

# **El Hacker**

**Por:**

**Lilliana Castaño Garcés  
Fernando Castro T**

**Investigación Genealógica**

**Universidad de Antioquia  
Medellín  
2007**

## Introducción

Realmente es difícil decir cómo aparece en la historia el concepto de Hacker, miles de personas han intentado remontarlo a tiempos muy lejanos, algunos Filósofos que he leído, han tenido la descabellada idea de decir que Platón era un Hacker, posiblemente Platón era un revolucionario del pensamiento y posiblemente uno de los filósofos más grandes de toda la historia; pero este texto no intenta ser un texto filosófico aunque puede terminar siéndolo debido a la formación filosófica a la que estamos intentando acceder en este momento, yo delimitaré la existencia de este pensamiento al surgimiento de las tecnologías de información, la computación o la informática (Como prefieras llamarlo), todos estos hechos son anteriores a lo que hoy conocemos como la sociedad de la información ya que ésta surge como una consecuencia de la investigación en los campos antes mencionados.

Debo decir que la computación como la conocemos ahora, tiene sus orígenes en la guerra, durante la segunda guerra mundial se desarrollaron máquinas que hacían cálculos para descifrar las comunicaciones de los enemigos y de esta manera tener ventaja en el campo de batalla, los aliados, en especial Estados Unidos, lograron desarrollar la computación electrónica.

Así pues, el objetivo de este texto es realizar un estudio genealógico, en relación con la propuesta de Michel Foucault<sup>1</sup>. En este sentido, nos preguntaremos cómo surge el pensamiento Hacker -desde los 60 hasta los días de hoy-, qué relaciones de poder están en juego y trataremos de escudriñar en la historia cómo estas relaciones se construyen.

Se preguntaran porqué hablar de pensamiento Hacker en relación con

---

<sup>1</sup> A la genealogía no le interesa el origen de las cosas, le interesa la procedencia y eso quiere decir que no va en busca de un principio metafísico, sino que escudriña en el proceder de las cosas y busca en ellas los motivos ocultos, las razones de fuerza o las necesidades de dominio por las que ha surgido un momento histórico, una ciencia, un saber o una entidad o un estado. La genealogía ha de preocuparse por la procedencia, detrás de las estrategias de poder, estrategias que parecen ocultarnos en una historia optimista que rescata de manera positiva el desarrollo del devenir del hombre, la genealogía parece ser un devenir de momentos sin fecha, que nos relatan cómo el poder está detrás de cada uno de los momentos históricos, la genealogía nos muestra las luchas internas y externas y no espera por un fin lleno de paz y armonía, ya que las luchas son el fundamento, según Foucault, de la existencia de los saberes y las instituciones, nuestro pensamiento está en constante lucha con sus propias ideas y las de los demás; de esta manera, la genealogía "...busca la emergencia de las identidades y de las esencias, investiga cómo éstas aparecen a partir del juego azaroso de las dominaciones..."

ciertas estrategias de poder que se hacen visibles en la historia, muchos dirán que el movimiento Hacker y su pensamiento, obedece a una comunidad imparcial donde lo que menos interesa es acceder al poder o ejercer algún tipo de poder sobre las personas; la idea optimista de liberar la información y de hacer accesible el conocimiento a todas las personas, puede ser la muestra de una relación de poder o una estrategia de dominación que está en juego en las relaciones del hombre y la máquina, y más allá de eso las relaciones que se establecen a través de la tecnología y la vasta red donde tiene cabida la concepción de la palabra Hacker.

## El Hacker

*" Y Entonces ocurre... Se abre una puerta a un nuevo mundo... Corriendo a través de la línea telefónica, como la heroína a través de las venas de un adicto, se emana un pulso electrónico, buscaba un refugio ante las incompetencias de todos los días... Me encuentro con un teclado. "Esto es ... Aquí pertenezco..." Conozco a todo el mundo aquí... aunque nunca me haya encontrado con ellos, les dirigiese la palabra o escuchase su voz... Les conozco a todos... Maldito crío. Ya está enganchado otra vez al teléfono. Son todos iguales... " <sup>2</sup>*

¿Porqué conectarse? Es una necesidad inherente al ser humano encontrar conexiones donde podamos desplegar toda nuestra capacidad creativa y de alguna manera competir con las otras personas, parece que es evidente sostener una actitud crítica ante las cosas que se nos presentan a diario; es por eso que nos conectamos, la conformidad no es parte de nuestro universo ya que estamos en constante lucha con nosotros mismos, tenemos que luchar con las voces que intentan acallar nuestras voces de protesta, luchar contra un conocimiento mediocre y condenado por un régimen que intenta someternos por medio de "Bienes Sociales", intentamos aprender cosas que no quieren que sepamos, cosas que tienen miedo que veamos y usemos, les da miedo que revelemos sus secretos técnicos y salgamos de la mediocridad en la que nos mantienen en su ejercicio del poder. Los mecanismos de control creen que el conocimiento es poder, nosotros mismos lo hemos creído y se lo hemos demostrado al mundo, nuestra actitud nos lleva por el camino de la esperanza de creer en un mundo mejor, tenemos una actitud positiva frente a lo que hacemos y demostramos al mundo, pretendemos liberar el conocimiento, pero las consecuencias son nefastas; porque a pesar de nuestros intentos de ayudar y posibilitar un cambio, la sociedad nos ha marcado como delincuentes, nos han llamado terroristas, ¿porqué? Porque tienen miedo de nuestro poder, poder que ahora no podemos negar.

Este texto intenta mostrar cómo un Hacker se relaciona con el poder, cómo se forma y cómo aparece el concepto de Hacker en los diferentes mecanismos del poder y cómo se transforman las relaciones de poder que de alguna manera han formado el actual conocimiento hacker; porque no hay que negarlo, ser un hacker o pretender serlo, se da en el juego de diferentes relaciones de poder, se da en la confrontación con los otros, con las luchas internas que se evidencian a la hora de querer adquirir un conocimiento.

---

<sup>2</sup> Tomado del Manifiesto Hacker, <http://www.informatica-pc.net/hackers/hackers.html>

*"Hacker es el neologismo utilizado para referirse a un experto en varias o alguna rama técnica relacionada con la informática: programación, redes de computadoras, sistemas operativos, hardware de red/voz, etc. Se suele llamar hackeo y hackear a las obras propias de un hacker."*<sup>3</sup>, muchos están de acuerdo con esta definición de Hacker y la defienden a capa y espada con miedo a las consecuencias legales que puede traer asumir ciertas posiciones adoptadas al respecto; puede que un hacker no pueda denominarse pirata informático, pero es claro que una persona con las suficientes capacidades técnicas puede ser considerado, en el contexto social como un individuo peligroso, es por ello que el concepto de hacker a través de la historia ha estado marcado por momentos donde no logra distinguirse la diferencia que hacen los mismos hackers entre Crackers<sup>4</sup> y/o Pirata informático.

