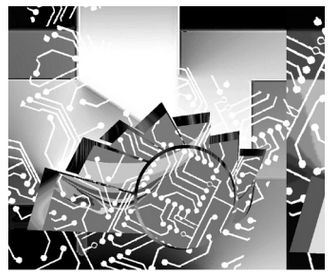

HACKERS EN LA SOCIEDAD DE LA INFORMACIÓN: ANÁLISIS DE SU DINÁMICA DESDE UNA PERSPECTIVA SOCIAL

HACKERS ON THE INFORMATION SOCIETY: ANALYSIS OF DYNAMICS FROM A SOCIAL PERSPECTIVE

Octavio J. Salcedo*

Carlos A. Fernández**

Lilia Castellanos***

Fecha de envío: Junio 2011
Fecha de recepción: Junio 2011
Fecha de aceptación: Noviembre 2011

Resumen

Desde los comienzos de la era de la información han existido seres geniales, creadores, aventureros, inconformes, entusiastas e innovadores, que han revolucionado con sus acciones y creaciones la sociedad en todos los aspectos; una sociedad que en gran parte ha cambiado por el avance de las ciencias de la computación y el auge de las tecnologías de la información y las comunicaciones (TIC). Estos personajes han despertado controversias de todo tipo, especialmente por el desconocimiento y el sensacionalismo de los medios de comunicación, quienes los han estigmatizado ante la opinión pública, en el límite de la delincuencia o el terrorismo informático. El presente artículo busca desmitificar el término *hacker* y es el resultado de un estudio serio, juicioso y dedicado del fenómeno *hacker*, que busca hacer justicia para su accionar y destacar los inmensos aportes que han hecho a las ciencias de la computación y al desarrollo de las TIC, sustentado en el análisis del fenómeno desde diferentes enfoques de investigación (técnicos, sociales, culturales, legales, políticos y económicos).

Palabras clave

Cibercultura, cibergrupos, cibersociedad, ciberterrorista, *cracker*, nética.

Abstract

Since the beginning of the information age have been a group of people who have given

* M.Sc. En Economía, M.Sc. en Ciencias de la Información. Universidad Distrital Francisco José de Caldas. Correo: osalcedo@udistrital.edu.co2 PhD in Micro Systems. AXP Microeletrônica. E-mail: christophebricout@yahoo.fr

** Ing. Sistemas, Físico-Matemático. Universidad Distrital Francisco José de Caldas.Correo: securecaf@gmail.com

*** Ingeniera de Sistemas, M.Sc(c).En Ciencias de la Información. Universidad Distrital Francisco José de Caldas: lilia.castellanos@gmail.com

an impulse by the curiosity and the creation to several technologies, a society that has largely changed by the advance of computer science and the rise of Information and Communications Technologies (ICTs). These characters have sparked controversy at all levels, especially due to ignorance and sensationalism of the media, those who have been stigmatized in the public eye, within the limits of computer crime or terrorism. Under these conditions, the term hacker for many is synonymous with computer crime, vandalism, cyberterrorism and for the few, the people great, innovative, creative, and disciplined and with a constant desire to learn more than anyone. This article seeks to demystify the term hacker and is the result of a serious, thoughtful and dedicated Hacker Phenomenon, seeking justice for their actions and highlight the enormous contributions made to computer science and the development of ICT, based on analysis of the hacker phenomenon under different research topics (technical, social, cultural, legal, political and economic).

Key Words
Cyberculture, cibergrupos cybersociety, cyberterrorism, cracker, netic.

Introducción

Algunos tildan a los *hackers* de piratas de la información, cuando en realidad son piratas del conocimiento y de la libertad, no usan un parche en el ojo ni un gancho en su mano derecha; por el contrario sus únicas armas son su conocimiento, su imaginación creadora, su computador, su conexión a Internet, sus herramientas y lenguajes. Su espacio no son mares bravíos y turbulentos sino la navegación hasta las fronteras del World Wide Web en la inmensidad del Internet, de los sistemas operativos, del software de base; su gancho son las herramientas y el conocimiento que día a día desarrollan. Su pensamiento es rebelde, como ha sido el de las personas inconformes que buscan encontrar la verdad y el conocimiento para beneficio de todos y no de unos pocos. En este sentido y de acuerdo con las definiciones del Jargon File [1], se pueden mencionar varias definiciones del término *hacker* que extienden el concepto más allá de los límites teleinformáticos, entre las cuales sobresalen:

- Persona que disfruta explorando los detalles de los sistemas programables y busca cómo expandir sus posibilidades, al contrario de la mayoría de los usuarios, que solo prefieren conocer lo mínimo para utilizarlos.
- Experto o apasionado de algo.
- Aquel que disfruta con el reto intelectual de superar las limitaciones de manera creativa.

