Revista Latina de Comunicación Social
30 – junio de 2000

Edita: Laboratorio de Tecnologías de la Información y Nuevos Análisis de Comunicación Social
Depósito Legal: TF-135-98 / ISSN: 1138-5820
Año 3º – Director: Dr. José Manuel de Pablos Coello, catedrático de Periodismo
Facultad de Ciencias de la Información: Pirámide del Campus de Guajara - Universidad de La Laguna 38200 La Laguna (Tenerife, Canarias; España)
Teléfonos: (34) 922 31 72 31 / 41 - Fax: (34) 922 31 72 54

[Mayo de 2000]

Internet: un cuerpo enfermo y un campo de batalla

Dr. Raymond Colle ©

Servicio de Computación, Informática y Comunicaciones

Pontificia Universidad Católica de Chile

Resumen

Al celebrarse en 1999 los 30 años de la primera conexión telemática, los innumerables beneficios obtenidos de la conformación y desarrollo de esta red de redes pueden hacer olvidar que también es fuente de nuevos problemas y que está causando fuertes "dolores de cabeza" tanto a sus desarrolladores como a sus usuarios. Se abordan principalmente aquí los problemas vinculados al crecimiento de la red -como lentitud, limitaciones del protocolo TCP/IP, creciente dificultad para realizar búsquedas efectivas, etc.- y al mal uso de la misma ("guerra" digital, acciones de "piratas" y otras actividades delictivas), así como algunas de las acciones o proyectos tendentes a aportar soluciones (nuevas funciones de navegación, Internet 2, etc.).

Introducción

La informática de los años noventa ha adquirido la capacidad de transformarse en un medio de comunicación, al unir su poder de procesamiento con las telecomunicaciones, no sólo para permitir que este poder sea compartido sino para que se transforme en el "combustible" de la difusión del conocimiento. Uniéndose han dado origen a la telemática, cuyo epítome es la red mundial Internet, red compuesta de millones de ordenadores "servidores de información" y un número incontable de "clientes".

Al celebrarse este año los 30 años de la primera conexión telemática, los innumerables beneficios obtenidos de la conformación y desarrollo de esta red de redes pueden hacer olvidar que también es fuente de nuevos problemas y que está causando fuertes "dolores de cabeza" tanto a sus desarrolladores como a sus usuarios.

En el presente trabajo se sintetizan los resultados de una investigación llevada a efecto por el autor en la propia Internet en 1998 y 1999, para el Servicio de Computación, Informática y Comunicaciones (SECICO) de la Pontificia Universidad Católica de Chile, con el objeto de reunir información acerca de los principales problemas que están surgiendo a la luz.

Se abordan principalmente aquí los problemas vinculados al crecimiento de la red -como lentitud y creciente dificultad para realizar búsquedas efectivas- y al mal uso de la misma ("guerra" digital, acciones de "piratas" y otras actividades delictivas), así como los intentos imperialistas para lograr su control total.

1. Dolores de crecimiento

1.1. El desarrollo de Internet

Internet fue inventada en 1963 por Larry Roberts, contratado por Ivan Sutherland, que era el director de ARPA, en ese momento una oficina de Procesamiento de Información del Departamento de Defensa de Estados Unidos. Eran los tiempos de la guerra fría y se deseaba crear un sistema de enviar mensajes desde un punto A hasta un punto B que fuese inmune a posibles ataques con misiles nucleares.

Basada en este sistema se creó en 1969 (fecha que se celebra este año) la primera red: "ARPANET", red del Departamento de Defensa. Internet nació de la evolución de "ARPANET", uniendo inicialmente a científicos y centros universitarios de computación. En 1974, ARPANET se transformó en NSFNET, al asumir su coordinación general la Fundación Nacional para la

Ciencia, de Estados Unidos. Se fue extendiendo primero a Inglaterra, después a Noruega y luego a Japón.

La NSFNET adoptó en 1986 el protocolo de comunicación TCP/IP. En esa fecha, ya había 3.000 servidores conectados a la red, por sólo 200 en 1981 (Maurer, p. 10). En este período, a los ingenieros se fueron sumando otros científicos, médicos, maestros y estudiantes.

Crecimiento de servidores de Internet	
AÑO	**Nº de servidores**
1969	4
1981	200
1986	3.000
1990	150.000
1996	600.000
1999	60.000.000

Durante años, Internet sirvió casi exclusivamente para enviar mensajes: cartas, informes científicos y aplicaciones computacionales. El modelo comunicacional respondía al del correo tradicional -para el correo electrónico- y al de la biblioteca -para los depósitos de aplicaciones ("FTP")-: yo envío algo a alguien o yo voy a buscar algo a un determinado lugar: origen, destino y contenido son conocidos antes de actuar. Pero en 1989, Berners-Lee concibió el "lenguaje" HTML de definición, presentación e intervinculación de documentos como proyecto para organizar documentos del CERN (Centre Européen pour la Recherche Nucléaire, de Ginebra).En 1991 el sistema empezó a funcionar para el envío de documentos a través de Internet, dando origen en 1991 a la World Wide Web. Así se formuló el protocolo de transferencia para hipertextos (HTTP) basado en el sistema "MIME" (Multipurpose Internet Mail Extensions) utilizado para el correo electrónico. En noviembre de 1993 se produjo un cambio significativo, cuando Andreessen desarrolló la versión 2 del browser "Mosaic", incluyendo etiquetas que permitían embutir objetos dentro del documento (esencialmente campos de datos formando formularios) y enviar información sobre el estado de estos objetos al servidor, lo cual introducía un alto poder de interactividad. (Gaines, B. & Shaw, M., p. 730). Mientras tanto, en 1992 se fundó la Internet Society y esa debería ser, por lo tanto, la fecha oficial del nacimiento de la Internet que hoy conocemos. A partir de entonces, la World Wide Web conoció un rápido desarrollo en el ámbito mundial, en todo el ámbito académico y científico. Pero dicho éxito llamó la atención de la industria y del mundo del comercio y las presiones para abrirles la red llegaron a tal punto que la Fundación Nacional de la Ciencia norteamericana, que sostenía la red, decidió abandonar su participación y permitir su libre uso para todos. Así, desde 1996, la WWW dejó de ser una herramienta circunscrita al mundo de la ciencia y de la enseñanza y, poco más de un año después de su liberalización se contaban ya con más de veinte millones de páginas con todo tipo de contenidos: científicos, académicos, comerciales, artísticos, pornográficos (estimados en 2%) y personales. Ya no tiene sentido calcular el número de usuarios de Internet, como tampoco se cuentan los usuarios de televisores o de teléfonos pero es posible que la conexión a Internet se transforme luego en un nuevo indicador de desarrollo sociocultural, como estos otros medios de comunicación. La capacidad de comunicación multimedial de las redes, puesta en evidencia por la World Wide Web, está llevando a una profunda transformación cuyos límites no se visualizan aún. Sólo está claro que los usuarios tendrán cada vez más posibilidades de comunicación y más capacidades de procesamiento.

