LORENZO VILCHES*

La construcción social del virus informático

INTRODUCCIÓN

En el mundo de la microbiología y en el de la microinformática existen unas criaturas llamadas virus que dan lugar a un tipo de vida real o artificial cuyo sistema de existencia escapa al control humano y al control de la información respectivamente. Ambos suponen un gran riesgo para los sistemas de vida.

Pero aunque la naturaleza del virus consiste en un efecto de reproducción programada e incontrolada de un tipo de información, no siempre se trata de efectos malignos o mortales. Por ejemplo, gracias a un virus llamado *JC*, los científicos han podido determinar quiénes eran, muchos siglos antes de la llegada de Colón, los pobladores de América. Este virus, alojado en el riñón del ser humano, no es necesariamente patógeno y ha sido de mucha utilidad a la paleontología. Aunque en ocasiones, este virus puede sufrir una fatal mutación entre los enfermos de Sida originando una especie de arteriosclerósis múltiple que puede acabar con la persona infectada en seis meses.

En el ámbito de la ecología de sistemas de vida artificial (llamado también ciberespacio técnico científico), los trabajos de Minsky y Rucker han significado un cambio de paradigma científico al eliminar los límites entre

* Doctor en Ciencias de la Comunicación por la Universidad Autónoma de Barcelona. Director del master en Escritura para Cine y Televisión de la misma universidad. E.Mail: imtv25@blues.uab.es

la vida real y la vida artificial. En ese área de estudio se colocan las tentativas químicas de sintetizar las moléculas autorreplicantes, los análisis lingüísticos de los sistemas de auto-conservación, la robótica y el diseño de computadores capaces de evolucionar hacia nuevas formas.

La premisa de la vida artificial consiste en que la base de la vida es la información contenida en un sistema dinámico y complejo capaz de reproducir copias más complejas que las originales[1]. Estas criaturas pueden ser integradas en una forma corporal (los robots) o pueden vivir en un computador. La dependencia de estas criaturas de un *software* las hace extremadamente predispuestas a una avería por fallo de un sistema (a veces basta la equivocación de un sólo número para bloquear toda una red de información). Los peligros de los virus son un retrato de los peligros inherentes a toda forma de vida artificial. Si no se controlan los virus en el ecosistema de la información, se pueden derivar consecuencias fatales para quienes viven del trabajo o de las prestaciones de los sistemas informáticos. A mayor dependencia de los sistemas de *software* mayor es el riesgo para los sistemas humanos —diferentes son las consecuencias de un virus en un programa de tratamiento de texto en un ordenador personal que un virus en un programa, pongamos por caso, de vuelo de un *airbus*—.

"Los virus informáticos no son destructivos en esencia. Su finalidad es controlar al ordenador para poder hacer una copia de sí mismo. Se trata de un aparato reproductor. Una vez ejecutado el programa con el virus, se reproduce en una copia exacta y esta copia, una vez ejecutada reproduce una copia exacta, etc. Se trata de un sistema perfecto de serialidad al infinito".

Un ejemplo de los riesgos a que están sometidos los usuarios de la microinformática son los, precisamente, virus informáticos. Las bases de datos de los servicios secretos de un país, de una red de bancos, de los archivos de un gobierno o de centros de investigación científica, así como los programas de trabajo de las personas en todo el mundo, están sometidos constantemente al peligro de los virus. Por ello, la cultura popular (sometida sobre todo a la información distribuida en forma capilar a través de internet) y los medios de comunicación, lo han tenido fácil a la hora de explotar las fantasías de (auto) destrucción y las predicciones de averías universales o milenarias de los virus informáticos, comparables a la alarma suscitada por el 'efecto 2000'. De ahí que las posibles analogías entre los peligros del virus informático y ese otro gran mal finisecular que representa el virus del SIDA no hagan más que reforzar la experiencia humana paradójica y connatural al género humano frente al mal: el rechazo y el temor frente a una fuerza invisible y destructora que se combina con la gran fascinación por la capacidad de reproducción, sobrevivencia, adaptación y mutabilidad de los virus (biológicos y artificiales).