En estas condiciones, cualquier persona que se apasiona por el arte o la ciencia que practica y que disfruta con los retos intelectuales que se propone y alcanza podría tener un perfil *hacker*. Los métodos y procedimientos usados por él son similares a los utilizados por la comunidad científica: inicialmente se plantea un problema que resolver, se realiza una experimentación práctica y mediante observación directa se hace un registro y análisis de datos. Posteriormente se establece una hipótesis o solución factible. En las dos comunidades se establecen diferentes grupos que compiten planteando diversas hipótesis para la resolución de un mismo problema. De ello se derivan una multiplicidad de teorías, lo cual resulta muy benéfico, pues la diversidad de ideas, soluciones y críticas objetivas enriquecen el conocimiento. Con la adopción del nuevo modelo de resolución de problemas,

los *hackers* y los científicos se dedican a publicar sus trabajos de forma que estos sean probados, verificados y desarrollados. Por lo anterior, no es raro encontrar muchos científicos que han desarrollado actitudes de *hacker* en sus investigaciones, lo cual les ha permitido interactuar y desarrollar progresivamente nuevas teorías e invenciones.

Los *hackers* crearon Internet, Unix, Linux, la World Wide Web y un largo etcétera, además de la mayoría de elementos que las componen; ellos fomentan la libertad en el uso de herramientas, sistemas y lenguajes no privativos con *copyleft*; desarrollaron los lenguajes y técnicas de programación, las telecomunicaciones y siguen luchando en un mundo cada vez más globalizado y abierto.

La cibersociedad y la cultura *hacker*

En la medida que la sociedad va siendo influenciada por las tecnologías de la información y la comunicación (TIC), se presentan cambios en todos los ámbitos (social, político, económico, académico y cultural); la aparición de estos cambios se remonta a la segunda mitad del siglo XX; cuando en 1946, después de tres años de trabajo, un equipo de ingeniería de la Universidad de Pennsylvania dirigido por J. Presper Eckert y John Mauchly crearon un aparato al que denominaron Electronic Numerical Integrator and Computer (Eniac). De allí en adelante durante varias décadas los computadores fueron máquinas enormes, complejas, costosas y de muy difícil manejo; por lo cual en los años 50 y 60 solamente las empresas que podían destinar recursos para su implementación y administración tenían acceso a estos *mainframes*.

Las computadoras de ese entonces estaban fuera del alcance del ciudadano común, hasta que Ed Roberts, fundador de MITS, creó un aparato llamado Altair 8800 que usaba un procesador Intel 8080 de 2 MHz, tenía únicamente 256 bytes de memoria, no tenía disco duro, monitor ni teclado y el usuario se comunicaba a través de interruptores y luces de su panel frontal. A partir de ese momento las computadoras salieron de las grandes factorías a los hogares y comenzó la transformación de toda la humanidad. Esta revolución tecnológica ha venido modificando el comportamiento, el conocimiento y el pensamiento social y ha forjado la configuración de una nueva sociedad de la información, denominada cibersociedad [2].

El estudio de la cultura *hacker* resulta de gran importancia e interés, teniendo en cuenta los nuevos paradigmas científicos y tecnológicos de la sociedad de la información (cibersociedad) y la nueva cultura tecnológica y digital (cibercultura), que sirven de marco social, político y tecnológico a personajes míticos, entre los cuales se destacan los *hackers*. Estos, contra la desinformación de los medios, se constituyen en verdaderos revolucionarios de las tecnologías de la información, cuyo accionar ha permitido el notable desarrollo tecnológico alcanzado por la ciencia informática y las telecomunicaciones. Para ello se apoyan en modelos de conducta relacionados con la libertad de información, la descentralización, la democratización del conocimiento, la apertura de los medios, el equilibrio social, y se constituyen en una cultura libre [4], creadora y de innovación constante. Algunos sociólogos y filósofos, entre ellos Manuel Castells (profesor universitario, catedrático de sociología y de urbanismo en la Universidad de California en Berkeley) y Pekka Himanen (filósofo finlandés, investigador en Finlandia e Inglaterra y en las universidades de Stanford y Berkeley), han dedicado algunos de sus escritos al estudio del fenómeno *hacker*, motivados por la gran admiración que sienten por

esta cibercultura, la lógica interna que regula sus actividades, sus fuerzas conductoras, su actitud, su ética y el enorme desafío espiritual que suponen para esta época. Se considera, así, que la cultura y el fenómeno *hacker*, como reflejo de la cibersociedad, merecen ser estudiados profundamente, y se rescatan con ello sus innumerables aportes al desarrollo de la teleinformática al acercar la tecnología de la información a los pueblos, sin distinciones políticas, económicas y sociales.