1.2. "Tacos" en la carretera

Debe quedar claro que el concepto de red desarrollado por Roberts es todo lo opuesto al concepto de "autopista de la información", que se tiende a utilizar erróneamente. Basta la crecida de un río que corte un puente o un terremoto en una región propensa a la actividad sísmica para que la carretera quede cortada (cosa que se conoce muy bien en Chile). Esto, en Internet, sería impensable. Incluso cuando fallaron los accesos a miles de servidores norteamericanos, a mediados de 1997, se debió no a un corte en la red sino a la difusión y copia automática de archivos de direcciones amputados (los terminados en ".net" y ".com"), es decir a un proceso pensado para una mayor seguridad, que falló por un error humano (no respetar una señal de alerta). Es posible, sin embargo, comparar Internet con una red de carreteras como la que existe en Europa: con numerosas vías, de diferente calidad, que conectan pueblos y ciudades de múltiples maneras. Y con todos los problemas de saturación ("tacos") que se observan constantemente allá. Es el problema de la estrechez del "ancho de banda", o sea del canal que une un nodo (servidor) con otro y que debe dejar pasar centenares o miles de comunicaciones simultáneas. Producto, principalmente, del auge de la información comercial, la cantidad de usuarios ha crecido más rápidamente que la capacidad de la red y que la velocidad de respuesta de los servidores, por lo que la WWW se llama hoy "World Wide Wait". Como consecuencia de este atochamiento en los canales de telecomunicación y de la creciente dificultad para la comunicación de contenidos científicos, la comunidad académica -principalmente de las universidades de Estados Unidos- ha protestado por esta situación y, dada su irreversibilidad, se ha unido para crear un sistema propio e independiente de la WWW. De este modo, la norteamericana Fundación Nacional de la Ciencia, que había sucumbido ante la presión del sector empresarial, tuvo que reasumir el papel de sostenedor de una red académica y científica específica. Se trata del Proyecto "Internet 2", el cual -obviamente- no pretende establecer otra red de telecomunicaciones, sino desarrollar una familia nueva de aplicaciones avanzadas que mejoren notablemente la comunicación entre instituciones de investigación y enseñanza. La misión declarada

del proyecto consiste en: "Facilitar y coordinar el desarrollo, despliegue, transferencia de tecnología y operación avanzada de aplicaciones distribuidas y de una red de servicios que mantenga el liderazgo norteamericano en la investigación y la educación superior y acelere la disponibilidad de nuevos servicios y aplicaciones en Internet." (www.internet2.com) Mediante estas aplicaciones y protocolos de comunicación exclusivos, Internet 2 pretende asegurar la existencia de una red especializada reservada a los investigadores. Estas aplicaciones deberán asegurar un óptimo uso del ancho de banda de los canales, asegurar la interactividad, facilitar la educación a distancia y la formación permanente. El proyecto forma parte de una iniciativa de la Casa Blanca llamada "Next Generation Internet" (NGI), anunciada en febrero de 1997, cuya meta es asegurar al mundo científico comunicaciones mil veces más rápidas que las actuales (también con el fin de mantener la hegemonía norteamericana en esta área). Pero la filosofía del NGI no descarta la posterior transferencia de las nuevas funcionalidades al sistema "abierto" (Internet-WWW), lo cual no deja de ser inquietante para el mundo académico. Hoy participan en el proyecto 120 universidades, empresas (las principales compañías de telecomunicaciones y computación) y algunas agencias federales estadounidenses, todas las cuales formaron en octubre de 1997 el consorcio UCAID (Corporación Universitaria para el Desarrollo Avanzado de Internet), al cual ya se están asociando universidades de distintos países mientras diferentes gobiernos están estudiando los ajustes tecnológicos que podrán requerir las infraestructuras de telecomunicación de sus países para permitir las conexiones internacionales. Los primeros productos ya aparecieron en el curso del año 1998 y están funcionando ya varios "gigapops" (los nuevos "nodos" optimizados) en Estados Unidos y, desde este año, el primero en Suramérica (en Brasil). En cada una de las universidades que participan en el proyecto existe un equipo de desarrolladores e ingenieros que trabaja para desarrollar y hacer posibles las nuevas aplicaciones requeridas. Además de que las redes de I2 serán mucho más rápidas, las aplicaciones que se desarrollen utilizarán todo un conjunto de herramientas de red que no existen actualmente. Por ejemplo, una de estas herramientas es conocida como garantía de calidad de servicio (QoS o Quality of Service guarantees). Hoy, toda la información que circula por la red recibe la misma prioridad. La implantación de la QoS permitiría a las aplicaciones solicitar por sí mismas una cantidad determinada de ancho de banda o una prioridad específica. Esto permitiría que dos ordenadores que estuviesen procesando una aplicación como la teleinmersión se pudiesen comunicar entre sí a la alta velocidad requerida para las interacciones en tiempo real. Al mismo tiempo, aplicaciones de red menos intensivas como la WWW necesitarían utilizar únicamente la velocidad necesaria para funcionar adecuadamente.

Es importante darse cuenta de que la diferencia de velocidad proporcionará mucho más que una WWW más rápida. Se prevé que una red entre 200 y 1.000 veces más rápida que la actual posibilitará aplicaciones que cambiarán la forma en que la gente trabaja e interactúa por medio de los ordenadores. Aplicaciones como la teleinmersión y las bibliotecas digitales cambiarán el modo en que la gente utiliza los ordenadores para aprender, comunicarse y colaborar. Quizás las más apasionantes posibilidades son las que aun no imaginamos pero que se desarrollarán durante la vida del proyecto I2.

1.3. ¡Los números no resisten!

El protocolo IP es el sistema que permite a los computadores "entenderse" entre sí para la comunicación de datos. Un componente esencial de este protocolo es la forma en que identifica los servidores: los números IP. Los números IP son determinados por los dueños de los dominios (ver más adelante) y se asocian a éstos a través de tablas administradas por los "servidores de nombres" (DNS). Hasta hace poco se utilizaba la "versión 4" del protocolo IP, de la cual se está pasando progresivamente a la versión 6 (IPv6) a fin de permitir un mayor número direcciones, ya que con la versión 4, la capacidad del sistema estaba prácticamente copada. Es un proceso parecido a lo que ocurrió con los números de teléfono de nuestra capital cuando se tuvo que pasar de un sistema de 6 dígitos a uno de 7. En el caso de los números IP, se pasa de un sistema de 4 bloques de cifras a un sistema de 6 bloques (de 256 posibilidades cada uno). Un nombre de dominio es un identificador usado para designar a un computador, o a un conjunto de computadores en la red. Por ejemplo, el nombre "puc.cl" agrupa a todos los computadores de la Pontificia Universidad Católica, mientras que "iluvatar.scc.puc.cl" designa a un computador llamado "iluvatar" dentro del Servicio de Computación -Secico-, que a su vez se encuentra dentro de la Universidad Católica. Internet se ha convertido en un caos de direcciones, del cual es poco probable que se salga algún día. Este caos está compuesto por miles de dominios agrupados en unos 200 "dominios superiores", que son los sufijos finales de las direcciones de Internet como ".com", ".net", ".gov.", "edu.", y "org". Éstos se definieron cuando la web era apenas la vía de comunicación para una elite. A estos dominios genéricos o temáticos (comercio, red, gobierno, educación, organización) se agregaron los dominios territoriales, donde cada país es representado por dos letras (como 'cl' para Chile y 'es' para España). Estos dominios superiores son la primera gran división que deben decodificar los computadores que establecen las conexiones (los "servidores de nombres" o DNS). El gobierno norteamericano, que tuvo algún día tuición sobre los nombres, mientras Internet dependía de la Fundación Nacional de la Ciencia, desistió definitivamente de intervenir en el tema y propuso la creación de un ente internacional, compuesto por compañías privadas, para hacerse cargo de la gestión de las denominaciones de Internet. (No obstante, Washington -preocupado por cualquier decisión relativa a Internet que pueda amenazar la seguridad nacional- se ha reservado el derecho de vetar las decisiones que tome dicho organismo, y no hará efectiva su salida de la gestión de los dominios hasta el año 2000). Si bien ya está establecida la división más importante (los dominios nacionales y los primeros dominios genéricos), se está proponiendo la creación de nuevos dominios temáticos que permitan saber -a partir de la dirección URL- a qué tipo de servidor (y de contenidos) se accede en esta dirección. Algunos países han optado por introducir siglas de dominios temáticos como subdivisión de su dominio nacional, pero esto es poco frecuente por ahora. Los dominios genéricos, ".com", ".edu", ".net" y ".org" pertenecen a empresas privadas. El negocio del registro de dominios de estos tipos ha pasado de ser una actividad monopolística, llevada a cabo en exclusiva por la compañía Network Solutions Inc. (NSI), a un mercado de competencia real, en el que participan unas 49 empresas. Se debe contratar con ellas el nombre de dominio de "segundo nivel" (que corresponde al servidor de Internet) si se quiere ser parte de uno de estos dominios temáticos. Estas empresas "registradoras" son coordinadas por la Internet Corporation for Assigned Names and Numbers (ICANN), entidad sin ánimo de

