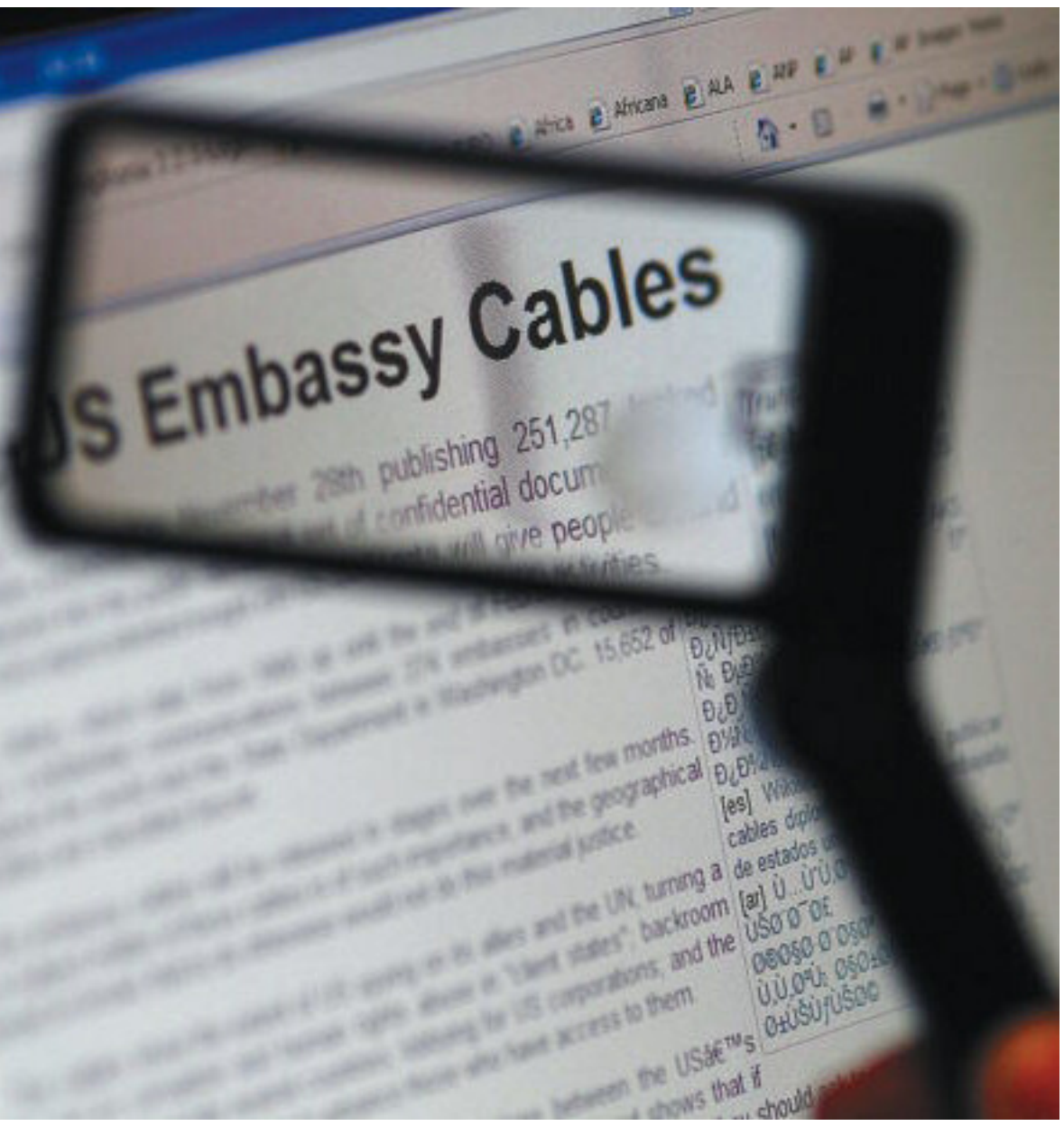
La menor lista de espera quirúrgica: 61 días

cultura

Documenta, las olimpiadas del arte sin concepto

cine

La secuela de la fracasada 'Tron' aspira al taquillazo



La información secreta difundida por Wikileaks y los ataques que sufrió después han agitado la Red. / GETTY

Esa misma noche consiguieron hacer que cayese la página web de Visa. Se quedó varias horas sin página web y muchas más con intermitencias. La compañía ha emitido un comunicado en el que reconoce que "algunos sitios webs de Visa están experimentando un tráfico mayor del habitual, lo que ha dificultado el acceso a los mismos de forma intermitente. Estamos trabajando para solucionarlo y esperamos que el servicio esté restaurado en breve".