El Hacker es una persona con interés por conocer todo aquello que atañe a un tema específico; en nuestro caso, estos temas están relacionados con la informática, las telecomunicaciones, las redes de datos en general; se puede decir, interesados en conocer el funcionamiento de todo lo relacionado con la red; así, adquieren conocimientos de electrónica, de programación etc, inicialmente con el interés de mejorar su conocimiento en este tipo de temas, pero entonces nos preguntamos ¿para qué obtener ese conocimiento? ¿sólo por tener la sensación de saber algo que las otras personas no saben y que algunas corporaciones intentan ocultar? En teoría la ética Hacker nos dice que el conocimiento obtenido se utiliza, ya sea para poder mejorar de alguna manera el sistema que intenta comprenderse, o para divulgar información que desde el punto de vista del Hacker debería ser libre.

*"El conocimiento debe ser libre"*, es la gran premisa que justifica la mayoría de las acciones de los Hacker, ¿pero debe ser realmente el conocimiento libre o más bien, puede ser el conocimiento libre? La pregunta por el asunto de si una cosa puede ser o no libre, es uno de los problemas que "El Hacker" ha planteado a la creciente sociedad de la información.

Al principio la red era simple y anárquica, en el principio sólo los entusiastas de la red navegaban por ella y corrían sus programas sin mayores complicaciones; para conectarte era necesario tener tu propio ordenador y tú mismo te tenías que encargar de crear las conexiones físicas para llegar a la red, en ocasiones bastaba con tener un módem

---

<sup>3</sup> Tomado de :<http://es.wikipedia.org/wiki/Hacker>

<sup>4</sup> Según la Wikipedia: Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño.

conectado a una línea telefónica, hacer que el ordenador marcara un número para conectarte a una red, llena de expectativas por lo que podías crear para ella y con la información contenida en ella, en ese tiempo la información sólo era información y aún no se perfilaba ningún tipo de poder que tratara de asumir el control, o ejercer el poder sobre la forma de uso de la red, porque en este tiempo la red consistía en un ámbito de investigación, era la época de ARPANET, (1969 – 1974).

Pero rápidamente, esta red se convirtió en algo llamativo para los empresarios, las corporaciones, los gobiernos, entre otras entidades. Estos organismos encontraron en la red la posibilidad de comunicarse rápidamente, realizar transacciones, negocios y todo lo que conocemos hoy como sociedad de la información, en ese momento el Hacker -aquel que había ayudado a crear la red- es visto como un personaje peligroso porque tenía el conocimiento para controlar la red; los Hacker tenían el poder de acceder a cada uno de los ordenadores de las organizaciones que ingresaban a formar parte de la red.

De mano de las instituciones nacieron los prejuicios en contra de los hacker y estos, en su defensa, crearon todo un argot para defenderse de las denominaciones negativas que empezaban a aparecer y crear temor en los organismos del estado, entidades bancarias y público en general. Esta es la época donde las instituciones empezaron a ejercer su poder para tratar de controlar la red. Así pues, el término de delincuente fue aplicado ahora a los hacker, dado que ellos constituían un amenaza para los emporios del poder social y económico, sólo en este momento, cuando ya los hacker habían ayudado al desarrollo de la computación y el Internet y de éste se querían apoderar las multinacionales, se difunde la idea de que los hacker son un peligro público y comienza la persecución contra los hackers (1975 – Hasta la actualidad).

En este momento comienza la lucha por liberar la información, las corporaciones se esmeran en cifrar cada nuevo descubrimiento o aplicación lanzada en el mundo de la informática y/o en la red, los Hacker, en su afán de saber qué hay detrás de estos nuevos “servicios” rompen los nuevos códigos, entran en los nuevos sistemas y se crea una verdadera guerra entre el conocimiento profundo del sistema y las instituciones con miedo de liberar la información que es considerada como confidencial. La lucha por el conocimiento libre toma nuevas formas y se diversifica, por una lado aparecen nuevas formas de denominar a las personas que accedían a los sistemas, Los Hacker se autodenominan amantes del conocimiento e individuos poco peligrosos a quienes no les interesa causar daños a los sistemas, por ello crean el término “CRACKER”, este es un individuo que para los mismos Hacker es

peligroso, es aquel que rompe un sistema, se apropia de datos, roba una tecnología para obtener algún beneficio por lo general económico.

Pero los medios no han soportado tanta terminología y han preferido ignorar el clamor del Hacker; y al igual que los Crakers han sido tratados como delincuentes, esto pasa porque quien tiene el conocimiento es considerado como un individuo peligroso para la sociedad de la información, debe mantenerse al margen y se trata todo el tiempo de limitar sus acciones.

En la lucha por el conocimiento, se ejercen diferentes relaciones de poder tanto de quienes intentan acceder al conocimiento como los Hacker, como de quienes intentan detenerlos; quienes intentan detenerlos han logrado echar mano de las organizaciones gubernamentales que crean normas con el fin de aterrorizar el accionar del Hacker y limitarlos, crear miedo mediante las leyes, que muchas veces los castigos en contra de una acción de un denominado Hacker son mas fuertes que asesinar a una persona, el castigo por bajar una canción de la red, es mas fuerte que para quien roba en la calle, de esta manera se muestra también el miedo que tienen las organizaciones a quienes quieren poseer el conocimiento de cómo funcionan las cosas, y también de aquellos quienes lo poseen.

Los gobiernos presionados por otras organizaciones, crean nuevas leyes en pro de preservar la creciente "sociedad de la información" en pro de preservar su orden y mantener los datos seguros en la red, las leyes, en teoría, se crean para proteger la sociedad, pero ¿de que nos protege una ley anti-Hackers? se nos dice que se nos protege de las posibles pérdidas de información que pueden causar los Hackers, de los ataques a los bancos, a las corporaciones, se protegen los datos, ¿pero qué es un dato en sentido informático? un dato es ceros y unos, almacenados en un disco duro, un disco duro es un sistema de almacenamiento electromagnético creado para guardar datos, un dato puede ser la información de una persona, las paginas web que vemos en la red, nuestra información bancaria; los Hacker, en teoría, no muestran interés por estos datos, quizá lo haría un Craker, pero estas leyes no se crean para proteger al ciudadano, estas leyes están amparadas por las grandor corporaciones que manejan nuestros datos y no quieren mostrar cómo realmente están siendo usados los datos de los ciudadanos que pretenden proteger con las leyes anti-Hackers, muchos de los ataques de los Hacker a estas corporaciones han mostrados sistemas que las corporaciones han creado para vigilar a los ciudadanos que protegen las supuestas leyes, los gobiernos han creado sistemas electrónicos utilizando las mejores herramientas de los Hacker, para crear sistemas

que leen los correos electrónicos, escuchan las llamadas telefónicas, para intervenir en general la comunicaciones, así que nos preguntamos El Hacker en ocasiones, intenta revelar los asaltos de los mismos organismos que pretenden defendernos, y los organismos invaden nuestra privacidad con la excusa de defendernos, ¿de quien? De nosotros mismos al parecer, porque el enemigo público somos nosotros mismos; esto último nos recuerda a Foucault cuando reflexiona sobre el momento de surgimiento de la idea del sujeto como el mayor peligro para la sociedad.

