Fraude, terror, propaganda, planes terroristas. La Red permite todo La industria online puede ayudar a poner orden

SERVIDORES DEL TERROR

Por David Talbot ILUSTRACIÓN DE TAVIS COBURN

EL 12 DE OCTUBRE DE 2002, DOSCIENTAS dos personas fallecían en una discoteca de Bali, Indonesia, por la explosión de las bombas que un terrorista suicida hizo estallar sobre la sala de baile de un bar de turistas y por la acción, momentos después, de un segundo terrorista que detonó una furgoneta Mitsubishi cargada de explosivos aparcada en el exterior. Recientemente, el cerebro de los ataques—Imam Samudra, un militante islamista de 35 años conectado con al-Qaeda—ha escrito en la cárcel un memorándum donde ofrece un esbozo de fraude con tarjeta de crédito por internet de lo más sofisticado, recomendándolo a los musulmanes radicales como medio de financiación de sus actividades.

Según las autoridades policiales, las pruebas encontradas en el ordenador portátil de Samudra demuestran que trató de financiar el atentado de Bali cometiendo acciones fraudulentas en Internet. Y sus nuevos escritos sugieren que el fraude online—en 2003 solamente en Estados Unidos costó a las compañías de tarjetas de crédito 1.200 millones de dólares—puede llegar a ser, si no lo es ya, un arma clave en el arsenal terrorista. "Conocemos que grupos terroristas por todo el mundo se han financiado mediante el delito" dice Richard Clarke, el antiguo zar antiterrorista de los presidentes Bush y Clinton. " Comienzan a existir bases para llegar a la conclusión de que una de las formas como se financian es a través del ciber-delito".

El fraude online se uniría por tanto a otras importantes maneras con la que los grupos terroristas explotan Internet. Es de sobra conocido que los conspiradores del 11 de Septiembre usaron Internet para sus comunicaciones internacionales y la búsqueda de información. Cientos de sitios web de jihadistas se usan con el propósito de hacer propaganda y de conseguir fondos, y son de acceso tan fácil como cualquiera de las páginas de los más importantes noticieros. En 2004 la Web fue inundada con el vídeo, en toda su crudeza, de la degollación de rehenes perpetradas por los seguidores de Abu Musab al Zarqawi, el líder terrorista nacido en Jordania y que opera en Irak. Este no fue un fenómeno marginal, cientos de millones de personas descargaron los archivos del vídeo, una especie de inmenso espectáculo medieval facilitado por innumerables compañías de web hosting, Suministradores de Servicio Internet, o ISPs. " No se dónde está el límite. Pero ciertamente lo hemos rebasado ya, abusando de Internet", dice Gabriel Weimann, un profesor de comunicación en la Universidad de Haifa, quien rastrea el uso de Internet por los grupos terroristas.

Enfrentarse a estos innumerables retos va a requerir nueva tecnología y, como alguno dice, una mayor autoregulación por parte de la industria online, aunque sólo sea para evitar gravosos cambios o unas mayores restricciones que algún día podrían llegar, bien por orden de las autoridades legales o por las propias exigencias de seguridad en interés del negocio. Según Vinton Cerf, uno de los padres fundadores de Internet con los que codiseñó sus protocolos, los contenidos de extrema violencia en la Red es "un enigma tremendamente difícil de tratar y resolver de forma constructiva". Pero él añade "no significa que no debamos hacer algo, la industria tiene una considerable cantidad de información en potencia, aunque se trate de imaginar como auto disciplinarse a escala mundial. La pregunta es, ¿qué parte de la industria puede hacerlo?" Los impedimentos son muchos, advierte: La información puede venir literalmente de cualquier sitio, y aunque los principales actores de la industria acuerden las restricciones, los usuarios de Internet podrían obviamente seguir intercambiando contenidos entre ellos mismos. "Como siempre, la gran pregunta será, ¿quién decide qué es contenido aceptable y sobre qué base?"