Diego Guerrero, autor del libro *Fraude en la Red*, relativiza el efecto de esta caída: "Es publicitario, para hacer ruido. Echan abajo la web de las tarjetas de crédito pero no el servicio en sí, que sería delito. Es decir, la gente puede seguir comprando. Ahora mismo solo generan perjuicio de imagen y económico". En medio de toda esta alarma colectiva este experto llama a la calma: "El nivel de dificultad para entrar en estos servidores es muy elevado. A veces se pueden escapar datos pero penetrar en su sistema es mucho más complejo".

A raíz de que Amazon se negase a hospedar a Wikileaks en sus servidores, la empresa de venta por Internet es el nuevo blanco. La solución a esta supuesta deficiencia se ha encontrado también en la propia Red, los sitios espejo que replican el contenido que no quieren que salga a la luz. Al igual que Paypal, la plataforma dominante en el pago virtual. Mientras que algunos críticos protestan dándose de baja de estos servicios, cada vez son más los que hacen una protesta más agresiva y toman el teclado como arma.

Los seguidores de Wikileaks más molestos con la detención de Julian Assange no cesan de dar enlaces en Twitter con herramientas para que más internautas se sumen a la acción.

José Alcántara, autor de *La sociedad de control* y *La neutralidad de la Red*, cree que estas acciones no las realizan profesionales sino *lammers*, personas sin gran preparación, en muchos casos adolescentes que no saben programar pero sí ejecutar un programa en lenguaje Javascript para hacer un ataque constante y descentralizado. "Crean turbas y, como todo el mundo sabe, con las turbas no se puede argumentar", lamenta.

> Panda denuncia que existen bandas de chantajeadores de empresas

> Adolescentes sin gran preparación pueden participar en sabotajes

En su opinión, las consecuencias de lo que denomina "gamberrada" va a costar muy caro: "Nos jugamos batallas como la neutralidad de la Red. Un uso irresponsable de su poder, como es el caso, no hace más que dar motivos para que se legisle en contra y se prime el control de Internet".

Lo que le está pasando factura a este grupo es, precisamente, la constante demostración de lo mucho que pueden hacer. En la mañana del miércoles celebraron en Twitter el bloqueo de la página de MasterCard. Las consecuencias llegaron poco tiempo después. El sistema de *microblogging* cerró la cuenta llamada @Anon_Operation. Los activistas crearon una nueva minutos después. Duró pocas horas en línea. Este cierre, junto con la acusación de censura, han convertido a Twitter en un nuevo blanco.

El sistema de Twitter no ha caído pero sí que ha sufrido varios intentos de denegación de servicio. Algo parecido ha ocurrido con Facebook tras cerrar la página de estos activistas.

El caos generado en la Red no está recibiendo mucha condena aunque no llega a los aplausos con que se recibe el que se tumbe la página de la SGAE. "A los canallas se los ve a veces con simpatía por su sentido de la justicia", indica Antoni Gutiérrez-Rubí. "Es como con los *okupas,* se genera un cierto placer con este cachete digital".

El nivel de las protestas de estos activistas espontáneos va en paralelo con el proceso contra Julian Assange. Gutiérrez-Rubí ve claramente una estrategia orquestada para deteriorar su imagen. "Ya están tocando su reputación, van a comenzar a cuestionar las motivaciones que le han llevado a crear un medio como Wikileaks, a sembrar dudas sobre la financiación de la página... Esto no ha hecho más que empezar", advierte.