En las páginas que siguen hemos intentado ilustrar esta historia paralela de los primeros años del virus informático y del virus del SIDA proyectándola sobre esa gran pantalla de construcción social de la realidad que conforman los medios de comunicación.

▸ BIOGRAFÍA DEL VIRUS

Los virus informáticos tienen estructuras y funciones con características que bien pueden llamarse bélicas, biológicas y lúdicas a la vez.

A finales de los años cincuenta, salió de los *Laboratorios Bell* un juego *(Core Wars* o *Guerras del centro)* que consistía en componer programas para un ordenador simulado. El objetivo del juego era sobrevivir, utilizando para ello técnicas de ataque, ocultamiento y reproducción análogas a los virus biológicos.

En 1970, se elaboran en el *Palo Alto Reseach Center* programas basados en técnicas virales de reproducción. Estos virus eran benéficos pues se dedicaban a controlar el estado de salud de las redes y permanecían ocultos durante la actividad diurna de los ordenadores para activarse por la noches cuando la actividad había cesado. Ese mismo año, cuando internet comenzaba su andadura en la red militar y universitaria *Arpanet,* un investigador puso en circulación un programa virus *(Creeper* o *El rastrero)* que desafiaba a que le cazaran. Entonces otro investigador lanzó un virus-antivirus *(Reaper* o *segador)* que se reproducía comiendo *creepers.*

En 1981 se crea el programa para Appel II, *(Cloner)* que se autorreproducía escribiendo un verso en pantalla. Al año siguiente, siempre para la misma marca, se crea un programa parásito indetectable.

[1] LEVY, L. **Artificial life: A report from the Frontier where computer meet biology.** New York: Random House, 1992. s/p.

En 1983, Fred Cohen propuso un programa que podía modificar a otros para añadir una copia evolucionada de sí mismo. A este procedimiento de programas que generan copias de sí mismo se les denominó 'virus' por primera vez.

En 1984, la revista *Scientific American* publica el juego *Core Wars*, dando inicio a la experimentación popular de los virus por parte de los usuarios, aunque ya en 1972 la revista *Software: Practice and Experience* (AT&T) había publicado el juego informático *Darwin*.

En 1986 se conoce el primer virus, proveniente de Pakistán, para *PC y sistema operativo MS-DOS, denominado Brain. Portaba un mensaje y la advertencia de "Cuidado con este virus, comuníquese con nosotros para vacunarse"*, un número de teléfono y dirección. También en 1986 se presenta el *Virdem*, un programa que se copia a sí mismo incluyéndose a otros programas de .COM.

En 1987, proveniente de Alemania Federal, se envió un programa *(Christmas Exec Mail Worm)* que dejaba inutilizado por un corto período de tiempo a una red de ordenadores IBM.

El año 1988 es el año más prolífico en virus. En marzo se conoce el primer virus de *software* comercial, aunque de carácter benigno. El personal de *Aldus Corporation* descubrió miles de copias del programa de dibujo *Freehand* destinado a Macintosh II con un mensaje de paz para sus usuarios. En mayo se da a conocer el *Jerusalem* o *Viernes 13*, un virus que debía activarse en esa fecha aniversario de la fundación de Israel, y cuyo origen muchos atribuyeron a fines terroristas.

Ese mismo año fue sentenciado a siete años de prisión y multa de doce mil dólares Donald Gene Burleson por haber inutilizado datos de ordenadores a través de un virus que funcionaba como una bomba de tiempo.

En noviembre de 1988 más de seis mil ordenadores de Vax y Sun, pertenecientes a militares y a universidades, fueron infectado por un virus que, sin destruir los archivos, colapsaba a los ordenadores con copias de su programa.

En 1989, se conocen dos virus muy populares entre las publicaciones especializadas. Uno, el *Dark Avenger*, un virus mutante, proveniente de Bulgaria y célebre por su potencia devastadora. En ese año, en un paquete de información sobre el SIDA se colocó a *Caballo de Troya*. Una compañía panameña, responsable del virus, exigía el pago a cambio del código de desencriptación. También en 1989 ocurre el primer caso de histeria causada por la labor de desinformación de los medios de comunicación alrededor del virus *Datacrime* que se activó de octubre a diciembre.