lucro creada a fines de 1998 para gestionar el nuevo sistema de registro compartido. Sin embargo, aún la NSI mantiene la base de datos central con los nombres de dominios y la ICANN está sufriendo graves problemas económicos por cuanto debería financiarse con aportes procedentes de las cuotas de las empresas registradoras, que aún son mínimas (o rehusadas, como en el caso de NSI). El desarrollo mundial de la Red y la saturación de los dominios genéricos, sobre todo ".com", han provocado una reacción internacional, auspiciada por un organismo denominado CORE (Council of Registrars), que propone la creación de siete nuevos dominios genéricos: .firm, .shop, .info, .web, .rec, .arts y .nom, dedicados respectivamente a empresas, puntos de venta, puntos de información, páginas en Internet, actividades recreativas, actividades artísticas y páginas personales. Así se descongestionaría un poco la red, al menos durante algún tiempo. CORE cuenta con el apoyo de IANA (Internet Assigned Numbers Authority), encargada de la administración de los DNS desde 1984 y de varios organismos internacionales y proveedores de Internet. Los subdominios, dominios institucionales o de "segundo nivel" (como "puc" para la Pontificia Universidad Católica o "ull" para la Universidad de La Laguna) que permanezcan en dominios nacionales son definidos generalmente por organismos públicos o semipúblicos de cada país. Para Chile, por ejemplo, está a cargo de ello el Departamento de Ciencias de la Computación (DCC) de la Universidad de Chile (http://www.nic.cl). De esta forma, las direcciones no sólo tienen un sentido práctico, sino un valor comercial incalculable. Los derechos de una dirección pueden costar miles de dólares y las disputas legales están a la orden del día. Es obvio que una gran empresa, con nombre conocido, querrá tener su propia marca como nombre de dominio (por ej.: www.cocacola.com). La dirección de Internet de una empresa es algo tan importante casi como su nombre o su logotipo. Por ejemplo, alguien que quiera visitar la web del New York Times intentará usar: http://www.newyorktimes.com. En este caso no habrá acertado, y le saldrá un mensaje en su pantalla indicándole que la dirección no existe. Esto no tendría mayores problemas si no fuera porque alguien se ha dedicado a comprar dominios que deberían corresponder a algunos periódicos y ha redirigido a los visitantes de esas páginas a las de la empresa "Stormfront" -vinculada a organizaciones racistas, fascistas y nazis- que los reciben con las palabras "Orgullo Blanco del Mundo", de tinte claramente racista (Diario del Navegante, 11/10/98). Otros han comprado dominios para luego revenderlos a las empresas que legítimamente deberían poseerlos o, incluso, a empresas competidoras, para dificultar el acceso a las empresas originales. Los tribunales han tendido a dar la razón al demandante si contaba con el registro oficial de su marca antes de que fuera solicitado el dominio. Hoy, el registro de marca es una de las cosas que se pueden exigir antes de otorgar un nuevo dominio. (En el caso de Network Solutions, no lo exige previamente pero es el único caso en que acepta un reclamo y una rectificación posterior). De hecho, lo que gatilló la puesta en vigencia de las regulaciones establecidas para el dominio cl fue una guerra de inscripciones de nombres protagonizada por cuatro empresas que, en pocos días, solicitaron tantos nombres de dominios como lo que se había inscrito en los diez años anteriores. Este diluvio de solicitudes incluía cientos de nombres correspondientes a marcas registradas bien conocidas, y generó gran revuelo entre las empresas afectadas, que temieron que su propiedad sobre esos nombres estuviera siendo amenazada. Hoy, el DCC (NIC Chile) exige numerosos antecedentes antes de otorgar un nuevo nombre (y cobra por el trámite que antes era gratuito).

1.4. Motores: ¿de búsqueda o "de pérdida"?

La WWW tiene más servidores y módulos de información que lo que es posible revisar en toda una vida. Como lo recuerdan Smith, Newman y Parks, las aplicaciones diseñadas para acceder a la WWW en condición de cliente -los "browsers" o visualizadores, como Netscape o Microsoft Explorer-, como su nombre indica, han sido diseñados esencialmente para ver la información, no para facilitar la búsqueda o planificar una "navegación", a pesar de que usan la metáfora del viaje. ¡La WWW está hoy diseñada para facilitar la producción y exhibición de contenidos (emisión), pero no para facilitar su recuperación!

Los motores de búsqueda operan en su mayoría desde 1996 (y algunos antes) y no han crecido todos en forma proporcional a la multiplicación de los servidores y de las páginas web (que se estiman ya en más de 200 millones). El siguiente gráfico muestra la evolución de los principales buscadores, la que se diferencia de acuerdo a la política de cada uno. En efecto, si AltaVista, por ejemplo, trata de acumular datos de todas las páginas que logra encontrar (razón por la cual es el más completo de todos, con un registro que supera los 140 millones de páginas web), otros trabajan con criterios de selección más estrictos (como Lycos, con cerca de 40 millones, o Excite, con cerca de 60 millones).

Tanto los motores de búsqueda como los catálogos temáticos tienen todos su propio algoritmo de búsqueda (no público), por lo que generan diferentes respuestas. Ni lo lectores ni los autores disponen de procedimiento alguno que permita alterar la forma en que operen, por lo cual no es posible diseñar las páginas o la estructura de un sitio para que se vea mejor reflejada en un catálogo o una respuesta a una solicitud de búsqueda. (Algo de esto está cambiando, con nuevos atributos del lenguaje HTML, que permiten definir descriptores de contenido de las páginas, pero cada buscador puede atribuir mayor o menor relevancia a este dato). Así, la tarea de buscar implica también encontrar el motor de búsqueda más satisfactorio o combinar varios. La dificultad llegó a tal punto que se crearon sistemas de "meta-búsqueda" (como Inference - http://www.infind.com/ -) que hacen búsquedas paralelas a través de diferentes servicios de búsqueda, comparando las respuestas obtenidas. Pero, nuevamente, los algoritmos utilizados varían y son desconocidos para los usuarios (e inalterables) a pesar de que juegan un rol mucho más significativo a este nivel. Un estudio reciente accesible por la WWW, sin embargo, permite conocer más de cerca y contar con una evaluación -periódicamente actualizada- de los servicios de 15 motores de búsqueda: se trata de "Web Matrix", que muestra una serie de características de cada uno junto con una calificación de acuerdo a diez criterios de evaluación (Ver Slot, M., "Web Matrix").

El producto de una exploración personal a través de uno de estos sistemas de ayuda será una mini-red de nodos visitados y de páginas. Entre éstas, el lector establecerá -mentalmente o eventualmente mediante anotación en su computador- vínculos relacionados con el contenido informativo, los que, probablemente, no estarán representados por hipervínculos informáticos, a

no ser que construya una "página web" en su computador, con las anclas y vínculos necesarios para acceder a estas páginas externas o a las copias que puede guardar de ellas. Pero -al momento de redactar este texto- las aplicaciones actuales no permiten crear estos vínculos en forma automática ni menos apuntar a posiciones específicas en el interior de una determinada página, a menos que se utilice un editor de HTML para modificar cada una de ellas, lo cual es evidentemente engorroso y exige un avanzado conocimiento de los procedimientos requeridos.

Estas críticas han llevado al surgimiento de dos grandes iniciativas tendentes a modificar los servicios y ajustarlos mejor a las necesidades de los usuarios: por una parte la estructuración de sub-redes específicas -como Internet 2, que será privativa de universidades y centros de investigación-, y las aplicaciones de hipertexto de "cuarta generación". De este modo, ya existe otro conjunto de aplicaciones cliente-servidor, el "HyperWave", que permite manejar de esta forma los vínculos, pero es hoy poco difundido. Es compatible con las páginas web comunes (puede leerlas) y es posible que inspire una próxima generación de web o que se utilice en Internet 2.