Los medios de comunicación se encargan de desinformar sobre la funcionalidad de los Hackers en la sociedad de la información, estos medios “tradicionales” como la radio y la televisión refuerzan la visión que los organismos de poder intentan vendernos sobre el nuevo individuo peligroso que se ha creado en esta sociedad, un individuo que puede hacernos demasiado daño. Los medios de comunicación y la historia tradicional poco ayuda a que las personas se enteren de los diferentes contrastes de la sociedad de la información, de las amenazas que los organismos del estado crean al vigilar las comunicaciones de una sociedad particular, de la posibilidad que tiene el estado de vigilar nuestras líneas telefónicas y el control que ejerce sobre medios como la televisión y la radio, pero ellos no son el individuo peligroso, son aquellos que intentan revelar sus secretos ejerciendo el poder que les da conocer en profundidad los misterios de la vasta red.

He aquí un ejemplo de ello:

*Hace 40 años Nueva Zelanda creo un servicio de inteligencia llamado GCSB “Government Communications Security Bureau “ el equivalente a la NSA americana. Ahora y en colaboración con la NSA, crean Echelon. Un avanzado sistema de espionaje a escala mundial, que junto con UKUSA y el empleo de Satélites Intelsat, las nuevas inteligencias gubernamentales pueden desde hace tiempo acceder e interceptar todas las comunicaciones tradicionales como el teléfono, el fax o el correo electrónico.*

*Esto queda patente desde que en 1996 Nicky Hagar´s nos muestra otro tipo de espionaje secreto, descubierto en su libro Secret Power, Nicky revela que estamos siendo espiados en todo momento. Según su libro, Nicky afirma que lo que estamos escribiendo ahora es susceptible de ser espiado incluso en el borrador desde nuestro PC, mediante el método TEMPEST. Este sistema de espionaje aprovecha la radiación electromagnética de la pantalla del monitor para recibir todo lo que se muestra en tal monitor. Por otro lado, cuando se termine este artículo y se envíe por el correo electrónico a la sección de Maquetación, éste será inmediatamente interceptado por la estructura Echelon y por supuesto analizado palabra a palabra.*

*Por otro lado, si enviamos un fax a un colaborador o se realiza una llamada telefónica a dicho colaborador para confirmar que se ha recibido el artículo, Echelon también dispondrá de una copia del fax y de la conversación telefónica. Pensar en todo esto,*

*simplemente le pone a uno los pelos de punta.*

*En 1948 se formaliza UKUSA después de interceptar varias comunicaciones de radio secretas durante la segunda guerra mundial. Junto con Echelon, UKUSA "denominada Spy Network" potencia las posibilidades de controlar las comunicaciones globales desde los satélites Intelsat. El jueves, 12 de junio de 1984, Rob Muldoon conviene en el parlamento lo que sería el primer paso para crear Echelon. Diez años más tarde, el 15 de enero de 1994 los técnicos de satélites interceptan comunicaciones extrañas en los satélites, fecha en la que se revela la existencia de UKUSA.*

*Desde entonces todas las comunicaciones son interceptadas por Echelon y Ukusa y descifradas por técnicos expertos en busca de información confidencial de un posible movimiento militar, terrorista o de otra índole. Todo esto bien podría parecer una película de Ciencia-Ficción pero lo cierto es que no es así. Europa ya dispone de Enfopol, la respuesta a Echelon y Rusia anuncia su propio sistema de espionaje a gran escala.*

*Parece que la guerra fría deja paso a la guerra tecnológica en un tiempo en el que predomina el poder de la información y la obsesiva idea de que nuestro vecino está urdando un plan de invasión inminente. Desde el 3 de julio del 2001 la Red Echelon existe de forma oficial, fecha en la que la comisión de Investigación del parlamento Europeo aprobó por 27 votos a favor. Ya no hay duda alguna de su existencia. Las fuertes sospechas de que consorcios europeos habían sido espiados por Echelon se consolida cuando se descubre cómo Airbus perdió en 1994 un contrato de 6.000 millones de dólares en Arabia Saudita a favor de la McDonnell Douglas, o el contrato de 1.600 millones de dólares para la vigilancia del Amazonas que Thompson-Alcatel perdió en beneficio de la norteamericana Raytheon Corp.*

*Evidentemente esta situación va mas allá de los límites del Hacking, la seguridad o la ética, ya que sólo se limitan a comentar los hechos, pero no a zanjar tal amenaza. Sin embargo, Echelon, Enfopol u otras organizaciones tecnológicas no son las únicas amenazas a tener en cuenta o que existen, sin ir más lejos, Bill Clinton se empeñó hasta hace bien poco, en incluir el Clipper chip en los aparatos de teléfono, a fin de poder intervenir la comunicación deseada. El Clipper chip es un codificador seguro contra Hackers, pero que dispone de una puerta de atrás para todos los efectos de los gobiernos, es decir, la CIA o simplemente la policía federal, puede descifrar la comunicación con una segunda clave.<sup>5</sup>*

*Desde el uso de palomas mensajeras y en la segunda mundial ya se intentaban descifrar mensajes "Hacker es aquel que trata de averiguar cosas y esto se puede aplicar en las comunicaciones que existieron mucho antes que los ordenadores. De modo que se desmiente que los HACKERS tengan una edad temprana. Ya en la segunda guerra mundial se trataba de descifrar los mensajes del enemigo".<sup>6</sup>*

*Sin embargo, la adopción del término Hacker para designar unas prácticas sociales y una comunidad, surgió en momento en el cual los*

---

<sup>5</sup> Hernandez Claudio, Hackers los piratas del chip y de Internet 2001, Pág. 82

<sup>6</sup> hacker 2001

ordenadores no se habían desarrollado lo suficiente, y no existían las computadoras personales, sino lo que se conoce como Mainframe; a las cuales tenían acceso unos pocos operadores, y los demás programadores, que trabajaban sobre las tarjetas perforadas, estaban supeditados en espacio, tiempo, conocimiento y poder, a las grandes organizaciones que poseían los ordenadores y a los operadores.