El 2 de marzo de 1992 aparece *Michelangelo* el virus más célebre para los medios de comunicación y que terminó siendo un verdadero fiasco, pues su poder de contaminación pasó de las previsiones de cinco millones a unos cuantos miles de ordenadores. Dos años después, en 1994, se conoce el virus *Natas* que contaminó los ordenadores mexicanos.

En 1995 aparecen dos virus que infectan a dos célebres *softwares*. El primero es un virus del lenguaje del procesador de textos Word para PC y Macintosh. El segundo virus es *Bozza* que fue inoculado en el Windows 95.

▸ NATURALEZA DEL VIRUS

▴ *Qué es el virus informático*

No a todos los programas informáticos destructivos se les llama virus y no todos los virus son destructivos.

Existe una base social de hipocondriacos al virus informático, justificada por la complejidad de la tecnología y por las dudas sobre sus reales ventajas. Y además por la relativa escasez, todavía, de los virus en los aparatos domésticos. Los mass media explotan este desconocimiento y crean cada tanto una realidad social —combinando la ignorancia de la propia experiencia con el peligro potencial— de histeria en la opinión publica. Los efectos de tales informaciones se trasladan a los propios errores que vienen atribuidos a los virus, cargando a estos de una culpabilidad que exonera de las propias responsabilidades.

El virus informático tiene a veces toda la apariencia de un ataque bélico por sorpresa. O bien, se

disfraza de programa benéfico *(Caballo de Troya)* que, una vez dentro del ordenador hace explotar una 'bomba lógica' inutilizando el sistema operativo de la máquina.

El atacante creador y distribuidor de un virus raramente sale inmune y está expuesto al riesgo de contaminación dado que el ordenador (sobre todo entre los programas sofisticados) se utiliza como automóvil para transportar el código destructivo del virus.

Los virus informáticos[2] no son destructivos en esencia. Su finalidad es controlar al ordenador para poder hacer una copia de sí mismo. Se trata de un aparato reproductor. Una vez ejecutado el programa con el virus, se reproduce en una copia exacta y esta copia, una vez ejecutada reproduce una copia exacta, etc. Se trata de un sistema perfecto de serialidad al infinito. Así, el virus es un sistema reproductor de sí mismo en forma automática, un ARA (auto-reproductor-automático).

El virus informático se puede comparar con una unidad de vida simple cuyos objetivos principales son sobrevivir y reproducirse. Los organismos simples dependen del entorno inorgánico y no necesitan atacarlo para cumplir estos objetivos. El virus informático usa el disco duro del sistema del ordenador como fuente de energía para sus fines, no ataca a otros sistemas autrorreproductores y funciona como una unidad viviente simple. La cuestión está en que en la época de escasez de ordenadores un virus podía ser fácilmente controlado por el equipo del ordenador central. En una época de masificación de máquinas de ordenadores, por el contrario, los virus pueden escapar de cualquiera de ellos e infestar (e *infectar*) teóricamente a millones de aparatos informáticos dado que todos tienen la misma arquitectura básica y el mismo sistema operativo.

▲ *Clases de virus*

Hay dos tipos de virus conocidos en los sistemas PC. El primero es un virus específico para un archivo específico. Muchos programas de PC DOS y MS2 que no pertenecen al sistema operativo se guardan como archivos. Cada archivo tiene un nombre y una extensión (COM,EXE,SYS para DOS). El virus tiene como objetivo atacar a uno solo de estos archivos y así reproducirse. No puede atacar a un archivo para el cual no ha sido programado.

Hay otro tipo de virus conocido como el virus del sector de arranque *(boot sector virus)* que ataca un espacio determinado del disco duro. Este sector corresponde a la carga de memoria del ordenador y se ejecuta cada vez que se pone en marcha. El virus alojado en este lugar se apropia del ordenador cada vez que se le enciende, adelantándose a la puesta en marcha de un programa y antes de ser detectado.