El fenómeno *hacker*

Los verdaderos *hackers* tecnológicos son individuos con un alto nivel de conocimiento teleinformático, que en algunos casos se dedican a revisar y proponer soluciones a las vulnerabilidades en redes de computadores y sitios web. Los *hackers* no son delincuentes. Sin embargo, el término adquirió una connotación negativa debido a su uso generalizado, a la ignorancia mediática y a los intereses creados. A su alrededor se tejen muchas historias como sucede con los temas que han sido superficialmente estudiados y sobre los cuales existe desconocimiento y poca investigación; al respecto abundan varias interpretaciones acerca de lo que es un *hacker*, cuyas definiciones varían de acuerdo con la posición política, social y económica del grupo o individuo que lo defina, desde un intruso malintencionado hasta genios de las computadoras; no obstante, los *hackers* son representantes de la nueva sociedad de la información, fanáticos de la informática, que tienen una motivación creciente en aprender acerca de los sistemas, cómo desarrollarlos, optimizarlos y usarlos de forma innovadora y libre [3].

El término *hacker* ha adquirido diversos significados a través del tiempo, por lo cual es necesario hacer una retrospectiva y hacer un análisis evolutivo de este fenómeno, destacando los eventos más importantes que dieron origen a esta fascinante cultura. Inicialmente, se les llamaba *hackers* a los técnicos de telefonía por la forma en que solían reparar los teléfonos. Mediante un golpe seco y certero ponían de nuevo en marcha el teléfono (*hack* es hachazo en inglés) [4]. Con la aparición del computador ENIAC de Eckert y Mauchly, se formó una cultura técnica con cierta continuidad, consciente de sí misma, conformada por programadores entusiastas que creaban y manipulaban software por pura diversión, curiosidad y conocimiento.

Años más tarde, en 1959, un grupo de estudiantes del Massachusetts Institute of Technology (MIT) tomó el título de *hackers* de estos técnicos, por las soluciones que adoptaron para entrar sin autorización en la única computadora de la universidad, sin necesidad de penetrar físicamente en la habitación. Este grupo de alumnos, en su mayoría pertenecientes al TMRC (Tech Model Railroad Club: http://tmrc.mit.edu/), tomó un curso de programación con la computadora IBM 407. Los programadores no tenían acceso directo al sistema y requerían la intervención de un operador; en estas condiciones, los resultados de los trabajos académicos de programación solían demorar mucho tiempo y los jóvenes del TMRC lograron escribir sus programas directamente, registrar los resultados y operar sobre ellos desde una especie de miniordenador que se constituiría en la semilla del futuro computador personal. Poco después, la IBM 407 fue reemplazada por la TX-0, una computadora revolucionaria para su época, y el grupo del TMRC fue convocado por Jack Dennis, un antiguo miembro del grupo y profesor del MIT, para experimentar con el nuevo equipo. El TX-0 ya no funcionaba con tarjetas perforadas, en su lugar tenía incorporado un teclado que permitía a

los programadores observar los resultados de sus trabajos. A los de este grupo se los denominó *hackers* y ellos crearon la forma de relacionarse con las computadoras, conocerlas, experimentar con ellas y aprovecharlas al máximo, con la condición de otorgar libertad de acceso y circulación a los conocimientos obtenidos en sus investigaciones. Esta ética, con muy pocas modificaciones, se ha mantenido a través del tiempo.

La aparición de la red Advanced Research Projects Agency Network (Arpanet), en 1969, permitió reunir a *hackers* de toda Norteamérica en un grupo cohesionado e interconectado, reemplazando los pequeños grupos aislados. La cultura *hacker* se desarrolló en las universidades conectadas a la red, especialmente en los departamentos de informática y ciencias de la computación.

Otro foco importante en la cultura *hacker* lo constituyó el PARC (de Palo Alto Research Center), también conocido como Xerox Parc. Durante más de una década, en los años 70 y mitad de los 80, el PARC produjo una sorprendente cantidad de innovaciones revolucionarias en hardware y software. El mouse moderno, las ventanas y la interfaz gráfica basada en íconos fueron inventadas en este centro de investigación. Otros inventos y desarrollos importantes del PARC fueron la impresora láser, las redes de área local (Ethernet), las tecnologías de disco óptico y LCD, la interfaz gráfica de usuario (GUI), avances en la escala de integración de circuitos (VLSI), computación ubicua, programación orientada a objetos (OOP). Paradójicamente, la serie D de computadoras del PARC se anticiparon a los PC de los 80, en más de una década [5]. Infortunadamente, estos visionarios no tuvieron el suficiente reconocimiento en su propia empresa; no obstante, su influencia en la cultura *hacker* fue profunda.