*“Los verdaderos Hackers aprenden y trabajan solos y nunca se forman a partir de las ideas de otros, aunque es cierto que las comparten si estas son interesantes.”*

Un aspecto que consideramos de importancia, son los múltiples rasgos o caracterizaciones que han surgido desde y para los cibernautas, múltiples rasgos que muestran lo heterogénea que es la cibercultura; pequeños rasgos que singularizan y de alguna forma complejizan este mundo y muestran las discontinuidades y dificultades a las cuales se enfrenta la historia efectiva con respecto a las mediocres visiones tradicionales, totalizantes del pensamiento dominante al respecto. veamos:

*“Un Hacker busca, primero el entendimiento del sistema tanto de Hardware como de Software y sobre todo descubrir el modo de codificación de las órdenes. En segundo lugar, busca el poder modificar esta información para usos propios y de investigación del funcionamiento total del sistema”.<sup>7</sup>*

EL Hacker, es el primer eslabón de una sociedad " delictiva " según la prensa. Estos personajes son expertos en sistemas avanzados, en la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejas como la comunicación móvil. Su objetivo principal es comprender los sistemas y su funcionamiento. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de "he estado aquí" pero no modifican ni se llevan nada del ordenador atacado. Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

Este grupo es él mas experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

---

7 ((2001 ))

Crackers : Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas. Para los grandes fabricantes de sistemas y la prensa, este grupo es el mas rebelde de *todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, si no en que esta rotura es difundida normalmente através de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.*

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser difundidos de forma impune por otro grupo que será detallado mas adelante. Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Lammer: por lo general son personas que gastan altas cantidades de tiempo buscando en Internet herramientas que les permitan ingresar a otros sistemas o crakear un software o hardware, estos personajes no toman muy en serio la idea de ser hacker y se la pasan usando las aplicaciones intentando hacer el mayor daño posible, por lo general sus conocimientos son muy bajos a comparación de los conocimientos de una hacker o un craker.

Newbi: el verdadero aprendiz de Hacker, que lee todos los manuales y sigue todos los pasos requeridos para adquirir los conocimientos de un hacker, no ejecuta un programa malicioso sin necesidad, ya que primero intenta comprenderle en su estructura, se les encuentra en los foros de internet preguntando sobre el funcionamiento de las cosas, leen todos manual que cae en sus manos permitiéndoles adquirir altos conocimientos.

Phreaker: estas personas tienen conocimientos avanzados en los sistema de telefonía, se les considera los primeros Hacker, ya que los sistemas telefónicos existieron primero que los computadores, el interés de estas personas era realizar llamadas sin pagar los costos de la compañía telefónica.

Bucanero: es una persona que no tiene ningún tipo de conocimiento en las áreas antes mencionadas, se encargan de comercializar los

“productos” de los Crakers y buscar en la red herramientas que pueda comercializar en el mercado negro, o en todo tipo de mercados, los Crakers los buscan sólo con el fin de comercializar sus producciones.

Copy-Hacker: al igual que los bucaneros explotan los conocimientos de los Hackers y de los Craker, posee conocimientos medios y copia todas las herramientas ya sea para atacar un sistema y obtener un beneficio o comercializarlos a través de los bucaneros.

A la genealogía le interesa el discurso anónimo y cotidiano; el discurso que ha sido rechazado por no alcanzar, en el caso del movimiento Hacker, el rango de institucionalización. En este sentido, queremos presentar algunos testimonios que han sido ocultados, menospreciados, desvirtualizados y acallados por la institucionalidad en todas sus formas; tanto judicial, gubernamental como ideológicamente.

Es este caso, un caso muy cercano no sólo en tiempo sino también en espacio; el día 2 de diciembre de 2007 en el periódico el Colombiano salió un artículo con el tema de cultura Hacker, en el cual se entrevistan a varias personas de dicha cultura y se muestra el perfil del hacker, constatando los prejuicios que se han formado en la historia. Uno de los testimonios, de los cuales encontramos la versión completa, fué totalmente cortado, descontextualizado y acallado en su idea original y completa. veamos:

### **Jóvenes y ciberpiratas: una frágil frontera**

#### **Artículo publicado por el Colombiano, el 2 de Noviembre de 2007.**

*Juan Jaramillo es cauto y reservado, prefiere aparecer con su nombre real porque su identidad cibernética (Nick) podría traerle problemas: "he tenido varios apodos debido al peso de mis acciones", indica a través del chat.*

*Juan tiene 32 años, estudió ingeniería de Sistemas y su actividad en Internet empezó a los 18 años cuando la web era una telaraña de redes simple.*

*Juan vive en el distrito financiero de Medellín, una zona que aún concentra buena parte de las sedes de los principales bancos y de empresas del grupo empresarial antioqueño.*

*Desde el computador de su casa empezó a escalar las redes empresariales, sin pedir permiso. "Aprender, devorar cuanto cosa hubiera de redes", era la motivación de aquella época en la que pertenecía a un grupo de hackers duros llamados La Cúpula, una comunidad que se insertó en la cultura local de los años 90.*

*Jamás utilizó la red telefónica de su casa y acudía a las cabinas de telefonía pública para "chuzar" la línea de algún vecino y desde allí violar los pbx o conmutadores, así como los sistemas y las plataformas tecnológicas.*

*Sabía, por ejemplo, cuándo y cómo Conavi enviaba sus reportes a la Superbancaria, entre otros detalles. "Yo jamás robé plata pero daños sí admito que los hice", afirma.*

### **Por el ciber mundo**

*Flacman es su identidad cibernética. Hace parte de la comunidad Colombia*

*Underground y asegura que no es un pirata. No le gustan las clasificaciones pero advierte: "no quiero que me pregunten mis datos personales". Solo acepta que se le indague por su edad: 20 años.*

*Participa de los foros a los que entran jóvenes en busca de información.*

*En una sesión, un grupo de piratas de otros países, que invaden sitios del mundo, algunas veces al azar, para redireccionarlos a las páginas pornográficas, promovía su actividad en medio de una avalancha de correos de los participantes al foro, en los que se decía que eso no era propio de un hacker.*

### **-¿por qué crees que lo hacen?, pregunto.**

*"Están aburridos", dice. "Son Lammers. Los más odiados. Muchos de ellos se meten a los foros para saber como robarle la contraseña de correo electrónico a la novia (...) encuentran exploits (vulnerabilidades) o algo que hackear y lo hacen, pero no tienen pasión por saber cómo funciona el mundo", añade.*

### **Todo está en la red**

*En internet un mail irrumpe. Asunto: "claves". Al abrirse se describe cómo recuperar la contraseña de un correo electrónico. En la red de redes circulan con libertad, desde seriales de los últimos programas informáticos hasta instrucciones para violar un sitio web o descargar un keylogger, un programa que permite robar las contraseñas que se digitan en un teclado.*

*Sólo hay que oprimir la clave correcta o dar con el sitio indicado para resolver cómo lograr una acción. En los foros de páginas especializadas, los nuevos integrantes presentan sus credenciales: "soy Martín, tengo 21 años y estoy interesado en información sobre seguridad informática desde hace un buen tiempo. Tuve una fase de chico malo en mi adolescencia pero salí de ello. Quiero aventurarme en PHP/Pearl (lenguajes de programación)".*

*Si se da clic en el vínculo del Nick, aparece un mensaje que nombra las políticas de privacidad. En el ciber mundo, el Nick es una especie de pasaporte y una manera de conservar el anonimato.*

*"Incluso muchos solo me conocen por mi Nick y somos grandes amigos, pero no saben mi nombre real. Eso me encanta de la cibercultura", dice Lesath, un joven de 31 años, quien se nombra con una de las identidades cibernéticas que maneja. En la actualidad trabaja en proyectos de investigación sobre seguridad informática.*