▲ *La estructura del virus*

En teoría de la comunicación se estudia cada vez más el funcionamiento de los medios a través de las rutinas de producción. Estas determinan el carácter del mensaje y son parte de la estructura cultural y profesional que rigen los centros de producción de programas y contenidos.

Los virus informáticos están compuestos de funciones de estructura que Ludwig llama 'rutinas'. Estas rutinas componen la base de los virus que tienen dos funciones importantes: la función de búsqueda y la función de copia.

La función de *búsqueda* consiste en localizar un archivo o un territorio del ordenador para infectarlo. Según se localice en uno o en otro espacio, el virus será más rápido o más lento, podrá infectar a muchos discos o a uno solo. Mientras más complejo es el mecanismo de búsqueda, más espacio ocupa.

La función de *copia* necesita pasar desapercibida para no ser detectada, y por eso las más pequeñas son más efectivas. Un virus que solo infecta archivos COM puede obtenerse con una copia mas pequeña que las que infectan un archivo EXE, dado que la estructura de este es mucho más compleja. Con el fin de evitar ser capturados, algunos virus están dotados de una función de *antidetección,* que puede formar parte de las funciones de búsqueda o de copia. Con el fin de burlar los sistemas de vigilancia, los virus pueden activarse solo en ciertas fechas o a través de determinadas pausas de tiempo que el usuario realiza delante del teclado. Esta es la estructura básica de un virus. Aunque se les puede dotar de poder destructivo, o proponer juegos al usuario, en ultimo término se está exponiendo a los virus a la rápida detección y conocimiento de todos los usuarios. Si éste se encuentra con una cantidad de archivos repetidos, puede atribuirlo a un error personal o del sistema. Pero si se le destruyen los archivos o termina jugando con su enemigo, sabrá que está frente a un virus.

La simulación del virus es parte esencial de su eficacia ya que asegura la reproducción y sobrevivencia del virus. La ostentación lleva a su captura.

[2] LUDWIG, Mark. *Introduction to The little black book of computer viruses.* En LEESON, L.H. (ed.). **Clicking In.** Seatle: Bay Press, 1996.

▲ *El virus mutante*

A partir de los años noventa la vía utilizada para encontrar virus de ordenador fue detectarlos recurriendo para ello a cadenas de instrucciones. Estas se utilizaban cuando había escasez de virus y porque era un método sencillo. Lo que hacía el antivirus era recoger una muestra de un virus y extraer un pequeño segmento de su código esperando que fuera exclusivo de ese virus. Después escribía un programa que buscaba ese segmento de código en un disco duro. Una vez encontrado, el detector alertaría de la presencia del virus.

El motor de mutación del *Dark Avenger* vino a cambiar todo esto. Cada vez que aparecía ese virus se manifestaba una pequeña diferencia: no había cadenas fijas que buscar. Con la llegada de elementos como el motor de mutación mecánica, se debía buscar una forma más sofisticada de detección para reemplazar la técnica de cadenas de instrucciones. A esto, M. Ludwig[3] le llama 'análisis del código'. En algunos productos, el análisis de código toma la forma de invención (heurística). Estos programas buscan códigos que hagan cosas como las que el virus podría hacer, por ejemplo, un código que se automodifica, o códigos que busquen el archivo EXE, o códigos que modifiquen el motor de arranque. Otros códigos analizadores podrían identificar el motor de mutaciones del *Dark Avenger,* mirando o comparando las instrucciones que utiliza o no utiliza.

El problema es que estos códigos analizadores pueden ser burlados de la misma forma que los detectores y cadenas de instrucciones. Esto es precisamente un corolario al problema de las continuas averías de las máquinas de Turing. No hay un detector perfecto que pueda determinar si el programa contiene o no un virus a través del examen de su código.