En la amplia batalla contra el uso terrorista de Internet ya están en marcha algunos trabajos. Laboratorios de investigación están desarrollando nuevos algoritmos con el objetivo de facilitar a los investigadores el peinado a través de los e-mails y de los diálogos en chat-rooms para descubrir tramas delictivas. Por otro lado, los esfuerzos antispam de la industria están

proporcionando nuevas herramientas para autentificar remitentes de e-mail mediante criptografía y otros métodos, lo cual también ayudará a combatir el fraude; evidentemente, el aprovechamiento terrorista de Internet añade una dimensión de seguridad nacional a estos esfuerzos. El uso terrorista del medio y las respuestas que van surgiendo, van a conducir a una época en que la distribución de contenido online estará más estrechamente controlado y rastreado y la pregunta inmediata que surge es si esto será para mejor o para peor.

El auge del terror en Internet

Hoy en día, gran parte de los expertos están de acuerdo en que Internet no es exactamente una herramienta de organizaciones terroristas, pero si que está en el centro de sus operaciones. Hay quien dice que desde los ataques del 11 de Septiembre la presencia online de al-Qaeda ha llegado a ser más potente y relevante que su presencia física real. "Cuando decimos que al-Qaeda es una ideología global, donde encuentra su significado es en Internet," dice Michael Doran, un estudioso en Cercano Oriente y experto en terrorismo de la Universidad de Princenton. "Esto, en sí mismo, lo encuentro sorprendente. Hace apenas unos pocos años, una organización como ésta habría sido más bien de índole pseudo religiosa y no habría sido capaz de extenderse alrededor del mundo en la forma que lo hace con Internet".

El universo de sitios web relacionados con el terror se extiende, desde luego, más allá de al-Qaeda. Según Weimann, el número de sitios de este tipo ha saltado de solamente 12 en 1997 a los 4.300 de hoy (esto incluye sitios operados por grupos como Hamas y Hezbollath así como otros en Sudamérica y otras partes del mundo). "En siete años ha explotado y estoy seguro que el número crecerá semana tras semana", Weimann describió la tendencia en su informe "How Modern Terrorism Uses the Internet", publicado por el United States Institute of Peace y está ahora trabajando en el libro Terrorism and the Internet que saldrá al final de este año.

Estos sitios sirven para reclutar miembros, solicitar fondos así como promover y extender su ideología. "Aunque la percepción [común] es que no están [los terroristas] muy instruidos ni muy preparados en telecomunicaciones e Internet, sabemos que no es así," dice Ronald Dick, un antiguo director del FBI que dirigió el FBI´s National Infrastructure Protection Center. "Los individuos que el FBI y otras agencias encargadas de la Ley han arrestado tienen conocimientos en ingeniería y telecomunicaciones, se han formado en institutos académicos en todo lo referente a estas habilidades" (el militante Islamista, a pesar de sus raíces en el puritano Wahhabismo, no tiene inconveniente en surtirse del manantial que le ofrece la liberal educación Occidental: Khalid Sheikh Mohammed, el cerebro principal del 11 de Septiembre, se formó en ingeniería mecánica en EE.UU. y Ayman al-Zawahiri, el lugarteniente de Osama bin Laden, lo hizo como cirujano en Egipto).

La Web da a la jihad una cara pública. Pero a un nivel menos visible, Internet permite a los grupos extremistas organizar subrepticiamente ataques y recopilar información. Philip Zelikow, un historiador en la Universidad de Virginia y antiguo director ejecutivo de la Comisión 9/11 dice que los secuestradores del 11 de Septiembre usaron herramientas tan convencionales como chats-rooms y e-mails para comunicarse y la Web para obtener información sobre los objetivos. Según dice, "los conspiradores usaron Internet, normalmente con mensajes codificados, como un importante medio para sus comunicaciones internacionales" , (algunos de los aspectos sobre el uso de Internet por los terroristas se mantienen clasificados; por ejemplo, cuando se le pregunta si Internet intervino en el reclutamiento de los secuestradores, Zelikow dice que no lo puede comentar).