### **El cibercrimen**

*Para algunos jóvenes, explica Daniel Rojas, gerente de Canal Retail para la Región Andina de la firma de seguridad Symantec, el hecho de convertirse en hackers se torna en una manera simbólica de ganarse un espacio en el mundo tecnológico, a través de conseguir unas habilidades específicas.*

*Agrega que, en la mayoría de los casos, ellos no dimensionan las consecuencias de las actividades en las que incursionan. "Sin duda, la posibilidad de dominar la información permite ciertas ventajas sociales y económicas que pueden ser atractivas, lo que puede disipar cualquier consideración ética", remata Rojas.*

*A finales de 2006 se dio en el país la primera condena por piratería en internet que ponía de manifiesto una red de piratas a gran escala, de acuerdo con el mayor Fredy Bautista, director de Delitos Informáticos de la Policía Nacional.*

"Los encontramos buscando en la red", relató el mayor Bautista, en una entrevista telefónica. Él los llama Uploaders porque publican unos sitios donde ponen a disposición listados de software. "Hemos encontrado más de 3 mil títulos o programas a adquirir".

Pero el nivel de sofisticación de estos piratas es elevado. Es un mecanismo que se activa a través de un sitio en el que se pueden hacer compras completas, pues existe un enlace a entidades bancarias y un vínculo para la compañía de mensajería.

"Jamás tienen un contacto físico o verbal; es una transacción anónima en Internet por lo que es muy difícil rastrear".

Sin embargo, para los investigadores informáticos, la pesquisa parte de otras fuentes, como por ejemplo el comportamiento de sus movimientos bancarios.

La piratería, confirma Bautista, ya no está en las calles sino que se ejerce desde el computador del hogar con solo hacer clic.

"Ahora los jóvenes empiezan bajando de la web programas freeware (sin costo), o cracks (herramientas para adulterar un software), y como creen que nadie se da cuenta de sus acciones, por ser actividades que se hacen en su casa, terminan como hackers profesionales", precisa el Mayor Bautista.

### **El rastro y los motivos**

Jeimy Cano es un ciberdetective, o mejor conocido como perito informático. Utiliza las técnicas y los métodos de la computación forense para recolectar evidencias digitales y resolver un caso.

Tal como sucede en los crímenes de la vida real, en el mundo virtual, "si hay clic hay rastro". Por ello, Cano sigue las migajas electrónicas como una manera de detectar fraudes cibernéticos, intrusiones, fuga de datos y espionaje industrial.

Como director del grupo de investigación de computación forense de la Universidad de los Andes, considera que la preocupación actual no es ni siquiera la tecnología, sino que es la gente. "Un motivo es la distancia que hay entre un hacker y un pirata informático", concluye Cano

Justo estos "motivos" son los que empiezan a convertirse en dilemas éticos para muchos jóvenes quienes inician muy temprano su actividad en la red de redes.

"En la actualidad, los piratas informáticos ya no buscan hacerse un nombre dentro del mundo de la informática, sino que persiguen un beneficio económico mediante la consecución de información confidencial de empresas y personas", precisa Daniel Rojas.

Fernando Castro es un estudiante universitario. Le asusta clasificarse como un hacker, aunque tuvo una fase como tal. Prefiere llamarse un gomoso, un entusiasta, al que le gusta atacar sus propios sistemas para probar la seguridad.

"Yo no puedo decir si está mal o bien hacer desaparecer unos cuantos dólares, o sacar información confidencial para compartirla en la red, pero creo que las personas que

hacen esto al menos deben entender que realizan tales actos por una decisión que ellos mismos toman y que si son descubiertos corresponde asumir las consecuencias de sus actos", remata.

### **El testimonio**

*"Mi interés siempre ha sido probar qué tan seguras son las redes a las cuales estoy conectado.*

*Cuando estaba en la universidad, la mayoría de los servidores usaban un versión popular de Unix, que tenía varios fallos de seguridad. Al principio explotaba esos fallos con exploits (herramientas descargadas de la red), los modificaba y adaptaba para que hicieran algunas cosas que me llamaban la atención como enviar correos electrónicos a los usuarios de la universidad, o apagar los servidores para que el sitio web estuviera fuera de servicio, todo con el fin de aprender y sí, también de hacer el mayor daño posible.*

*Mi decisión era ser un intruso incisivo, porque por más que le advertía a los administradores de la red, no me hacían caso. Siempre que caía un servidor lo volvían a subir sin solucionar los problemas de seguridad que tenía el sistema, lo que me impresionaba bastante y me sentía en la obligación de atacarlo de nuevo a ver si algún día mejoraban el servicio.*

*En los últimos seis años, las cosas no han cambiado mucho, en cuanto a hacer la plataforma más segura por parte de la universidad, tanto que aún tengo cuenta con privilegio de administrador de uno de los servidores principales.*

*Ahora me dedico a atacar mis propios sistemas para probar su seguridad y trato de entender cómo funcionan las redes de los diferentes proveedores de Internet de la ciudad; juego con las redes wireless (inalámbricas) y con otro tipo de redes, que es el área que más me gusta. En mi caso la motivación siempre ha sido adquirir más conocimiento".*

*Fernando C., estudiante*

### **La opinión**

*"Algunos jóvenes empiezan bajando programas sin costo de Internet, y como creen que nadie se da cuenta de sus acciones, porque lo hacen en su casa, terminan convirtiéndose en hackers profesionales"*

*Fredy Bautista, jefe de Delitos Informáticos de la Policía*

### **Entrevista completa, realizada por la periodista del Colombiano al estudiante Fernando C.,**

#### **1. ¿Cómo asumen los jóvenes en Medellín la cibercultura Hacker?**

*Una pregunta difícil, creo que en Medellín y en todo el mundo la cultura hacker y/o cibercultura se ha desvirtuado con respecto a lo que era hace unos años; quienes nos iniciamos en el mundo de las redes de información desde el 95 conocimos un mundo virtual diferente, donde las personas a quienes nos interesaba la cultura hacker aprendíamos casi con las uñas y teníamos todo ese ideal de los hackers de antaño, digamos que se preservaba todo ese ideal de los años 70, además porque por esos días empezaba a hacerse popular el sistema operativo Linux, el clon de Unix por excelencia, que reanimó a la cultura hacker de los 90 a continuar con las ideas que*

*casi se pierden por culpa de surgimiento de los sistemas operativos propietarios. Creo que hoy en día ya no hay muchos hacker reales, creo que por alguna razón se creo un fanatismo, dejo de existir ese ideal de hacer las cosas por uno mismo. Hace unas semanas estando en un cibercafé, escuchaba a 2 niños de 16 años hablando acerca de atacar sistemas y de extraer datos de máquinas de sus amigos, me di cuenta de las siguientes cosas:*