Mientras tanto, solo resta tratar de precisar lo mejor posible los criterios de búsqueda formando conjuntos de palabras unidos por operadores lógicos que informen al servidor de nuestras exigencias. Los operadores más comunes para restringir búsquedas son las comillas (buscar frase completa), "AND" o "+" (incluir) y "NOT" o "-" (excluir). Para más detalles se puede consultar: http://www.searchenginewatch.com/facts/powersearch.html

2. Enfermedades infecciosas

En otro momento, hemos hablado de Mercurio, el mensajero de los dioses, y de sus problemas -técnicos- para realizar su tarea. Hemos de hablar ahora de Marte y de los objetivos no muy "santos" de algunos usuarios de la red de redes. El conflicto de Kosovo ha sido una oportunidad para descubrir que expertos "internautas" se unían para combatir a Milosevic y las instituciones serbias a través de Internet. También están presente en la WWW -desde hace tiempo- agrupaciones revolucionarias que no trepidan a recurrir al terrorismo como el IRA, la ETA, el Hizbollah, etc. ¿Puede Internet transformarse en un arma de guerra, militar o comercial, además de ideológica?

2.1. Guerra informática (Information warfare, IWar)

En el campo de la "guerra digital", se distingue habitualmente la guerra informática (Information warfare, IWar), la guerra de red (Netwar) y la guerra cibernética (Cyberwar).

La guerra informática es un concepto general, que se funda en las debilidades de las redes informáticas y la posibilidad de aprovechar sus defectos para causar daños a un "enemigo" que puede ser desde el computador de una pequeña empresa hasta los sistemas militares de un estado. Si bien la idea básica es esencialmente militar, las herramientas de esta guerra están también al alcance de civiles y -lamentablemente- de terroristas. El objetivo es afectar de algún modo el computador o la red del oponente para entorpecer su desempeño o destruir completamente su capacidad operativa, lo cual ya es posible con el mero envío de un virus.

La guerra de red o Netwar se refiere a conflictos amplios entre naciones o sociedades. Implica tratar de destruir, dañar o modificar lo que conoce o piensa una población-meta, por ejemplo para provocar un cambio de opinión o inducir a decisiones erróneas. Para ello pueden recurrirse a tácticas de propaganda, "subversión cultural", interferencia con medios locales, infiltración en bases de datos, etc. También puede ser usado por los gobiernos para combatir grupos disidentes, terroristas o traficantes. No se trata, por lo tanto, de dañar la operatividad de un computador o una red, sino de afectar la información contenida en ellos, ojalá sin que el oponente se dé cuenta.

La "guerra cibernética" implica mucho más que la "guerra informática" (IWar). Si bien involucra tecnología informática, se refiere a la utilización de ésta para conducir operaciones militares típicas: desde conocer (espiar) hasta destruir físicamente los recursos del oponente. Incluye desde la infiltración en los sistemas informáticos enemigos para obtener información hasta el control de proyectiles mediante computadores, pasando por la planificación de las operaciones, la gestión del abastecimiento, etc.

Para entender con facilidad el concepto de "IWar", se cita el ejemplo -ficticio- de la "Impresora Manchuria": se trata de una impresora láser de alta calidad y bajo precio, vendida a un país extranjero, que contiene un código de auto-destrucción. Una vez instalada masivamente, bastaría que el productor envíe por la red el código secreto para destruir la mayor parte del parque de impresoras de ese país. Lo mismo podría ocurrir con computadores de alta tecnologías (por ejemplos destinados al control aéreo) o con cualquier versión de sistema operativo de los PC.

De hecho ya existen y son utilizados ciertos tipos de "bombas lógicas" en software comerciales, como es el caso de rutinas que desactivan (cierran o bloquean) una aplicación en versión "demo" después de una fecha o un período de tiempo determinado. Hace falta muy poca imaginación para pensar en otras aplicaciones del sistema, mucho más destructivas: un demo de un procesador de palabras, por ejemplo, podría borrar el procesador de la competencia instalado en el disco duro o "actualizar" los archivos de documentos creados con versiones anteriores, obligando a comprar la nueva versión. Los virus son sólo otra familia de armas del mismo tipo.

La guerra informática puede ser de tres clases según Winn Schwartau -que publicó un libro sobre el tema-:

Clase 1: Guerra antipersonal

Esta clase de "guerra" incluye los ataques contra la privacía de los datos personales. Esto implica la revelación (o búsqueda no autorizada) de datos existentes en bases de datos que se suponen confidenciales o su alteración. Un ciudadano promedio tiene hoy muy poca posibilidad de controlar los datos que le conciernen y que han sido recopilados por diversas empresas (al abrir una cuenta corriente, al obtener y utilizar una tarjeta de crédito, al contestar encuestas, etc.). Estos datos no sólo pueden ser obtenidos ilegalmente por piratas sino que pueden ser vendidos por las empresas que los poseen y utilizados para fines de marketing u otros. Lo peor es que esta información puede ser alterada y cualquiera de nosotros podría aparecer con un prontuario judicial (falso), sin saberlo y sin poder reclamar. De ahí que los países de la Unión Europea formularan leyes bastante exigentes en torno a la protección de los datos personales y estén desincentivando el comercio electrónico con países que no tienen leyes equivalentes (propósito de la "Directiva 95/46/CE" del Parlamento Europeo, de octubre de 1998). Las condiciones mínimas de protección que insta a cumplir la directiva van desde la necesidad de que el ciudadano sepa dónde y para qué está almacenada su información personal, tener acceso a ésta en todo momento y poder modificar los datos incorrectos, así como evitar su utilización ilegal para procedimientos de mercadeo o publicidad. Esto ha creado dificultades en los intercambios con Estados Unidos cuya política consiste en remitir el problema al sector privado sin legislar al respecto.

Clase 2: Guerra corporativa

Este es el tipo de guerra que pueden mantener corporaciones y empresas de todo el orbe, recurriendo a métodos de piratería computacional para penetrar los sistemas computacionales de sus competidores, obtener acceso a sus bases de datos y a los resultados de sus investigaciones. Podrían incluso destruir antecedentes, haciendo que dicha destrucción parezca un accidente fortuito producto de un virus, con lo cual podrían ponerse en ventaja en el desarrollo de un nuevo producto. Este tipo de acción no es nuevo y se conocen varios casos ocurridos durante la guerra fría entre los EE.UU. y la URSS. Una nueva forma de combate de este tipo se ha desarrollado desde entonces: se trata del envío de estudiantes al extranjero, con la misión de "mantener los ojos abiertos" tanto en sus universidades como en las empresas que visiten o donde hagan su práctica, para luego informar a sus patrocinadores. Parecida es la táctica -ya casi diaria- de contratar talentos en empresas competidoras o de un sector en el cual se desea ingresar, para que traigan su "know-how" y se fortalezca con él las propias potencialidades o nuevos proyectos. Aunque algunos consideran que este fenómeno es algo connatural al mercado del trabajo, otros lo consideran una práctica desleal y algunos han llegado incluso a entablar por ellos demandas ante los tribunales (Amazon, la famosa librería enlínea, fue demandada en 1998 por contratar a un experto de otra firma experta en ventas enlínea). Otra forma de combate es la difusión por Internet de información falsa acerca de productos de la competencia. Así, por ejemplo, una empresa farmacéutica podría dañar seriamente las ventas de otra compañía dando a conocer una supuesta información científica acerca de contraindicaciones de un determinado fármaco producido por ésta. Hasta que se descubra el fraude, miles de médicos dejarían de recetar el remedio y las pérdidas serían enormes. Lo mismo podría pasar con relación a productos computacionales y otros, donde le sería muy difícil al consumidor controlar la veracidad de la denuncia. Ha pasado después de un accidente de un avión ATR, cuando un sitio web explicó lo ocurrido basándose en falsas especificaciones técnicas.

Según señala Haeni, la "guerra corporativa" ya es cosa de todos los días, aunque muy poco incidentes son dados a conocer debido a que multiplicarían los efectos negativos. Según un informe del Consejo de Estado de Francia, France Telecom sería objeto de 900 intentos de penetración de "hackers" por cada fin de semana. Sólo en 1995 el Departamento de Defensa Norteamericano detectó 38.000 ataques a sus sistemas.