Como remate, los terroristas están aprendiendo que pueden distribuir imágenes de atrocidades con la ayuda de la Web. En 2002, la Web facilitó la amplia difusión de videos mostrando la degollación del periodista Daniel Pearl del Wall Street Journal, y eso a pesar de la petición del FBI para que los sitios web no las pusieran. Después, en 2004, Zarqawi hizo del horrible método la base de su estrategia del terror, comenzando con el asesinato del contratista civil americano Nicholas Berg—que los agentes de la ley creen fue llevada a cabo por el propio Zarqawi. Desde el punto de vista de Zarqawi, la campaña fue un gran éxito. Las imágenes de rehenes ataviados de color naranja fueron cabeceras de los noticiarios por todo el mundo—y la extrema crudeza de los videos de sus asesinatos rápidamente diseminada por la Web. "Internet permite a un pequeño grupo difundir actos tan horrorosos y atroces en segundos, a escaso o ningún coste y a vastas audiencias, a escala mundial, en el más poderoso medio," dice Weimann.

Y hay un gran mercado para tal material. Según Dan Klinker, responsable de un destacado sitio online sobre violencia, Ogrish.com, el consumo de este material es muy activo. Klinker, que dice operar desde oficinas en el Este y Oeste de Europa y Nueva York, afirma que su finalidad es "abrir los ojos de la gente y hacerles conscientes de la realidad". Está claro que muchos ojos han captado estas imágenes gracias a sitios como este. Cada video de decapitación ha sido descargado desde el sitio de Klinker varios millones de veces, según dice, y el de Berg lidera la lista con 15 millones. "Durante ciertos sucesos (decapitaciones, etc.) los servidores apenas pueden manejar el demencial ancho de banda—a veces 50.000 a 60.000 visitantes por hora," dice Klinker.

Evitar terrenos resbaladizos

Es cierto que los usuarios de Internet que quieren eliminar contenido censurable pueden comprar una variedad de filtros software que procuran bloquear el contenido sexual o violento. Pero están lejos de ser perfectos y si bien existe un variado surtido de esquemas de clasificación de paginas Web, en distintas fases de implementación, no se aplica un sistema universal para esta clasificación—ninguno es obligatorio—que haría más efectivos a los filtros elegidos por los consumidores.

Pero aprobar leyes orientadas a permitir un filtrado más ajustado—por no decir el exigir el filtrado en la actualidad—es problemático. Leyes orientadas a bloquear el acceso de los menores a pornografía, como la Ley de la Decencia en las Comunicaciones y la Ley de la Protección Online de los Niños, han sido derribadas en los tribunales a causa de la Primera Enmienda, y el mismo destino han tenido algunas leyes estatales; a menudo por buenas razones: las herramientas de filtrado a veces rechazan lo bueno con lo malo. "Lo mejor de lo peor, los tribunales están más preocupados en proteger los derechos de la Primera Enmienda de los adultos que proteger a los niños del material nocivo," dice Ian Ballon, un experto en leyes del ciberespacio y socio en Manatt, Phelps, and Phillips en Palo Alto,

California. Según él, la pornografía " es algo en que los tribunales han estado más cómodos regulando en el mundo físico que en Internet." Las mismas cuestiones son aplicables a imágenes de extrema violencia, añade.

Desde hace décadas, la Comisión Federal de Comunicaciones impone "decencia" en las ondas nacionales como parte de su misión de conceder licencias y regular las emisoras de televisión y radio. En contraste, el contenido en Internet no está básicamente regulado. Así, en 2004, mientras millones de personas veían los videos de las degollaciones en sus ordenadores, la FCC multó a la CBS con 550.000 $ por retransmitir por televisión la exhibición del pecho de la cantante Janet Jackson durante su actuación en el intermedio de la Super Bowl.