- Las personas mas jóvenes que yo, ya no programan sus propias herramientas y trabajan bajo el sistema operativo Windows; creo que parte de ser hacker y de estar en el rollo de la cibercultura implica ciertas actitudes culturales como usar un sistema operativo que no haga todo por ti, que puedas hacer las cosas y que tenga las herramientas necesarias para crear tus propias herramientas; los sistemas operativos tipo Unix, nacieron en la red de la mano de los verdaderos hackers, es por eso que para pensar siquiera en ser un hacker, tu actitud debe ser la de los antiguos hackers, los que hacían sus propios scripts, los compartían con amigos, los modificaban y los perfeccionaban, hacían sus propios sistemas operativos, o al menos gastaban horas compilando programas que luego modificaban y utilizaban para un propósito específico.*
- Creo que en la actualidad la idea de ser un hacker se ha desvirtuado y se piensa que un hacker es una persona que ataca un sistema para conseguir algún tipo de información, conseguir una contraseña, un número de tarjeta de crédito o apagarle el computador a tus amigos, crakear programas bajados de internet (Pero la gente no hace sus propios cracks), pero ese tipo de cosas definitivamente están muy fuera de lugar de lo que es o fue algún día el concepto de hacker; un hacker aparte de ser un experto en sistemas de redes y computación, es a la vez un entusiasta que tiene casi como única intención saber cómo funciona el sistema y mirar si puede mejorarlo; si se comenten errores y se causan daños, éstos pueden repararse; ser un hacker implica estar consciente de las sediciones que se toman, no se es un hacker por suerte, ni por usar programas ya listos para atacar sistemas o conseguir algún dato que necesites, de esta manera quizás se aprende algo, puede que avances o simplemente seas un Lammer más. Y eso creo que es lo que pasa con la mayoría de los jóvenes de hoy que se llaman hackers, deda sacar de ese prejuicio a las personas que usan Linux y están en el movimiento de software libre conscientes de sus implicaciones sociales y culturales, estas personas desde mi punto de vista tienen algún germen de lo que fue algún día la cultura Hacker.*

## **2. ¿Crees que entienden las implicaciones éticas de este ejercicio?**

*Ni yo mismo entiendo muy bien las implicaciones éticas que tiene hablar, intentar o ser un hacker, creo que ser un hacker en los términos expresados en la respuesta anterior, depende de una actitud y una posición clara en tu vida sobre lo que quieres hacer con el conocimiento que obtienes con los sistemas, las redes, la cibercultura; yo creo que no se daña o se ataca un sistema por aprender, cada una de esas cosas depende de una decisión que has tomado antes de hacer lo que sea que se haya hecho y por lo cual te han denominado hacker; muchas veces eres un hacker porque otras personas dicen que eres un hacker, porque te ven hacer cosas que ellos no sabían que era posible o simplemente porque usas un sistema operativo diferente. Antes dije que era importante usar Linux o un sistema Unix para al menos aspirar a ser un hacker, pero esto no quiere decir que todas las personas que usen Linux sean hackers, por estos días Linux ha empezado a ser un sistema operativo para usuarios normales y eso de verdad que está muy bien.*

Creo que la cibercultura ahora está basada en el anonimato, antes también lo estaba y sucedía porque se era perseguido por ser denominado hacker; hacer algo de manera "anonima", por lo general suele ayudar a que se desconozca toda posición ética; yo no puedo decir si esta mal o bien hacer desaparecer de una multinacional unos cuantos dólares, o sacar información "confidencial" para compartirla en la red, pero creo que las personas que hacen esto al menos deben entender que asumen tales actos por una decisión que ellos mismos toman, y que si son descubiertos toca asumir las consecuencias de dichos actos. Pero los actos antes nombrados no son típicos en los hacker, no determina que eso sea lo que hacen los hackers, ya que sé de personas con todas estas capacidades y no las utilizan de las maneras nombradas más arriba u otras peores, porque no es la idea que tienen de ser un hacker, muchas veces basta con saber que se puede hacer y que tenemos la capacidad de hacerlo; aplicarlo implica tomar una decisión que puede hacernos pasar la línea entre lo ilegal o lo legal del contexto social en el que vivamos, y ahí es donde nuestras decisiones de hacer "lo correcto" o lo "perverso" se convierten tal vez en decisiones catalogables como éticas.

### **3. ¿Si te consideras hacker, has hecho alguna acción que haya sobrepasado los límites legales o la privacidad de personas o empresas?**

Hace algún tiempo, algunas personas me consideraron un hacker, yo no soy tan osado de auto denominarme alguna cosa, aún me autodenomino gomoso cuando alguien me pregunta si soy esto o aquello.

Mi interés siempre ha sido probar qué tan seguras son las redes a las cuales estoy conectado, cuando estaba en la Universidad, siempre estaba leyendo sobre servidores tipo Unix, daba la casualidad que en la universidad en la que estudiaba en ese entonces (2001 mas o menos), la mayoría de los servidores usaban un versión popular de Unix, que tenía varios fallos de seguridad, al principio explotaba esos fallos con exploits descargados de Internet, los modificaba y adaptaba para que hicieran algunas cosas que me llamaban la atención como enviar correos electrónicos a todos los usuarios de la universidad, o apagar los servidores para que la pagina de la U estuviera fuera de servicio, todo con el fin de aprender y si también de hacer el mayor daño posible, y claro aprender sobre administración de redes unix y servidores, debo aclarar que mi decisión era ser un intruso incisivo, además porque por más que le advertías a los administradores de la red, no te hacían caso, siempre que caía un servidor lo volvían a subir sin solucionar los problemas de seguridad que tenía el sistema, lo que me impresionaba bastante y me sentía en la obligación de atacarlo de nuevo a ver si algún día mejoraban el servicio en dicha universidad, las cosas no han cambiado mucho en 6 años 8 (en cuanto a la implementación de las mejoras y hacerlo más seguro por parte de la universidad), tanto que aún tengo cuenta con privilegio de administrador de uno de los servidores principales de dicha universidad.

Años antes, mi actividad "de entusiasta informático" consistía en leer, debo decir que tuve acceso a la red desde el 95 y que comencé a utilizar Linux en el 98, al principio como usuario normal; más tarde me interesé por su funcionamiento y todas las pruebas y ataques, o como se quiera llamar, se restringían a mi propia red; sólo después de salir del colegio decidí atacar algún sistema externo, el que más recuerdo es el mencionado anteriormente, ataque otros sistema pero era por que tenían la misma configuración de servidores que el de esa universidad en la que estudiaba antes.

Ahora me dedico a atacar mis propios sistemas para probar su seguridad, y de pronto

a tratar de entender cómo funcionan las redes de los diferentes proveedores de Internet de la ciudad, juego con las redes wireless y con otro tipo de redes, que es el área que más me gusta.

**4. Cuál era la motivación mayor para emprender este tipo de acciones hackers? Curiosidad, notoriedad....**

En mi caso la motivación siempre ha sido adquirir más conocimiento, con el fin de poder luego prestar algún servicio en el área de servidores y seguridad informática, para conseguir algo de dinero para vivir, no me ha gustado sobresalir, ni mucho menos aparecer en los diarios o escribir historias y/o programas con fines "bélicos".