Sin embargo, Julian Assange guarda un cartucho, el denominado seguro de vida en forma de archivo con filtraciones aún más relevantes. Nadie sabe lo que hay dentro pero se intuye que es de una relevancia superior a los cables aireados hasta ahora. Chema Alonso, reconocido además en varios encuentros de seguridad mundial, tiene una intuición con respecto al contenido del archivo encriptado: "Podría demostrar que Estados Unidos se encuentra detrás de Stunex, el ataque contra el núcleo del armamento nuclear iraní. Las consecuencias de esta revelación podrían generar una guerra no solo en Internet".

Los actos de apoyo a Julian Assange comienzan a tener eco en el mundo real.

Más allá de la ciberguerra, este caso abre el debate sobre el derecho que tienen las compañías para escoger a sus clientes a partir de decisiones oficiales.

El nuevo ejército

ANÁLISIS

David de Ugarte

Lunes, 1 de septiembre de 2003. Taipei. El primer ministro taiwanés llamaba uno por uno a los responsables de las principales instituciones y empresas del país. La inteligencia nacional había reportado que un ejército de *hackers* con base en las provincias chinas de Hubei y Fujian había contaminado con éxito y mediante 23 *troyanos* las redes de 10 compañías privadas. Estas redes habían sido usadas como plataforma para asaltar al menos una treintena de agencias gubernamentales y 50 compañías particulares. Entre las dependencias gubernamentales asaltadas con éxito estaban la policía, el Ministerio de Defensa, la Junta Electoral y el Banco Central. En una decisión sin precedentes, el Gobierno taiwanés aprobó no solo hacer público el ataque, sino también sus detalles técnicos, recomendando de paso a las empresas locales que no compraran *software* desarrollado en China ni contratar desarrolladores en aquel país.

Era el primer caso documentado de ciberguerra. El Ministerio de Información de Milosevic ya había sufrido ataques organizados y estratégicos en los noventa, pero tras ellos no había Estados, sino grupos de ciberactivistas y voluntarios de todo el mundo empeñados en hacer visibles los crímenes de guerra y entorpecer la propaganda oficial.

Pero las fronteras de la ciberguerra siempre son borrosas. El 27 de abril de 2007 las principales instituciones estonas, desde el Parlamento a los periódicos pasando por los bancos, veían caer sus sitios webs ante un ataque masivo originado en Rusia. El apagón informativo virtual se acompasó con violentas protestas de la minoría prorrusa en la calle. Durante horas, la confusión y el miedo hicieron a muchos temer un verdadero golpe de Estado postmoderno. Al año siguiente, durante el conflicto ruso-georgiano, el estratégico gaseoducto entre Bakú, Tblisi y Ceyhan se veía paralizado por un ciberataque ruso. Lo sería por segunda vez en agosto de 2009. En esta ocasión se usaron las mismas IPs que en Estonia.

Estos ejemplos revelan el lugar de la ciberguerra en la relación entre Estados: paralizar infraestructuras y generar alarma para producir desestabilización política. La ciberguerra es el ciberterrorismo de los Estados.

Y entonces, ¿todos estos ataques contra servidores corporativos que reclaman *vengar* a un Assange perseguido por las revelaciones de Wikileaks serían también ciberguerra? Una de las características de nuestra época es, como enunciaba Jesús Pérez Triana en *Guerras posmodernas,* el "ascenso de un nuevo tipo de actor internacional de escala cada vez más pequeña". Los mismos cambios tecnológicos que dan la posibilidad a pequeñas firmas de convertir un producto en fenómeno global o a un periodista en celebridad planetaria permiten que comunidades de escala casi invisible "colapsen" sistemas vitales en la actual estructura de la globalización. La postmodernidad se parece cada vez más al mundo descrito por Bruce Sterling en *Islas en la Red,* y, como en aquella mítica novela, la ciberguerra es solo la telonera de las estrellas por llegar.

David de Ugarte es socio del Grupo Cooperativo de las Indias y autor de *Los futuros que vienen: la descomposición global y la importancia de la comunidad en el siglo XXI.*

+EL PAÍS.com

▶ **Participe**

¿Justifica los ciberataques en respuesta al acoso a Wikileaks?