"La regulación de los contenidos de internet, si bien no es totalmente imposible, está obstaculizada por la variedad de lugares donde se pueden albergar", dice Jonathan Zittrain, codirector del Centro Berkman para Internet y Sociedad en Harvard Law School—y esto no tiene nada que ver con la Primera Enmienda. Como Zittrain lo ve, "es un regalo que los sitios estén por ahí, porque nos da una oportunidad para la contrainteligencia."

Como desestímulo, el procesamiento criminal ha tenido también un éxito limitado. Aún cuando los sospechosos de suministrar asistencia basada en Internet a las células del terror estén en los Estados Unidos, obtener condenas puede ser difícil. Al comienzo del pasado año, mediante la cláusula de la Ley Patriótica, el Departamento de Justicia de U. S. incriminó a Sami Omar al-Hussayen, un estudiante de la Universidad de Idaho, de usar Internet en la ayuda a terroristas. El Gobierno alegó que al-Hussayen mantenía sitios web que fomentaban actividades relacionadas con jihadistas incluyendo financiación de terroristas. Pero su defensa arguyó que él simplemente utilizó sus habilidades para promocionar el Islam y no era responsable del contenido radical de los sitios. El juez recordó al jurado que, en cualquier caso, la Constitución protege la expresión. El jurado exoneró a al-Hussayen de la acusación de terrorismo aunque dejó en suspenso la acusación en relación con su visado; al-Hussayen acordó volver a su casa natal de Arabia Saudí antes que enfrentarse a un nuevo juicio a cuenta del visado.

Richard Clarke

CHRISTOPHER HARTLOVE

La adopción por la Industria de controles editoriales mas estrictos sería una cuestión de buen gusto y de apoyo a la guerra contra el terror, dice Richard Clarke.

Tecnología e ISPs

La estrategia del Gobierno y del sector privado para combatir el terrorismo tiene varias facetas. Es seguro que agencias como el FBI y la National Security Agency—además de una variedad de grupos de observación, tales como el Site Institute, una organización sin ánimo de lucro establecida en la Costa Este y cuya localización pidió que no se publicara—vigilan estrechamente los sitios jihadistas y de otros terroristas para estar en la medida de lo posible al tanto de sus declaraciones públicas y de sus comunicaciones internas.

Es un inmenso trabajo, como buscar una aguja en un pajar, pero que puede rendir un constante flujo de interesantes informaciones de inteligencia o alarma. Por ejemplo, el Site Institute descubrió recientemente en un foro llamado Jihadi Message Board, una traducción al árabe de una página web de la Air Force que mencionaba a un aviador americano de origen libanés. Según Rita Katz, directora ejecutiva del Site Institute, la página jihadista añadía en árabe, "Este hipócrita irá a Irak en Septiembre de este año [2004]—Ruego a Alá que sus malas artes lo conduzcan a su propia carnicería. Espero que sea sacrificado al estilo Zarqawi, y después [vaya desde allí] a lo más profundo del Infierno." El Site Institute alertó al ejército. Hoy, en una de las paredes de su oficina cuelga una placa dando las gracias a la Air Force Office of Special Investigations.

Las nuevas tecnologías pueden también dar a las agencias de inteligencia herramientas para tamizar las comunicaciones online y descubrir tramas terroristas. Por ejemplo, hay investigaciones que indican que la gente con propósitos maléficos tiende a mostrar patrones distinguibles en la utilización de e-mails y foros online como los chats-rooms. Mientras que la mayoría de la gente establece, con el tiempo, una amplia variedad de contactos, los involucrados en un complot criminal tienden a contactar solamente con un restringido círculo de gente, dice William Wallace, un investigador de operaciones en el Rensselaer Polytechnic Institute.