El mismo año en que nació Arpanet, un ingeniero de Laboratorios Bell llamado Ken Thompson inventó el sistema operativo Unix [6]. Thompson había estado involucrado en el desarrollo de un sistema operativo de tiempo compartido llamado Multics. La idea era que Multics fuese más fácil de usar y de programar, para que el usuario y el programador pudiesen enfocarse en sus verdaderos trabajos. Laboratorios Bell abandonó el proyecto cuando Multics fue creciendo hasta convertirse en un enorme sistema aparentemente inútil. Ken Thompson aprovechó el entorno Multics y comenzó a realizar pruebas, implementando una mezcla de sus características y algunas ideas propias, en una vieja DEC PDP-7. Dennis Ritchie, otro investigador, inventó un nuevo lenguaje, llamado C, para usarlo en el naciente Unix de Thompson. Al igual que Unix, C fue diseñado para ser ameno, flexible y no imponer límites. El interés por estas herramientas se fue extendiendo por Laboratorios Bell y varios grupos de *hackers* se interesaron por su estudio y conocimiento.

En el Homebrew Computer Club, donde se presentó por primera vez la Apple I, diseñada y creada por Steve Wozniak, se formó un primer grupo del *underground* digital de jóvenes y *hippies* radicales que buscaban una revolución en la información a partir de las computadoras de hogar. Ted Nelson, uno de los primeros en hablar de computadoras personales, inventó los términos de hipertexto e hipermedia mucho antes de que sugiera Internet. Para ello fundó el proyecto Xanadu en 1960, el cual consistía básicamente en concebir un documento global y único que cubriera todo lo escrito en el mundo, mediante una gran cantidad de computadores interconectados, que contuvieran todo el conocimiento existente. También acuñó el término ciberfraude para calificar a quienes se oponían al otorgamiento del poder cibernético al pueblo [7].

Un grupo de *hackers* del Unix provenientes de Standford y Berkeley fundaron Sun Microsystems en 1982, entre ellos Andy von Bechtolsheim y Bill Joy, aprovechando el hecho de que Unix podría correr en hardware relativamente económico basado en el 68000; su visión fijó las normas para toda una nueva industria. Aunque los precios estaban fuera del alcance de muchos particulares, las estaciones de trabajo resultaban baratas para las empresas y universidades. Hacia 1984 existían en EE.UU. cuatro mil instalaciones de Bulletin Borrad System (BBS). Los BBS se componían de una computadora y un módem que se enlazaban a una red de computadoras personales con el objeto de centralizar información e intercambiar mensajes.

The Hackers Conference comenzó en 1984, con sede en California, como un encuentro anual de ejecutivos de tecnología, académicos, periodistas y empresarios de las telecomunicaciones. Desde ese entonces tienen lugar en el mundo otras conferencias de *hackers*, aunque la mayoría son de seguridad de información. Merecen la pena citarse las de Defcon en las Vegas, y el Black Hat, ambas creadas por el *hacker* Jeff Moss [8]. En este año también se publicó el libro *Hackers Heroes of the Computer Revolution* de Steven Levy [9], donde se estableció por primera vez las reglas generales del proyecto *hacker*. Los principios expresados por el autor todavía se mantienen y son respetados por la mayoría de *hackers* y de alguna manera regulan el propósito original del *hacking*: acceso libre a la tecnología digital y al conocimiento informático. Algunos de los principios de Levy son los siguientes:

- El acceso a las computadoras, con el fin de aprender, debe ser ilimitado.
- Toda información debe ser libre y gratuita.
- Los *hackers* deben ser juzgados por sus *hackeos* y no por su raza, edad, posición social o títulos.

En 1985 Richard Stallman, formó la Fundación del Software Libre (FSF, Free Software Foundation) y se dedicó a la producción de software libre, de calidad [10]. Su filosofía ha guiado desde entonces a muchos entusiastas y *hackers* y ayudó en la transición que iba a experimentar la cultura *hacker* a principios de esa década. En el año 1982 se comenzó la construcción de un clon completo de Unix, escrito en C y disponible gratuitamente. Este proyecto se conoció como sistema operativo GNU (GNU no es Unix) en una especie de sigla recursiva. El sistema GNU pronto se convirtió en un foco importante de la actividad de los *hackers* y durante más de una década, la Free Software Foundation de Stallman definiría en gran parte la ideología común de la cultura *hacker*.