Una motivación muy importante siempre ha sido la curiosidad, el saber cómo funcionan las cosas, desde el televisor, el radio, el PC,(Hardware), hasta las redes y los sistemas "seguros".

**5. En general, en el pasado las acciones de los hackers buscaban notoriedad, en la actualidad qué buscan?**

Creo que en ningún momento las acciones de los verdaderos hackers buscaban notoriedad, muchas veces bastaba con satisfacer la propia curiosidad, liberar algo de conocimiento para el público, mejorar los sistemas existentes, compartir sus programas; gracias a los verdaderos hackers de antaño, existe el Internet que hoy conocemos, las listas de correo, los servicios de mensajería, las mejoras en los sistemas de cifrado y seguridad se lo debemos a los hackers; y no quiero decir que ser un hacker es ser un Héroe, pero los hacker de antaño casi lo eran a pensar de todos "los delitos" que se cometieron, creo que cada uno de ellos ayudó a mejorar en algo los sistemas actuales.

En la actualidad los actuales hacker se han convertido, o son los "gurus" del software libre, están creando programas con el ideal de compartirlos con las personas y mejorar el uso de los sistemas de redes; hay una preocupación por la libertad de la información tal como en los años anteriores, pero ahora hay un movimiento global que se apoya en la red de redes para luchar por esos derechos que van de la mano de la condición humana.

**6. Crees en la clasificación que algunos aseguran existen en la que se diferencian los hackers de sombrero negro, gris o blanco; o una más moderna como los crackers, lammers**

Nunca han existido los hackers grises, negros o blancos, estos han sido mitos creados por autores de novelas fantásticas, por gente que realmente no sabe del tema, o por la sociedad, con el fin de entender algo que no entiende del todo; por mi parte, considero que o eres un hacker con las características que mencione anteriormente, o eres un Lammer, o un Craker, estas divisiones existen desde el 60 y creo que se debe conservar e informar de dichas distinciones. Un cracker está totalmente interesado en atacar sistemas para obtener algún beneficio económico, por eso algunos crean virus, spyware, malware y esos bichos raros que les da al sistema operativo propietario que la mayoría de la gente usa; a los hacker actuales, si es que podemos llamarlos así, poco les interesa el tema de los crakers o lammers, para mí es una concepción social mal tomada debido a unos cuantos autores y a unos poderes sociales con la idea de malversar algo que no entienden y que le temen.

**7. En relación con el software libre hay una frontera interesante entre el Open Source y la cibercultura hacker. Es correcta esta apreciación?**

*Creo que esta pregunta está mal planteada; creo que la cibercultura hacker en la actualidad está completamente ligada al software libre, no sería posible concebir el software libre sin hackers como Richard Stallman, Linux Torvalds, Eric Raymond entre otros.*

*Creo que debo hablar de lo que es para mí la cibercultura, tema que se ha mencionado en la entrevista, la cibercultura hace referencia a una concepción colectiva del potencial de acercamiento social y cultural que trae para las personas la virtualidad que ofrece Internet -cuando Internet empezó a convertirse en lo que es ahora, con sus sistemas de mensajería instantánea, los grupos de trabajo en línea entre otros-. En el caso del software libre la cibercultura podría entenderse como toda esa comunidad que se generó alrededor de la idea de compartir, de la idea de que el conocimiento debe ser libre y por ende, las herramientas con las cuales nos enfrentamos a las redes y a los sistemas deben ser libres y entendibles; la posibilidad de descargar y modificar o negociar un programa, sin implicaciones legales negativas, es el principio básico de la cultura del software libre y en mi caso creo que es este principio el que define la cibercultura del pasado y de la actualidad, lo que se salga de esta idea, desde mi punto de vista, raya en el fanatismo y el desconocimiento de lo que se está haciendo.*

*El Open Source es otra cosa que en ocasiones raya en lo comercial pero que no trataré en esta respuesta.*

**8. Muchas de las personas quienes bajan contenidos por Internet sin pagar como música o software lo hacen porque creen que tienen un derecho frente a contenidos propietarios inalcanzables por su costo ...qué consideraciones tienes sobre esto?**

*Esto en términos "legales" se llama piratería, desde mi punto de vista la piratería no es mala y no se debe permitir la satanización de la misma, creo que la piratería de alguna manera es sana porque ayuda a que las disqueras y editoriales tomen conciencia sobre la explotación a los artistas, muchas veces los mismos artistas terminan incitando a la piratería de sus cosas; para eso ha aparecido Creative Commons, aire incondicional y licencias que pretenden proteger al artista con un modelo donde desaparecen los intermediarios entre el artista y el receptor, de esta manera se deja de llamar piratería el bajar una canción o un libro que esté bajo una de las licencias anteriores; en el caso del software y los programas de Internet creo que la piratería es innecesaria, ya que existe todo tipo de software libre para remplazar los software que no podemos comprar y que además no tenemos por qué comprar, el modelo del software propietario está en decadencia desde sus mismos inicios ya que desde mi punto de vista esa concepción va en contra de la naturaleza del ser humano informático, igual que Richard Stallman me pregunto que pasaría si tus amigos empiezan a cobrarte por las recetas de cocina, creo que eso es un problema que se ha manifestado entre el año pasado y este año con el asunto de las patentes de software, pero no quiero alargarme en este tema.*

## **Comentarios al artículo:**

Fernando Castro

Administrador de Redes

Estudiante de Filosofía, UdeA

Dice:

*Quedo con un sin sabor en la boca después de leer el artículo sobre piratas que publicaste en el colombiano el día de hoy. Primero el título ya está cargado de una cantidad de prejuicios que acompañan el concepto Hacker que todas las personas tienen; segundo, porque en tu artículo no haces la diferenciación, que debe hacerse, entre hackers, crackers, lammers, bucaneros, piratas, copy-hackers, entre otros. Tu artículo, tristemente para mí, lo único que hace es confirmar todos los temores que se han creado alrededor del término hacker y prácticamente lo dejas en el "concepto" de un adolescente desadaptado que encuentra en la informática una especie de refugio donde es aceptado por "sus conocimientos".*

*Me parece que dejas de un lado la definición del manifiesto hacker, y en ningún momento haces referencia un poco a los desarrollos y a los avances que gracias a los hackers se han logrado en la "informática", creo que eso era algo necesario si se pretendía ser objetivo con el artículo, ya que como te dije antes, lo único que deja este artículo para un lector desprevenido es una especie de temor hacia las personas que se denominan hacker; además, no queda claro a quién puede denominarse un verdadero hacker, la actividad del hacker no empieza por bajar programas piratas, ni mucho menos usarlos o venderlos, eso es algo que puede hacer cualquier persona y no es el interés de los Newbies (Los verdaderos aspirantes a hacker).*