Este fenómeno resulta bastante predecible. "Muy pocos grupos de gente se comunican de forma asidua solamente entre ellos", dice Wallace. "Es muy raro; no se fían de gente fuera del grupo a comunicar. Cuando el 80 por ciento de las comunicaciones son dentro de un grupo regular, es cuando pensamos que encontraremos

grupos que están planeando actividades sospechosas". Desde luego, no todos estos grupos tienen por qué estar relacionados con actividades delictivas, y puede que encontremos hasta reuniones de antiguos compañeros de Instituto. Pero el grupo de Wallace está desarrollando un algoritmo que limitará el campo de las llamadas redes sociales a aquellas que justifiquen el ser vigiladas por los funcionarios de inteligencia. Se ha previsto que el algoritmo esté listo y entregado a las agencias de inteligencia este verano.

Y desde luego, la extensiva lucha contra el spam y el fraude online continúa a buen ritmo. Uno de los mayores retos a los que se enfrentan las fuerzas antifraude es la facilidad con la que los timadores pueden elaborar sus e-mails, de tal forma que parezcan provenir de fuentes conocidas y fiables, tales como colegas o entidades bancarias. En una estafa conocida como "phishing," su táctica consiste en engañar a los receptores para que revelen sus números de cuenta y claves. El evitar tales estafas, según Clarke, "es aplicable al antiterrorismo porque evitaría gran cantidad de ciber-delitos, a través de los cuales puede que se financien [los terroristas]. Esto podría dificultarles la adquisición de identidades, que usan sólo una vez, para sus comunicaciones".

Nuevos métodos de autenticación pueden ofrecer una línea de defensa. El pasado otoño AOL suscribió un sistema diseñado por Microsoft, llamado Sender ID, que elimina ciertos agujeros en la seguridad y compara las direcciones IP (Protocolo Internet) del servidor que está enviando el e-mail entrante, con una lista de servidores autorizados a enviar correo desde la fuente que da a entender el mensaje. Yahoo, el mayor proveedor de e-mail con cerca de 40 millones de cuentas, está rodando su propio sistema, llamado Domain Keys, que etiqueta cada e-mail saliente con una firma encriptada que puede utilizarse por el receptor para verificar que el mensaje viene desde el dominio pretendido. Google está usando tecnología con sus cuentas Gmail, y otros grandes ISPs, incluyendo Earthlink, hacen algo similar.

En definitiva, los mayores ISPs están reaccionando por sí mismos. Sus "condiciones de servicio" son normalmente lo bastante amplias como para permitirles la libertad de retirar sitios censurables cuando así se le pide. "Cuando se habla acerca de una comunidad online, el poder proviene del individuo," dice Mary Osako,

Terrorismo e Internet

En la última década, según el uso de Internet se ha ido extendido a través del globo, la interacción online ha llegado a formar parte de muchos fenómenos sociales—incluyendo el terrorismo.

Las organizaciones terroristas están aprovechándose del alcance global de Internet para reclutar miembros, conseguir fondos y extender sus ideologías. Gabriel Weimann, un profesor en la Universidad de Haifa en Israel, identifica 4.300 sitios web distribuidas por el mundo relacionadas con el terror.

Arriba se representa una muestra de sitios web terroristas y la localización de sus servidores. Esta lista fué suministrada por el Site Institute, un grupo de observación situado en EE.UU. que vigila grupos jihadistas.

El fraude online es desde luego un fenómeno distinto, pero las autoridades legales están preocupadas cada vez más porque pueda llegar a ser una fuente de financiación de terroristas. Como el número de usuarios de Internet se aproximará a los mil millones en muy pocos años, estas tendencias pueden llegar a ser aún más acusadas. **STACY LAWRENCE**

FUENTE: NATIONAL WHITE COLLAR CRIME CENTER AND THE FEDERAL BUREAU OF INVESTIGATION (FRAUD DATA); MERCHANT RISK COUNCIL (PROBLEMATIC NATIONS); SITE INSTITUTE (TERRORIST WEBSITES); IDC (INTERNET USAGE).