Clase 3: Guerra global

Esta categoría se aplica tanto a las relaciones entre industrias y poderes económicos como entre naciones. Ya no se trata de robar secretos o producir algún daño limitado sino de recurrir a métodos que permitan destruir al enemigo. Aquí los recursos a invertir son lo de menos porque -aunque cuantiosos- son menores que los que se requerirían para una guerra convencional. Una inversión de 200 millones de dólares en recursos para la guerra informática serían suficientes para poner de rodillas al sistema económico norteamericano, lo cual está al alcance de cualquier país del tercer mundo. La relación "costo-beneficio" es -desgraciadamente- muy ventajosa para los terroristas y los gobiernos enemigos. La distancia no juega ningún papel y no existen medidas preventivas que puedan dar una seguridad absoluta.

La CIA plantea que sus futuros enemigos no pretenderán atacar el país con armas nucleares sino penetrando en sus sistemas informáticos y causando verdadero daño a su poderío militar y a su economía. ¿Y por qué los terroristas van a elegir este tipo de acciones? Pues hay dos razones de peso. La primera es que a través de Internet se mueven billones de dólares en pequeñas transacciones comerciales con una protección bastante baja. La segunda razón es que se pueden causar desastres militares casi tan graves como los que se pueden ocasionar en el campo de batalla y sin salir de casa. (Diario del Navegante, 7/7/98).

Se debería quizás agregar una "Clase 4"

La "guerra personal" contra un estado. En efecto, el 28 de diciembre de 1998, un grupo de hackers norteamericanos, la "Legion

of the Underground", ha declarado la "ciberguerra" contra Irak y China, amparándose en que en ambos países no se respetan los derechos y libertades fundamentales y llamando a la destrucción masiva de todas las redes informáticas de estos países. Su primera víctima ha sido el servidor oficial del gobierno iraquí, que sucumbió el 7 de enero. Sin embargo, el resto de la comunidad de hackers se opone frontalmente a este tipo de medidas. En el manifiesto que estos otros grupos publicaron, declaran "oponerse totalmente a cualquier intento de usar el poder del hacking para amenazar o destruir las infraestructuras de comunicación de cualquier país", por cuanto "las redes de comunicaciones son el sistema nervioso de nuestro planeta". También, a raíz del bombardeo de la embajada china en Belgrado (mayo, 1999), los internautas chinos han inundado la Red con consignas anti EEUU, han entrado en la web de la embajada estadounidense y han colapsado las charlas en directo, condenando las acciones de la Alianza.

2.2. Terrorismo y antiterrorismo

En 1997 se descubrió que la ETA tenía publicadas páginas de propaganda en diversos sitios de Internet. Esto dio origen a una campaña de protesta, enviándose numerosos mensajes de correo electrónico a los responsables de dichos sitios y a los principales motores de búsqueda. Si AltaVista, Infoseek, Yahoo, Lycos deciden no almacenar estas url, difícilmente ETA y los proetarras podrán divulgar sus mensajes. En Ole, un buscador español que participó activamente en la campaña, nunca han estado localizadas. Si bien enviar opiniones y protestas es un medio legítimo de expresión y de presión, no lo es el generar en forma automática miles de mensajes idénticos -con el mismo contenido reprobatorio o con un mensaje ilegible de miles de caracteres- con el fin de "tumbar" al servidor en cuestión, cosa que ocurrió efectivamente y que fue la razón final para que el Institute for Global Communications (IGC) -principal afectado- dejara de sustentar el Euskal Herria Journal, diario en que aparecía la página de la ETA. Este medio de contraataque es un claro procedimiento de guerra informática -llamado "mailbombing"-, igual de condenable que la propaganda en favor de un movimiento terrorista. Hay que aclarar que el IGC se presenta como una organización sin fines de lucro que provee servicios de Internet a "activistas que trabajan por la paz, la justicia social y económica, los derechos humanos y la sustentabilidad del entorno". (Es posible preguntarse por qué razón defendían la presencia de la ETA entre ellos). IGC, en su comunicado -que reemplazó las páginas del diario etarra-, aceptó los legítimos mensajes expresando disconformidad, pero protestó con razón ante el mailbombing que afectó a su servidor y, con ello, a sus clientes habituales. El Euskal Herria Journal se podía ver en http://osis.ucsd.edu/~ehj/. Desapareció de IGC y de Geocities, donde también estaba. El movimiento islámico Hamas tiene su propio sitio web (http://hamas.org "no oficial", en inglés; tiene enlace a un sitio oficial en árabe). También tiene sitio propio el Hizbollah (www.hizbollah.org), el KuKluxKlan y múltiples otros grupos extremistas. El sitio del Sinnfein, de Irlanda del Norte, se cuida de remitir a otro sitio al referirse al IRA (a páginas de estudiantes de la Universidad de Texas). Pero propaganda y mailbombing no son las únicas expresiones de presencia del terrorismo. Así, por ejemplo, en agosto del 98, los Tigres tamules, rebautizados para esa oportunidad como "Tigres negros de Internet", lanzaron un ataque contra la red que une las embajadas de Sri-Lanka, bloqueando todas las casillas electrónicas de sus representaciones en el mundo. En septiembre, los mensajes secretos del servicio de seguridad del presidente de los Estados Unidos aparecieron divulgados en un servidor de Internet.

2.3. La indecencia

El tema que llama más especialmente la atención de padres de familia y educadores es la presencia de páginas con sexo explícito y otros contenidos pornográficos. Aunque es una fracción ínfima en el concierto de todas las páginas de web (estimada en menos del 3%), algunas de esas páginas se encuentran entre las más visitadas, por lo cual no es difícil encontrarlas.

En 1996 se intentó legislar sobre la materia en los Estados Unidos ("Communications Decency Act"), pero la Corte Suprema resolvió finalmente que prohibir la publicación de estos contenidos iba en contra de la enmienda constitucional que consagra la libertad de expresión, siendo el principio que no se prohibe lo que el usuario (lector) puede evitar por su propia decisión. También se tomó en cuenta que ya estaba prohibida la producción de publicaciones con contenidos "claramente obscenos" o de pornografía infantil. Se concluyó que impedir el acceso a las páginas sobre sexo era de responsabilidad de los padres de los menores, y no una responsabilidad pública o de los servidores de Internet. Promover sistemas que ayuden a los padres a seleccionar los contenidos es hoy la posición oficial del gobierno norteamericano.

El hecho es que los servidores comerciales que ofrecen pornografía no son tan fácilmente accesibles, ya que funcionan sobre la base de suscripciones -pagadas- (y, por lo tanto, se requiere tener una password para acceder a sus páginas). El peligro real para los menores, por lo tanto, no está ahí, sino en las numerosas páginas no comerciales, que los pornófilos han creado e instalado en servidores que acogen sin control alguno a quienes quieren publicar (como es el caso de "Geocities", uno de los sitios más grandes y más famosos, creado justamente -al principio- con el fin de abrir una tribuna a homosexuales y lesbianas).

La ley de uno u otro país -para controlar esta difusión- es en gran parte letra muerta en Internet. Siempre se puede encontrar la forma de publicar una página en un país donde no tiene vigencia dicha ley. Ya ha ocurrido en Chile cuando algunos medios de prensa publicaron en páginas web -en el extranjero- las informaciones que los tribunales prohibían difundir en el país (como en el juicio por lavado de dinero). Obviamente, legislar no es una solución y sí lo es el control parental (y el auto-control), lo cual ha sido confirmado -mediante encuestas- como opinión mayoritaria en diversos países como Estados Unidos y Australia. Como dicen algunos investigadores norteamericanos: "Si algunos padres deciden que no deben intervenir al respecto, no hay razones para creer que deba intervenir el gobierno". Hay muchos otros temas -y situaciones- que los padres pueden querer controlar y no piden para ello la intervención del gobierno.

Numerosos países, sin embargo, tienen una legislación parecida o más dura que la de Estados Unidos con relación a publicaciones pornográficas. A pesar de que se pensaba que no podrían tomarse acciones contra éstas en Internet, por la dispersión de las fuentes, demostró lo contrario la "Operación Catedral", de septiembre de 1998, que se llevó a cabo simultáneamente en unos veinte países, bajo la coordinación de Interpol. ¡Se destruyó de este modo una red de pedofilia que contaba con unas 100.000 fotografías en Internet!