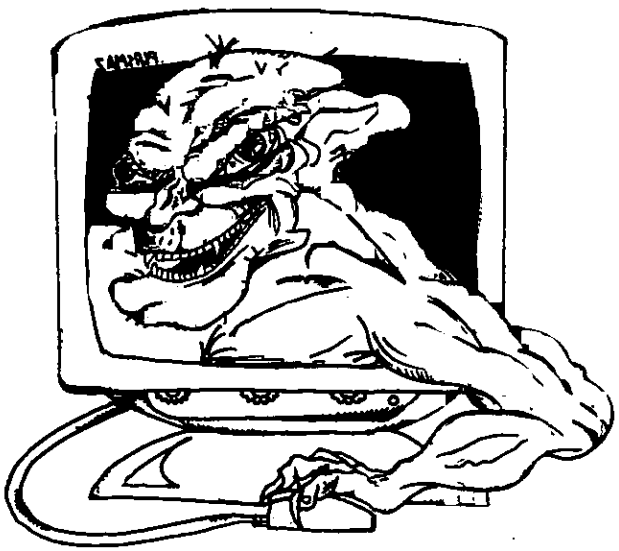
Otro tipo de tecnología llamada chequeo integral es frecuentemente utilizada para encontrar virus. En estos casos se miran los cambios que existen en el *software*. El chequeo integral tiene dos problemas: primero, que como lo que éste hace es detectar cambios, un virus tiene que ejecutarse y reproducirse por lo menos una vez para ser notado. Sólo un detector puede prevenir que un virus se ejecute en el ordenador. Segundo, que a la mayoría de la gente no le gusta usar el método del chequeo integral, especialmente si no tienen una formación técnica, porque no entienden qué significan los cambios en sus archivos. Se puede utilizar la tecnología que desactivaría a los virus antes de que se ejecuten, pero es imperfecta. O bien, puede dejarse que se ejecuten y luego capturarlos.

Los virus mutantes y la teoría de la evolución de Darwin es uno de los posibles campos de examen de las nuevas generaciones de virus. Según Ludwig[4], los algoritmos genéticos se han mostrado muy aptos para solventar ciertos tipos de problemas. Cualquier cosa que pueda replicarse y pasar información genética, con posibles modificaciones a su descendencia, está sujeta a la evolución. Esto incluye a los virus informáticos.

La evolución de los virus, puede, de hecho, ser muy efectiva para evadir escáner y analizadores de código. El problema es que la evolución, así como la entendemos, es algo abierto y cerrado. Un antivirus tiene sus límites gracias a Turing, y un virus puede encontrar esos límites y explotarlos gracias a Darwin.

Para tener éxito en el sentido darwiniano, debe ejecutarse una unidad de código autorreproductor. Si no se ejecuta, no habrá prole. Y morirá. Hay esencialmente dos caminos para que cada código sea ejecutado. Uno es ocultarse y apropiarse de una porción de CPU (Unidad Central de Procesamiento) en forma clandestina. La otra forma consiste en inducir al usuario para que lo ejecute. Estos dos componentes son esenciales para la vida electrónica cambriana. El virus debe entrar en el ordenador y ejecutarse una vez a mansalva. A continuación debe inducir al usuario a que lo deje quedarse.

El secreto y la seducción, dos teorías que en semiótica y en filosofía del lenguaje han servido para explicar la teoría de la acción comunicativa, podrían también mostrarse útiles para afrontar el mito de los virus en la sociedad posmoderna.



[3] LUDWIG, M. **Virtual Catastrophe: Will Self-Reproducing Software Rule the World.** En LEESON, L.H. Op. Cit.

[4] Ibíd.

▸ VACUNAS Y PREVENCIÓN DEL VIRUS

Existen dos tipos de comportamientos opuestos frente al virus informático. Algunos se dejan llevar por el 'pánico al virus', son dependientes de la información de los medios de comunicación y suelen infligirse daño a sí mismos por usar programas no adecuados de prevención o bien por no actuar correctamente debido precisamente al miedo. Sobre este comportamiento se reflexiona en siguiente apartado. Otros usuarios de ordenadores piensan que a ellos nunca le afectarán los virus y que toda la información sobre antivirus o prevención pertenece a la mitología popular alimentada por el *business system* de la era informática.