Netherlands 10
United Kingdom 8
Germany 7
Romania 6
Italy 4
Spain 5
Macedonia
Israel
Egypt
Russia
Tehran, Iran
qudsway.com
(Palestinian Islamic Jihad)
India
Thailand
Vietnam
Dubai, United Arab Emirates
palestine-info.info
(Hamas)
Nigeria 3
Ghana
Cyberjaya, Selangor, Malaysia
alqassam.info
(Hamas)
South Africa 9

LEYENDA

- **Localización del servidor** Website URL (Grupo terrorista)
- # Lugar en la lista de naciones con mayor fraude on line
- Paises identificados como proclives al fraude en el comercio en internet

usuarios de Internet /1.000 habitantes

- 400–600
- 150–400
- 50–150
- 10–50
- <10
- sin datos

Escaparate del fraude Online

En 2003 el centro de reclamaciones de delitos en internet en Estados Unidos recibió 124.509 denuncias. La clasifiación de paises por la ubicación de los defraudadores es la siguiente:

	País	*Casos*
1	Estados Unidos	76.4%
2	Canadá	3.3%
3	Nigeria	2.9%
4	Italia	2.5%
5	España	2.4%
6	Rumanía	1.5%
7	Alemania	1.3%
8	Reino Unido	1.3%
9	Sudáfrica	1.1%
10	Holanda	0.9%

directora de comunicación de Yahoo. "Animamos a nuestros usuarios a enviarnos [cualquier preocupación sobre algo controvertido] y actuamos sobre cada denuncia".

Muy poco, o demasiado

Pero la mayoría de los expertos legales, policiales y de seguridad están de acuerdo que estos esfuerzos, reunidos, no llegan a pesar de todo a una solución real. Las nuevas iniciativas anti-spam representan sólo la última fase de una batalla en marcha. "El primer paso es que la industria tiene que entender que hay un problema mayor del que quiere admitir" dice Peter Newmann, un científico de ordenadores en SRI International, un instituto de investigación sin ánimo de lucro en Menlo Park, California. "Se necesita que haya un inmenso cambio cultural para crear sistemas dignos de confianza". Según él, hasta los esfuerzos para usar criptografía para confirmar la autenticidad de los remitentes de e-mails son meros paliativos. "Aún existe un montón de problemas" con la seguridad online, dice Newmann. "Se parece a un gran iceberg. Esto elimina un cuarto de porcentaje, tal vez un 2 por ciento, pero lo que sobresale es muy poco".

Pero si bien es verdad que las respuestas existentes son insuficientes para encauzar el problema, también es cierto que estamos ante el riesgo de una sobre reacción. Si comenzaran a emerger conexiones concretas entre el fraude online y los ataques terroristas, los gobiernos podrían decidir que Internet necesita más vigilancia y crear nuevas estructuras reguladoras. "Los ISPs podrían resolver la mayoría de los problemas de spam y phishing si lo hicieran a través de la FCC," advierte Clarke. Aún cuando los escritos de los dinamiteros de Bali no hayan creado tal reacción, cualquier otra cosa puede producirla. En caso de que no se haga ningún descubrimiento sobre una fuerte conexión entre el fraude online y el terrorismo, otro disparador podría ser una acción de "ciberterrorismo" literal—el muy temido uso de Internet para emprender ataques contra objetivos como las redes de distribución eléctrica a ciudades, el control de tráfico aéreo o los sistemas de comunicaciones. Podría darse también que alguna exhibición online de un homicidio fuera tan espantosa que produjera una nueva obsesión por la decencia online, lo que sería visto con buenos ojos por una conservadora y recientemente nueva Supreme Court. Aparte del terrorismo, el disparador podría ser una pura decisión de negocio, como alguna que persiga el hacer Internet más transparente y más segura.