El siguiente problema es cómo dejar que los niños "naveguen" por Internet sin estar constantemente "mirando sobre su hombro" las páginas a que accedan. Éste ya no se considera un problema real, ya que -para solucionarlo- se ha creado software especializado, con dos formas de operar:

el bloqueo exclusivo: aplicaciones que contienen una lista de páginas o servidores a los cuales no se puede acceder (ejemplo: "CyberSitter"); algunos incluyen filtros que impiden la lectura de una página que no está en la lista si contiene determinadas palabras que el usuario puede definir (ejemplo: "Net Nanny")

el acceso inclusivo: aplicación o servidor que contiene un catálogo de servidores autorizados (ejemplo: "Specs")

el sistema mixto: existen aplicaciones que combinan ambos sistemas (ejemplo: "CyberPatrol", que usa la clasificación RSCAi de la que hablamos más abajo).

Los softwares de bloqueo, sin embargo, no son del todo seguros: pueden fallar si los sitios que se pretenden eliminar toman la precaución de evitar las palabras claves que se utilizan en los filtros. En este sentido, los de acceso inclusivo son más seguros, pero pueden limitar muchísimo la navegación (entre otras cosas, no pueden permitir el acceso a un "motor de búsqueda"). Al respecto es bueno saber que los principales directorios de web (como Yahoo o Galaxy) evitan generalmente esta categoría de contenidos.

La pornografía y la pedofilia no son los únicos temas que pueden producir escozor en Internet. También ha surgido el tema del racismo y, más globalmente, de la difusión del odio. Según el Centro Simon Wiesenthal, existen más de 600 sitios que promueven el racismo y el odio. Están creciendo las demandas para clausurar estos sitios y varios proveedores de Internet de diversos países han decidido bloquear sus direcciones. Pero otras organizaciones internacionales -como Internet Freedom- plantean que los proveedores no deberían intervenir y que el principio de la libertad de expresión ha de mantenerse a toda costa, a pesar de los abusos.

En otra posición, Internet Watch Foundation ha propuesto que los sitios de web sean clasificados tal como ocurre con las películas, a fin de facilitar el control y bloquear los accesos indeseables. Es también el enfoque que ha adoptado el Consorcio de la WWW (W3 Consortium): el de la autocalificación por los emisores y de selección automatizada en el ámbito de los usuarios. Bajo su patrocinio, el Laboratorio de Ciencias de la Computación del MIT ha desarrollado la tecnología "PICS" (Platform for Internet Content Selection) destinada a facilitar a los usuarios que filtren la información de acuerdo al grado de violencia, sexo o abuso de lenguaje. Este sistema ya ha sido integrado a las últimas versiones de los browsers como Netscape y Explorer. Exige que los creadores de páginas web incluyan en ellas la calificación (con una etiqueta "Meta"), de acuerdo a la escala definida por el RSCAi (Recreational Software Advisory Council on the Internet) -una asociación sin fines de lucro "al servicio de la familia", que propende a la toma de "decisiones informadas"-.

De ahí que, hoy, se puede distinguir entre servidores PICS (que incluyen la calificación) y no-PICS (o "PICS-free", algunos se publicitan como tales, como una forma de protestar contra todo tipo de censura). A mediados de 1998, 60.000 sitiosweb ya usaban la PICS. Para no ser excluido, si el usuario habilita esta función en su navegador, una página web deberá forzosamente tener embutido este dato. Obviamente, si es puesto por el emisor y decodificado sólo por el usuario -sin comprobación por terceros-, es aún posible engañar a los lectores, por lo que esta solución es bastante limitada.

2.4. La escoria humana

La droga, su publicidad, obtención y manejo de beneficios no están ausentes de Internet. No sólo el correo electrónico encriptado es un medio de comunicación entre traficantes, también están proliferando las páginas web que promueven su consumo o aconsejan, por ejemplo, acerca de su cultivo, como en el caso de la marihuana. Existen miles de páginas que, ya sea desde el punto de vista legal, científico, histórico o sociológico versan sobre las drogas y cuanto las rodea. Al menos así lo ha manifestado la ONU a través de un informe elaborado por la Junta Internacional de Fiscalización de Estupefacientes (JIFE) donde se hace hincapié en el riesgo que esto entraña. Según el diario español "El Mundo", existían en 1998 cerca de 29.000 páginas con referencias a la marihuana. Entre los sitios con mayor "prestigio" destaca la Asociación Ramón Santos de Estudios sobre el Cannabis, una ONG con sede en Barcelona, que tiene como objetivo el estudio de esa planta. Existen páginas que se concentran exclusivamente en los aspectos medicinales y otras que ofrecen semillas y derivados. Pero gran parte de las informaciones relacionadas con la marihuana en Internet se centran en aconsejar a los cultivadores. No descuidan ningún aspecto: desde la época del año propicia para la siembra hasta la temperatura, pasando por la importante distinción entre macho y hembra, ya que las femeninas son las únicas fumables. Y no faltan quienes promueven la legalización de todas las drogas. Para evitar que Internet y la globalización sean agentes del narcolavado, se formó en 1995 el "grupo de Egmont" (del nombre del palacio Egmont-Arenburg de Bruselas, donde se constituyó), que reúne a "Unidades de Inteligencia Financiera" de diversos países, decididos a expandir el uso de la red global de computación para diseminar información sobre narcotráfico y

lavado de dinero e interconectar las unidades de inteligencia de todo el mundo. Con el mismo propósito, expertos de todo el mundo se congregaron el 30 de junio de 1998 en Buenos Aires. La principal preocupación, en este caso, no era tanto el fluir de la droga misma sino la posibilidad de usar Internet para realizar un comercio ficticio y, así, lavar dinero. Eduardo Amadeo, jefe de la oficina de lucha contra el narcotráfico de Argentina, dijo que la globalización y apertura de los mercados abrían nuevas oportunidades para el lavado de los fondos procedentes del mercado ilícito de la droga, que según cálculos de las Naciones Unidas mueve unos 400.000 millones de dólares al año.

2.5. La fascinación por lo ajeno

El robo o la destrucción de información en Internet es también, desde sus inicios, una actividad que fascina a numerosos "expertos", que se valieron el calificativo de "piratas". El término "pirata" se aplica en sentido amplio a todo quien hace algo indebido con recursos de programación. Pero se han de distinguir diferentes conceptos y realidades. Limitándonos aquí a manipulaciones a través de la red:

los "hackers" (hacheros): son programadores que asumen el desafío que plantean los sistemas de computación (y entre ellos la protección de datos) y tratan de usar o desarrollar técnicas para quebrar estos sistemas, sea por puro "deporte" sea como labor crítica dentro de una organización, para mejorar sus propios sistemas de protección;

los "crackers": son los que hacen lo mismo o aún más con fines maliciosos, para hacer un uso indebido de la información obtenida o para destruir ésta causando daños que pueden ser incalculables.

La defensa reside en la instalación de cortafuegos (FireWalls), que son sistemas de hardware y software que separan a las redes privadas de las redes públicas, definiendo reglas o perfiles de usuarios (según la dirección desde donde se conectan) para limitar y controlar el acceso externo a ciertos servicios o ciertas máquinas de la red interna. Son la principal defensa frente a los accesos no autorizados y de su calidad depende el grado de dificultad que tendrán los piratas para ingresar al sistema y hacer de las suyas. Nadie está a salvo: han sido afectados desde bancos hasta la NASA y el Pentágono, ya que todo esquema de protección puede ser "quebrado" de algún modo, si se cuenta con recursos y conocimientos adecuados.

Una administración de servidores orientada a la seguridad ha de considerar esencialmente tres componentes:

el control de acceso,

el control de la presentación (de lo que puede ver el usuario) y

el control de la distribución.

* El control de acceso debe permitir identificar cada usuario que se conecte y, de acuerdo a sus características, otorgarle los privilegios que le correspondan jerárquicamente, desde sólo leer las páginas web, hasta ocupar algún software del servidor para efectuar operaciones y administrar -por ejemplo- las finanzas de la institución. Esto significa no solamente establecer sistemas que requieren password (y bases de datos protegidas que contengan estos password) sino también sistemas de encriptación de datos, para que ningún usuario no autorizado los pueda captar. La mayor dificultad será, posiblemente, la necesidad de permitir el acceso externo (usuarios no registrados) con "privilegios" extremadamente limitados, junto con usuarios internos registrados con acceso a contenidos más delicados. Es aquí donde los sistemas de seguridad intervienen en forma más decisiva y donde pueden entrar en conflicto con la flexibilidad.