El tema de los antivirus y la prevención en el mundo de la informática contiene abundantes referencias y analogías con informaciones sanitarias sobre el Sida. Examinamos aquí algunas de las más conocidas.

"Contrariamente a lo que muchos piensan y divulgan, el ciberespacio no está circunscrito ni originado por las tecnologías y la informática, sino que es un nuevo espacio social de comunicación que afecta a la concepción del yo y del otro".

Se calcula que el 50% de los virus pertenecen a aquellos que infectan el sector de arranque de los ordenadores. Esto se puede evitar si el usuario evita poner en marcha su ordenador desde un diskette. El interface del disquete se convierte así en medio potencial de contagio, semejante a las jeringuillas. Se aconseja al usuario de ordenador no dejar el diskette en la unidad del ordenador y retirarlos después de su uso. El disquete puede estar infectado, aún sin tener nada grabado en él, porque contiene un programa elemental que informa si el disquete no pertenece al sistema operativo. En este programa puede hallarse escondido el virus, infectando al disco duro antes de que éste active los programas antivirus.

Para evitar posibles accidentes, se puede desactivar el arranque desde un disquete a través de una operación en el *Bios* o memoria RAM. Otro sistema de seguridad es colocar una barrera de protección *(drive lock)* para impedir la entrada de un diskette que viene a ser análoga a una prótesis-interface anticonceptiva *(Diu* o preservativo).

Pero existen también otras vías de infección. Una de ellas es el modem. Existe un riesgo comprobado de contaminación temporal (mientras se use el programa) si se transfieren programas vía modem. Las infecciones por esta vía sólo pueden ocurrir a través de la transferencia de archivos, nunca por medio del arranque del ordenador. Lo mismo ocurre con internet si se bajan programas desde un *web on line* infectado. Sin embargo, otros afirman que es muy difícil ser infectado por esta vía. De todas formas se recomienda tener vínculos *(links)* y recibir programas desde sitios conocidos y controlados.

En el capítulo de las vacunas, se recomienda siempre someter a control antivirus incluso a los programas antivirus. Se aconseja también el recurso a diferentes sistemas de protección de los programas antivirus, tales como la búsqueda de firmas *(scan)*, chequeo de cambios de códigos de verificación, bloqueo a las operaciones sospechosas y protección del sector de arranque.

▸ EL SÍNDROME DE AUTOSUFICIENCIA ADQUIRIDA

Contrariamente a lo que muchos piensan y divulgan, el ciberespacio no está circunscrito ni originado por las tecnologías y la informática, sino que es un nuevo espacio social de comunicación que afecta a la concepción del yo y del otro. Este nuevo espacio de pensamiento (el contexto de la ubicuidad informática) y de percepción (la realidad virtual tanto lúdica como científica) de la dimensión humana está siendo constantemente afectado también por el discurso de los medios de comunicación tradicionales en una forma que bien podríamos llamar un 'nuevo espacio de construcción social de la realidad' (o 'hiper-realidad').

Existen una serie de coincidencias entre el nacimiento del discurso del virus del SIDA y del virus informático en los medios de comunicación. El virus tiene un protagonismo mayor que la propia enfermedad y ha pasado a tener entidad propia.

Nunca se valorará suficientemente el rol de los medios de comunicación en la propagación de rumores en situaciones emergencia, catástrofes naturales y crisis internacionales. En muchos casos la información periodística se adelanta, incluso, a los acontecimientos, y establece agendas de futuro con previsiones de comportamientos de cosas y personas.

Las agendas periodísticas juegan de tanto en tanto un rol central en la construcción de mitos modernos a través de sistemas culturales que llegan a constituir verdaderas rutinas de producción de opinión pública. En el caso de los virus que afectan a la salud, especialmente el del SIDA, y también en el caso de los virus informáticos, la utilización de las opiniones de los no expertos alcan-

zan un grado de autoridad de enorme fuerza persuasiva entre una población deseosa de creer en la fuerza de espíritus malignos, provengan estos del más allá o de las nuevas tecnologías. Las fuerzas del mal venden bien en la época de las autopistas de la información y de las tecnologías globales.