Zittrain coincide con Neumann pero también predice una latente sobre-reacción. Terrorismo o no-terrorismo, él ve una convergencia de las tendencias en seguridad, leyes y negocio que forzarán el cambio de Internet y no necesariamente a mejor. "Colectivamente hablando, se está yendo a cambios tecnológicos en cómo funciona Internet—impulsados bien por las leyes o por la acción colectiva. Si se mira que se está haciendo con el spam, se ve que se sigue este modelo," dice Zittrain. Y mientras el cambio tecnológico puede mejorar la seguridad online, continúa diciendo, "hará Internet menos flexible. Si no es posible para dos socios en un garaje escribir y distribuir el código de una killer-app sin esclarecerlo primero con intereses fuertemente establecidos, estemos preparados a perder el mismo proceso que nos proporcionó el Navegador de la Web, la mensajería instantánea, Linux y el e-mail."

El primer paso necesario: un cambio de cultura en la industria para reconocer que hay un problema mayor del que se quiere admitir, dice Peter Neumann

Aún no hay evidencia de que exista un esfuerzo concertado hacia controles más severos. Pero si algún día el contenido sumamente violento o el uso terrorista de Internet insta un nuevo impulso, la ocasión para acciones preventivas debería recaer en las ISPs y compañías de Web hosting. Es necesario que sus esfuerzos no se limiten a luchar contra el spam y el fraude. En relación con lo que publican, las compañías de Web hosting podrían actuar como sus antiguos primos, las emisoras de televisión y los editores de periódicos y revistas, realizando una ligera valoración editorial, con la simple puesta en aplicación de las actuales condiciones de servicio.

¿Se somete ya a esta evaluación el contenido de la Web? Normalmente no, pero a veces, un ojo esperanzado puede percibir lo que parecen ser sus resultados.

Consideremos la misteriosa inconsistencia entre los resultados obtenidos cuando introducimos la palabra "decapitación" en los principales motores de búsqueda. En Google y MSN, los primeros resultados son un paquete con una mezcolanza de enlaces hacia cuentas de noticias responsables, información histórica y sitios desagradables que ofrecen videos en toda su crudeza con mensajes tales como "Mundo de la Muerte, videos de decapitaciones en Irak, fotos de muertes, suicidios y escenas de crímenes". Evidentemente, estos resultados son el producto de algoritmos aplicados para encontrar los sitios que sean más populares, relevantes o vinculados.

Pero entremos el mismo término de búsqueda en Yahoo, y lo primero que presenta son los perfiles de las víctimas, tanto de EE.UU. como británicas, decapitadas en Irak. Los 10 primeros resultados incluyen enlaces a las biografías de Eugene Armstrong, Jack Hensley, Kenneth Bigley, Nicholas Berg, Paul Johnson, y Daniel Pearl, así como a sitios web conmemorativos. Debemos cargar la segunda página de búsqueda para encontrar un enlace a Ogrish.com. ¿Es esta tan extrañamente delicada ordenación, el aberrante resultado de un algoritmo tan insensible como los que nos salpican por doquier con enlaces gore? ¿O es que Yahoo, quizás en un guiño a la memoria de las víctimas y sentimiento de sus familias, hace una excepción de las palabras "decapitar" y "decapitación", tratándolas de forma diferente a como lo hace con palabras comparables temáticamente como "asesinato" y "apuñalamiento"?

Osako, de Yahoo no contesta a preguntas sobre este singular resultado de búsqueda, ciertamente no puede excluirse una explicación tecnológica. Pero está claro que este tipo de asuntos son muy delicados para una industria que hasta la fecha ha disfrutado de una mínima intervención y regulación. Richard Clarke dice, que en respuesta a reclamaciones, " la industria está muy dispuesta a cooperar y a ser buen ciudadano con tal de evitar la regulación". Si se va más lejos y se adopta una postura editorial estricta, él añade, "es una decisión de los ISP [y compañías de web hosting] hacer que sea tanto un asunto de buen gusto como de apoyo a los EE.UU. en la guerra global al terror". Si decisiones de este tipo evolucionan en una asunción por toda la industria de un mayor papel periodístico, podría a la postre, ser la ruta más segura hacia un medio más responsable—uno que es menos fácil de explotar y no tan vulnerable a una dura restricción. ■