* El control de presentación define las interfaces a través de las cuales los usuarios pueden acceder a las aplicaciones y datos, generando "vistas" ajustadas al tipo de usuario. Los servidores tienen generalmente interfaces de diálogo (sólo texto), que son cada vez menos conocidas y manejables para usuarios comunes, que requieren interfaces con menú y con posibilidad de operar con ratón. En aplicaciones específicas de telemática "no web", se requiere por lo tanto adaptar mucho más la interfaz al usuario, para que no necesite un entrenamiento extraordinario y tenga una interacción más natural. El sistema también debe estar diseñado para no exhibir información irrelevante (no requerida) y, eventualmente, combinar datos de diferentes fuentes (diferentes bases de datos) sin requerir del usuario operaciones especiales para combinarlas. El uso de estas interfaces es, también, un sistema que puede facilitar el control de acceso y aumentar así la seguridad.

* El control de distribución verifica qué software utilizan los usuarios y se asegura que todos tengan las aplicaciones y versiones adecuadas para su mejor desempeño. La tendencia es a instalar la parte más "dura" (la "inteligencia" de las aplicaciones) en los servidores, para que sea suficiente, algo como un visualizador de web para el usuario. Pero es conveniente que el administrador de servidores también administre el software repartido en los computadores de los clientes internos, si se quiere una interacción óptima.

En la World Wide Web, se ha desarrollado el protocolo SSL (Secure Locket Layer) que proporciona encriptación de datos, autentificación del servidor e integridad en la conexión de web. Descansa en un software especial instalado en el servidor de web, el que se identifica como "https:" (Secure HyperText Transfer Protocol) y con el icono de llave (o candado) entero en vez de llave quebrada (candado abierto) en la barra de estado (borde inferior). Los datos enviados a través de esta conexión (como el número de tarjeta de crédito, al hacer una compra, por ejemplo) no pueden ser descifrados antes de llegar a su destino. Al

contrario, los datos enviados por formularios en páginas no seguras (con icono de llave quebrada) viajan "en claro" igual que los mensajes de correo electrónico. El sistema S-HTTP es totalmente compatible con el HTTP tradicional y le agregan solamente elementos relativos a la seguridad de la transmisión (atributos de campos y encapsulamiento de datos de los formularios).

2.6. ¿La policía sobrepasada?

Scotland Yard también opina que la piratería a través de las redes de computadores será el rubro criminal más importante del próximo siglo. Frente a la nueva criminalidad que puede desarrollarse de este modo en Internet, los medios de las policías son bastante limitados aunque no totalmente ineficaces, como ha sido demostrado con la operación "Catedral" de septiembre de 1998, en que fueron detenidos centenares de sospechosos de pertenecer a una red de pedofilia, que abarcaba más de diez países. El FBI anunció que está en proceso de crear una unidad especial para perseguir el fraude en Internet (Internet Fraud Complaint Center). Recibirá las quejas en línea, para atender más eficientemente a los afectados, según anunció Julie Miller, portavoz del organismo. El FBI investigará los casos más importantes, mientras los casos menores serán derivados a las autoridades estatales o locales que correspondan. La policía francesa cuenta desde los años 80 con una sección de informática y desde 1997 con una "célula Internet" con una docena de investigadores especializados. Despachó más de 400 procedimientos en un año (1997), en su mayoría por estafas y pirateo de software. Pero Estados Unidos y los países anglosajones disponen de recursos mucho más poderosos como la red de espionaje satelital "Escalón", coordinada por la Agencia Nacional de Seguridad, que es capaz de filtrar dos millones de conversaciones telefónicas, fax y correo electrónico por minuto. Con el objetivo de conocer con detenimiento las nuevas formas de lo que se ha venido en llamar ciberdelitos, policías españoles, italianos y alemanes participarán en el proyecto Falcone, que incluye investigaciones y un curso de formación para agentes a través de un campus virtual basado en la experiencia de la Universidad Oberta de Catalunya. La investigación se centrará en detectar las nuevas técnicas de delincuencia en entornos informáticos, especialmente las que se producen de forma organizada, y en el estudio territorial de las legislaciones, algo que permitirá elaborar propuestas concretas para adecuar la legislación europea. La colaboración internacional, en el marco de Interpol, está creciendo y está empezando a dar frutos en los cuales pocos confiaban, ya que se considera generalmente a la Internet como "incontrolable". Se está empezando a demostrar que no hay impunidad total. En la mayoría de los países existen ya leyes aplicables. Pero la justicia es demasiado lenta: se requieren muchas veces días, semanas o meses para obtener órdenes de perquisición, mientras los servidores y los mensajes se crean y desaparecen en cuestión de horas o días. Pero muchos dejan huellas y la policía ha aprendido a descubrir y seguir éstas. La mayor dificultad, sin embargo, parece estar en la no-denuncia de delitos por empresas afectadas, para evitar la pérdida de credibilidad de sus sistemas de seguridad. Para mantenerse a cubierto y ayudar a la policía, se sugiere a los proveedores de Internet que conserven no sólo una base de datos de sus clientes sino también de todos los intercambios de mensajes, incluidas las consultas de páginas web. De hecho, los servidores de páginas web cuentan hoy con un sistema que registra la dirección (IP) de quién sea que las consulte. Generalmente utilizado para generar estadísticas respecto de las consultas, el sistema permite identificar cada lector y saber qué cosa lee (otra información que podría también ser catalogada y utilizada para fines de marketing). Esta lucha contra el delito es lo que ha llevado a Francia y algunos otros países a limitar o prohibir las comunicaciones encriptadas. En Francia, las empresas que ofrecen sistemas de encriptación deben comunicar sus claves a un organismo del estado, que podrá entregarlas a la policía en caso de necesidad. En los Estados Unidos, el ejército ha formado un grupo especial -como los SWAT- para luchar contra los ataques de hackers. La lucha se centra principalmente contra quienes han intentado atentar contra las instalaciones militares, pero desde dentro, es decir, a través de sus redes informáticas. El nombre de la unidad no tiene desperdicio: The Army Computer Emergency Response Team (ACERT), algo así como ‘equipo de respuesta de emergencias con ordenadores del ejército’. La base la tienen situada en el centro de información de las Fuerzas Aéreas Kelly AFB, en Texas. Pero aparentemente el peor problema de las fuerzas policiales es que los bandidos cambian de equipos y programas cada seis meses, mientras en los organismos policiales, el cambio es sólo, en promedio, cada 48 meses.

3. "El imperio contraataca"

Como si lo anterior fuera poco, la "aldea planetaria" se ve atacada por el mayor imperio informático del momento. Microsoft, como lo señala el juez Jackson en su reciente fallo, no sólo "ejerció su poder monopolístico mediante una conducta predatoria que atenta flagrantemente contra la competencia", sino que viene desarrollando una compleja estrategia para lograr el control total de la gran tela. La principal característica de Internet ha sido siempre su absoluta compatibilidad: opera y se ve exactamente igual independientemente del sistema operativo que se esté usando. Pero esto no es del gusto de Microsoft. Trató primero de ignorarla y desarrollar su propia red, "The MS Network", lo cual no prosperó. Entonces, cambió de estrategia y atacó en diversos planos. En el ámbito de los "clientes", ha logrado controlar ya a cerca del 90% de los usuarios de computadores personales reemplazando el sistema operativo DOS por versiones de Windows que integran el browser Explorer y se le ha acusado repetidamente de haber incluido una rutina (del tipo "cookie") que le permite conocer características de todos los PCs que lo utilizan para conectarse a la red e incluso, quizás, de leer la totalidad del contenido del disco duro de cada uno. Además, en 1996, logró que el Explorer fuese el navegador por defecto de America Online, cosa que felizmente fue revertida posteriormente con la compra de Netscape por America Online el año pasado. Para asegurar su dominio, ha hecho convenios con gobiernos para que se instalaran solamente PCs con el sistema Windows en reparticiones y escuelas públicas, logrando incluso -en algunos casos- que tramitaciones legales de las empresas o de los ciudadanos estén condicionadas al uso del Office sobre Windows. (¿En qué congreso internacional no se exige hoy que las ponencias sean escritas en "Word" para PC?) Junto con el Explorer, en otro decidido ataque contra el concepto fundador de Internet y de la WWW -que es la máxima compatibilidad para facilitar los intercambios-, rompió su compromiso con Sun relativo al uso del lenguaje Java y desarrolló su propia versión de Java y Javascript, no compatibles con otros browsers. (Java y Javascript son lenguajes de programación que