*Por otro lado, no me queda más que decirte que me siento algo decepcionado al leer estas páginas, ya que realmente esperaba que trataras el tema de manera diferente y pudieras mostrar una visión que no todo el mundo conociera y que fuera aclaratoria para las personas, y no desinformar a las personas y mostrar a los hackers como unas personas faltas de ética y responsabilidad alguna frente al conocimiento que tienen.*

Alonso Quintero

Ingeniero Electrónico, de la UdeA

Profesor de Redes Informáticas del Sena

Dice:

*Algún día hablaba con alguien que porque publicaban esos artículos y me decía que era la única forma de llamar la atención, que si se hablaba de hacking y cyberpiratas en otros termino a nadie le interesaría.*

*A nadie le importa el sentido altruista de un muchacho al crear tecnología. Lo que le importa son las historias a lo "hollywood" donde el chico de 5 años es capaz de robar por Internet.*

*La cúpula y la anticúpula, así como vándalos corp (años 90) existieron y aún existen después de haber resucitado en facebook, pero nunca tuvieron ese enfoque, lo digo con conocimiento de causa.*

*Siempre que se escribe algo así es poco lo que se puede rescatar. Solo porque quien escribe los artículos JAMAS habla con las personas adecuadas, porque las personas adecuadas no van a hablar de eso. Se conforman con el primero que habla y hasta*

ahí llega la investigación.

*Y como siempre los perjudicados son las personas que leen esos "artículos" y que no saben nada de informática, son los que quedan con los temores, con la paranoia y eso lleva a que las empresas se aprovechen y cobren "mas duro", diciéndole a los clientes: "Mi señora, leyó lo que salió en el Colombiano?, eso de hackers, de piratas?, ellos le pueden robar, es mejor que pague el seguro de la tarjeta ..."*

*En fin, solo otro articulo más que desinforma.*

### **Carta de un Hacker a una editorial:**

*Hola, soy Cybor. Probablemente no me conozcan. Tampoco pretendo salir en la prensa. Eso no me importa, sin embargo si hay otras cosas que me interesan mas que mi identidad. Por ejemplo, me interesan las aperturas de sistemas cifrados. Pero eso es algo que nadie te enseña. Eso tienes que aprenderlo por ti mismo. También me interesa que todos sepáis quienes somos y que no estamos solos en este peculiar mundo. Me interesa que sepan que no todos los Hackers somos iguales. También me interesa saber que la palabra Hacker tiene un significado muy curioso. En un articulo reciente se publicó que se nos conocían como piratas informáticos. es probable, pero creo que están tremendamente equivocados. Quiero reivindicar mi posición. Pero lo cierto es que cada vez que hablan de nosotros es para decir que hemos reventado el ordenador de tal multinacional con grandes perdidas o que hemos robado cierta información. estas cosas suceden y particularmente tengo que decir que estas cosas están al alcance de otros personajes mas peligrosos que nosotros. En nuestro mundo habitan los crackers y los phreakers. También están los snickers y cada uno de ellos tiene su cometido, pero para la mayoría todos somos iguales y todos somos piratas informáticos.*

*Pero quiero ir por pasos. ¿ que te parece saber de donde procede la palabra Hacker ?. En el origen de esta palabra esta el término Hack - algo así como golpear con un hacha en ingles-, que se usaba como forma familiar para describir como los técnicos telefonicos arreglaban las cajas defectuosas, asestándoles un golpe seco. También mucha gente arregla el televisor dándole una palmada seca en el lateral. Quien hacia esto era un hacker. Otra historia relata como los primeros ordenadores grandes y defectuosos, se bloqueaban continuamente y fallaban. Los que las manejaban se devanaban los sesos creando rutas para aumentar la velocidad y cosas parecidas.*

*Estas cosas se denominaban Hacks y a los que lo hacían se les llamaban Hackers. Otra denominación se le hacia a aquel experto en cualquier campo que disfrutaba modificando el orden de funcionamiento del aparato. De esta forma siempre superaba las limitaciones y esto le producía una alta satisfacción. A estas personas también se les llamaban Hackers. Pero pronto surgieron otros acrónimos como Crackers. este acrónimo surgió allá por el año 1985, y fue inventado por los propios Hackers para diferenciar a aquel que fisgaba en un ordenador con aquel que creaba un virus dañino o copiaba un software. Así, frente a un ordenador ajeno un Hacker y un Cracker no son la misma cosa.*

*Por otro lado en algunas ocasiones un Hacker es muy útil porque siempre detecta un agujero en cualquier programa nuevo. Esto es bueno para ponerlo en conocimiento de la empresa que ha creado el programa. El Cracker aprovecharía este error para entrar en el programa y copiarlo. Aparte del Cracking existen otras formas de vandalismo*

tecnológico. Así, el Phreaking, por ejemplo es la manipulación de las redes telefónicas para no pagar las llamadas. El Carding se refiere al uso ilegal de las tarjetas de crédito. Y el Trashing consiste en rastrear la basura o residuos de los sistemas informáticos en busca de información como contraseñas.

Pero, volviendo a los Hackers. ¿ Como son ? ¿ Que aspecto tienen ?. Cuando alguien oye mencionar la palabra Hacker rápidamente se le viene a la cabeza un adolescente ojoso, con los ojos inyectados en sangre que ha pasado las últimas 24 horas delante del ordenador. esta imagen esta estereotipada. No es así. Un Hacker puede ser cualquier estudiante de informática o electrónica, que sale con los amigos y que tiene novia. Un Hacker es una persona normal como tu. Los Hackers son casi siempre gente joven. Quizás somos los que mas nos interesamos por la tecnología. Un Hacker normalmente despierta el gusanillo a temprana edad. Y no se hace de la noche a la mañana. Cuando logra serlo después de realizar un Hack, se busca un apodo y no da la cara por cuestión de seguridad. La gente todavía no confía en nosotros y nos ven con ojos malos. Normalmente al final de todo somos contratados por empresas importantes para ayudarles en su trabajo. y otra cosa que hacemos es contar como funciona la tecnología que se nos oculta. Este método se llama enseñar y creo que no es nada malo. De modo que si un Hacker escribe un libro es porque tiene algo que enseñar y nada mas. Bueno, creo que ya he escrito bastante. son las doce y media de la noche y mis padres ya se han acostado. Mañana tengo que madrugar. Y sobre todo quiero que quede buena constancia de lo que somos.

*Cybor, Bangor Diciembre del 96 Maine*

Esta carta o testimonio fue escrito hace más de 10 años y aún sigue vigente para todas las regiones del globo. De alguna manera esto nos lleva a cuestionarnos por el mantenimiento y dominio de ciertos paradigmas durante tanto tiempo, a pesar de tantas muestras, de casos múltiples que dan a entender la heterogeneidad del movimiento o comunidad hacker.

## **Bibliografía**

Hernandez Claudio, Hacker, 2000

Hernandez Claudio, Hackers los piratas del chip y de Internet 2001

Carlos Gradin. Internet, hackers y software libre. Editora Fantasma

Pekka himanen. La ética del hacker y el espíritu de la era de la información.