El recurso a la autoridad de las opiniones impresionistas constituye en muchos casos lo que la *Air Force* de Estados Unidos ha llamado el 'síndrome de la suficiencia'[5], previniendo de que la opinión de los pretendidamente expertos no debe influir en los no expertos y que los no expertos no deben tratar de influir en los demás: "Las personas que sufren el síndrome de la suficiencia ofrecen conclusiones extraídas de unos pocos datos y establecen suposiciones como si fueran hechos"[6]. Esto no sólo sucede en los campos estratégico-militares. Los medios de comunicación son los principales propagadores del síndrome de la suficiencia. La opinión de los expertos en un determinado campo de la vida pública los convierte en expertos en otros medios. Este es un fenómeno que en España tiene sobre todo su caldo de cultivo en las tertulias de la radio. En un país que lee poco, las tertulias radiofónicas mezclan en el turmix de la actualidad a periodistas, políticos, faranduleros y folklóricas que tan pronto opinan sobre las verdaderas causas de las guerras en el mundo mundial, o las contraindicaciones del viagra, como acerca de la corrupción política en Rusia y las bondades de la dieta mediterránea.

Durante la crisis del Golfo, los rumores y las falsedades de uno y otro bando, publicadas en los principales medios del mundo, formaron parte de la diplomacia. El Gobierno de los Estados Unidos utilizó la CNN para enviarle mensajes y ultimátums a Sadam, sustituyendo así las vías diplomáticas por la televisión satélite.

La guerra del Golfo se hizo en gran parte a través de la televisión, y los periodistas actuaron en muchos casos como expertos en diplomacia. El virus informático tuvo también su protagonismo en la batalla de los rumores. En 1992 se publicó en Estados Unidos *News &World Report,* un reportaje sobre el virus de la *guerra del Golfo* en el que se decía que poco antes de la guerra, la *National Security Agency* había interceptado impresoras con destino a Irak a las que la NSA había secretamente inoculado un virus. Inmediatamente la ABC abrió su telediario con aquella historia en la que incluso se mostró un video de explicación sobre el virus. Luego se demostró que se trataba de algo muy parecido a lo que había publicado *InfoWorld5* en abril de 1991.

También en 1992, durante "la crisis del virus *Michelangelo*", la NBC mostró un reportaje sobre el pánico de la gente a través de la declaración de un vendedor de un establecimiento que afirmó que el pánico era justificado. Según esta opinión, recogida como una afirmación irrefutable por la televisión, el pánico se justificaba si los clientes creían que su ordenador tenía un virus. Los periodistas preguntaban a la gente si quería ser entrevistada sobre el virus. Tenían preferencia aquellos que creían que su ordenador estaba infectado.

El pánico al virus *Michelangelo* fue general, por lo menos en Estados Unidos. Los investigadores habían descubierto en 1991, al examinar los discos duros de IBM, un nuevo virus informático que se desencadenaría cada 6 de marzo, aniversario del artista italiano. Al año siguiente, un fabricante anunció que había despachado medio millar de PC infectados, el mismo día en que otro fabricante anunciaba su decisión de incluir programas antivirus en cada ordenador. A partir de aquí, los medios de comunicación se adueñaron del asunto. La *United Press International* entrevistó, por ejemplo, a la Asociación Internacional contra el Terrorismo Informático. Poco después, esta agencia distribuía un despacho anunciando que muchos miles de ordenadores en el mundo serían víctimas de *Michelangelo*. La agencia *Reuter* calculó que unos

[5] ROSENBERGER, R. **Michelangelo Fiasco: A historical timeline.** Associated Press International, 1995.