permiten crear aplicaciones que funcionan en todos los sistemas operativos sin necesidad de modificaciones, de ahí su popularidad en Internet, y el disgusto de Microsoft). Al mismo tiempo atacó el lenguaje HTML -el básico de las páginas web- lanzando el paquete de aplicaciones "Office 98" con capacidad para generar páginas web usando las etiquetas Html (las marcas propias de este lenguaje) de un modo no conforme con las especificaciones del W3C, que es el consorcio internacional que regula este lenguaje y la forma de operar de la WWW. De este modo, las páginas generadas, por ejemplo, con "Word", no se verán correctamente si no se cuenta con el Explorer (o versiones posteriores, adaptadas, de otros browsers, obligados a "ponerse a tono"). En el mundo de los "plug-ins", que extienden las funciones del browser para exhibir secuencias televisivas, ha desarrollado su Windows Media Player como respuesta al RealPlayer, de Real Networks Inc. Por el lado de los servidores, ha seguido una estrategia parecida desarrollando el Windows NT (hoy Windows 2000) y la aplicación FrontPage. Felizmente, en este campo, la Fuerza del software libre está logrando derrotar al Imperio: el sistema operativo Linux y el "web server" Apache son utilizados en el 70% o más de los sistemas medianos (mientras los más grandes residen en computadores con sistema Unix). También se han denunciado repetidamente diversas fallas de seguridad del Outlook Express, la aplicación de correo electrónico, que permitían acceder fácilmente -sin permiso- a los mensajes de cualquier usuario. Pero el "lado oscuro de la Fuerza" no se extiende solamente sobre los servidores y clientes de la WWW: también ataca áreas de contenido y áreas de soporte físico. En efecto, Microsoft ha comprado diversas empresas proveedores de servicios de Internet (portales, buscadores y proveedores de casillas de correo e.). Simultáneamente se ha asociado con importantes empresas de telecomunicaciones y de televisión de Estados Unidos, logrando controlar parte importante de las redes. Se unió a Ericsson en el mercado de los celulares. También controla el desarrollo de los sistemas y aparatos (las "TV set top box") que permitirán navegar por Internet utilizando televisores y, a la vez, contar con servicios de televisión digital a pedido ("Digital pay per view"). En el nuevo campo de los "libros digitales", ataca el establecido "Acrobat" con su propio "e-book Reader", formando alianza con varias grandes editoriales y librerías como Barnes&Noble. Con el sistema Windows CE, ya controla la mayor parte de los "asistentes personales" o computadores de bolsillo (PDA). ¡Etc., etc.! Bill Gates, a través de su empresa Corbis, ha comprado los derechos de reproducción digital de la mayoría de los museos del mundo, así como las principales colecciones históricas de fotografías.

> "La posición monopolística de Microsoft, así como el hecho de que utiliza tal posición para expandir su monopolio, representa un grave problema para el mundo libre. Si una compañía elimina las posibilidades de elegir de los consumidores, y subordina la organización de Internet para su propio beneficio se elimina lo que Internet ha sido hasta ahora: democrática, libre e incensurable y se llega a lo que Scott McNealy, presidente de Sun, llama la economía de planificación central de Bill Gates: el absolutismo, que se creía superado." (Di Pedra)

Conclusión

Es de esperar que los paladines de la democracia, como nuevos Pasteur y nuevos "jedi", logren derrotar tanto las infecciones como los intentos imperialistas. Pero esto también depende los usuarios en general y de su conciencia del peligro, es decir de todos nosotros.

El presente trabajo es una versión actualizada de la ponencia "Los dolores de la red de redes", presentada por el autor en el II Encuentro Nacional de Investigadores de la Comunicación, Santiago de Chile, noviembre de 1999.

Bibliografía

- BIEBER, M., & col.: "Fourth generation hypermedia: some missing links for the World Wide Web", International Journal of Human-Computer Studies, v. 47, 1997, pp. 31-65.- CIA: Declaración del director de la CIA ante el Congreso: http://www.cia.gov/cia/public_affairs/speeches/dci_testimony_062498.html

- COLLE, R.: "Conceptos básicos de computación", Pontificia Universidad Católica de Chile http://www.puc.cl/curso_dist/cbc/

- CONSEIL D'ETAT: Rapport du Conseil d'Etat http://www.internet.gouv.fr/francais/textesref/rapce98/accueil.htm

- GAINES, B.R., SHAW, M.L.G.: "Knowledge acquisition, modelling and inference through the World Wide Web", International Journal of Human-Computer Studies, 1997, nº 46, pp.729-759.

- GARFINKEL, S. L.: The Manchurian Printer, (C) 1995, (Reseña en The Boston Sunday Globe, March 5, 1995, Focus Section, P. 83)

- HAENI R.: An introduction to Information Warfare (http://www.seas.gwu.edu/student/reto/infowar/info-war.html)

- HEARST, M: "Interfaces for Searching the Web", Scientific American, March 1997 (http://www.sciam.com/0397issue/0397hearst.html)

- HELINSKI, P.: "Web-site usability engineering", Web Techniques, 1997, vol. 2 nº 4, pp. 39-43.

- HIN, D.: "Intelligent Agents as a Basis for Natural Language Interfaces", Berkeley (CS), U, of California, 1993.

- INTERNET 2: http://www.internet2.edu/

- Koda, T.: "Agents with Faces: A Study on the Effects of Personification of Software Agents.", Tesis, Boston, Instituto Tecnológico de Massachusetts, (Media Lab.), 1997, (Http://www.media.mit.edu/~agents/~tokomo/)

- LE MONDE: Cybercrime, http://www.lemonde.fr/actu/nvtechno/cybercrime/

- MAES, P.: "Intelligent Software", Scientific American, 1995, Vol. 273, Nº 3, September, pp. 84-86.

- Mathe, N. & Chen, J.: "A User-Centered Approach to Adaptive Hypertext Based on an Information Relevance Model", Paper, 4th International Conference on User Modeling (UM94), Hyannis, Cape Cod, Mass., Agosto 1994.

- MAURER, H.: "Hyperwave: The next generation web solution", Harlow, Addison-Wesley, 1996.

- MOSSBERG, W.: "Microsoft: ni ángel ni demonio", Wall Street Journal Americas, 18.11.1999.

- NN: Internet 2, Revista Novática, nº 127 y 128. (http://www.ati.es/PUBLICACIONES/novatica/1997/127/intdos.html

- OFFICE OF INTERNATIONAL CRIMINAL JUSTICE: http://www.acsp.uic.edu

- I. PEDRA: "Internet vs Microsoft", http://wwwest.uniandes.edu.co/~di-pedra/antims/netvsms.html

- Rusilovsky, P. & Beaumont, I.: "Adaptive Hypertext and Hypermedia", Paper, 4th International Conference on User Modeling (UM94), Hyannis, Cape Cod (Mass.), agosto, 1994.

- SCHWARTAU, W.: Information Warfare.

- SLOT, M.: "Web Matrix" (http://www.ambrosiasw.com/~fprefect/matrix/

FORMA DE CITAR ESTE TRABAJO EN BIBLIOGRAFÍAS:
Colle, Raymond (2000): Internet: un cuerpo enfermo y un campo de batalla. Revista Latina de Comunicación Social, 30. Recuperado el x de xxxx de 200x de:
http://www.ull.es/publicaciones/latina/aa2000qjn/91colle.htm