[6] TONGUE & QUILL. S/d.

cinco millones de ordenadores ya hospedaban al virus. Algunas compañías de informática aprovecharon publicitariamente el momento ofreciendo gratuitamente un programa de detección del virus. Las televisiones seguían entrevistando a los vendedores de ordenadores que repetían lo que leían en la prensa. A la compra de programas antivurus sobrevino la de libros sobre el tema. Los expertos que abrieron la boca para rebajar la histeria colectiva no tuvieron ningún eco entre los periodistas. La histeria fue en aumento hasta el punto que la agencia Reuter vaticinó que uno de cada cuatro ordenadores en Estados Unidos sería infectado. En realidad, *de lo que se hablaba en los medios era del miedo al virus, y nadie prestó atención a la naturaleza del virus.* El ser famoso por un día (Andy Warhol) ha llegado, después de aprovechar la catapulta de los platós televisivos, también al reino de la informática. Muchos recibieron la petición de un niño que se moría de una enfermedad incurable y deseaba tener su nombre en el libro de *Guinnes* por haber recibido la mayor cantidad de *e-mailes* por su pronto restablecimiento. A ningún usuario le interesó demasiado la enfermedad o el enfermo, lo importante era lograr una hazaña ciberespacial.

El 6 de marzo las agencias de noticias tuvieron que conformarse con un número muy por debajo de los cinco millones de infectados previstos, entre diez y veinte mil. De improviso, todas las noticias sobre *Michelangelo* acabaron el día 7. Quienes habían estimado en cinco millones a los infectados, culpabilizaron a los mismos medios de haber rebajado la cifra debido a la histeria. Por su parte, los expertos pensaron que precisamente la campaña de los medios elevó la cifra de los damnificados, muchos de los cuales causaron daños irreparables a sus ordenadores movidos por la histeria del virus. Estos, a su vez, responsabilizaban a *Michelangelo* de sus propios errores, presumiendo de haber sido atacados por el virus. ◂

VIDAS PARALELAS

	VIRUS DEL SIDA	VIRUS INFORMATICO
1981a	Primeros casos de sida en homosexuales. Los Angeles.	Programa CLONER autorreproduc. para Appel II
1981b	Primeros datos sobre el SIDA como infección vía sexual/ sanguínea.	Programa parásito indetectable para Appel II
1983	Primera descripción virus del SIDA (LAV) I. Pasteur	Primera descripción virus informático (VAX 11/750) F. Cohen
1984	Aislamiento del virus del SIDA (HTLV3)	Difusión pública del *Core Wars*
1985	Aparición prueba de detección.	Desarrollo de sistemas de detección
1986a	Descubrimiento del VIH2 I. Pasteur	Primer virus para PC/MS-DOS (Brain) y vacuna. Pakistan.
1986b	Antivírico AZT (azidotimidina)	Virus *Virdem* (se incluye en .COM)
1989		Virus mutante *(Dark Avenger)* Bulgaria. Virus en software SIDA 'Caballo de Troya'. Panamá
1991-1992	Progresos en el conocimiento de la enfermedad. Primeros ensayos humanos de vacunas potenciales	Virus *Michelangelo:* el gran fiasco de los medios de comunicación. Virus *Bozza* para Windows 95

▸ BIBLIOGRAFÍA

LEVY S. Artificial Life: A report from the Frontier where computer meet biology. N. York: Random House, 1992.

LUDWIG. M *Introduction to The Little Black Book of Computer Viruses*. En Hersfman Leeson, L. (ed), **Clicking In.** Seatle: Bay Press, 1996.

LUDWIG, M. *Virtual Catastrophe: Will Self-Reproducing Software Rule the World.* En L.H. Leeson (ed). **Op.Cit.**

MINSKY N. **The Society of Mind.** N.York: Simon and Shuster, 1986.

ROSENBERGER, R. **Michelangelo Fiasco: a historical timeline.** Associated Press International, 1995.

RUCKER R. *Artificial Life.* En RUCKER R; Sirius R.U.; NV.Q.(editores). **Mondo 2000, A User's Guide to the New Edge.** N.York: HarperCollins, 1992.

UGALDE CORRAL H. *Historia de los virus.* En **Personal Computer.** México, Marzo 1996.