En 1991, un estudiante de la Universidad de Helsinki, llamado Linus Torvalds, había empezado a desarrollar un *kernel* libre para máquinas 386 usando el conjunto de herramientas de la FSF, y un profesor de la Universidad de Helsinki, Ari Lemke, le animó a colgar su sistema operativo en la web universitaria para compartirlo [11]. Desde entonces, Linux ha atraído a muchos *hackers* de Internet con la intención de ayudar al desarrollo y crecimiento de Linux, un sistema Unix completo de código fuente totalmente abierto y redistribuible. La evolución de Linux ha sido completamente diferente de la de otros sistemas operativos. Desde el primer momento, fue programado de forma eventual por un gran número de voluntarios coordinados a través de Internet. La calidad se forjaba sin estándares rígidos o autocracia; en vez de ello se usa una estrategia sencilla de hacer publicaciones semanales y obtener la respuesta de cientos de usuarios en cuestión de días.

A finales de 1993, Linux podía competir en estabilidad y fiabilidad con muchos de los Unix comerciales y contaba con una cantidad inmensamente mayor de software, colaboradores y entusiastas programadores. Por su portabilidad, velocidad y desempeño, comenzaba a atraer adaptaciones de aplicaciones comerciales. Un efecto indirecto de este desarrollo fue la desaparición de casi todos los pequeños proveedores de Unix propietario. Berkeley Systems Design Incorporated (BSDI) prosperó ofreciendo los programas fuente completos junto a su Unix basado en BSD y cultivando estrechos lazos con la comunidad *hacker*.

A finales de los 90, las principales actividades dentro de la cultura *hacker* eran el desarrollo de Linux, herramientas de seguridad, aplicaciones y la universalización de Internet. La World Wide Web había convertido a Internet en un medio de comunicación de masas. Esta popularización de Internet confirió a la comunidad *hacker* cierta respetabilidad y autoridad política y en 1996 los *hackers* desarrollaron una amplia coalición contra la llamada "Acción por la Decencia en las Comunicaciones" (CDA), impidiendo la llegada de la censura a Internet [12].

Desde sus comienzos, los *hackers* han sido perseguidos por las autoridades y han sido estigmatizados por los medios de comunicación como ciberdelincuentes; esta interpretación errada ha cambiado un poco, en el sentido de diferenciar ligeramente a los *hackers* de los *crackers* maliciosos; no obstante, con el alcance creciente de Internet y el acceso de nuevos cibernautas a la red, han proliferado diferentes tipos de atacantes, incluyendo *crackers*, piratas de software, novatos (*lammers*), *script kiddies* y delincuentes electrónicos, cuyo accionar ha sido asimilado al término *hacking* [13].

Como se evidencia en la reseña histórica anterior, mucho ha sucedido desde que este grupo de estudiantes del MIT marcara, apenas sin darse cuenta, una definición para este tipo de actos de conseguir unas horas delante del computador; hoy es toda una cultura. Desde entonces las técnicas de *hacking* y la propia tecnología han cambiado mucho, y el espíritu *hacker* de investigación, conocimiento, colaboración y anonimato sobrevive a pesar de la estigmatización y mala información de los medios masivos.

No obstante, la participación de los *hackers* en el desarrollo de las TIC es innegable, y a pesar de que no tienen reconocimiento por parte de las empresas y gobernantes, las comunidades científicas, académicas y universitarias han empezado a estudiar este fenómeno de una forma más equilibrada y justa; pues la investigación, la innovación y el desarrollo siempre está presente en el accionar de estos entusiastas gurús de la era de la información.

Características y personalidad

De acuerdo con el mito popular, es necesario ser un *nerd* para ser un *hacker*; pues al ser un marginado social, el *nerd* puede mantenerse concentrado en las cosas realmente importantes, como pensar y *hackear*. No obstante, en la actualidad los *hackers* distan mucho de este perfil, mantienen una concentración suficiente en las tareas de *hacker* para ser buenos en ello y disfrutan de una vida normal. El objetivo del *nerd* no es siempre generar un resultado, mientras que la actividad del *hacker* siempre tiene un resultado, de utilidad o no, pero siempre lleno de experiencia [14].

Hacker es quien se interesa por la tecnología, alguien que posee ansias de tener conocimientos sobre algo; alguien normal, con sus miedos

y sus dudas, pero que posee una fuerte voluntad para pasarse horas delante del computador probando cosas. Le encanta descubrir cómo funcionan los programas o por lo menos para qué sirve cada cosa. Al *hacker* le entusiasma todo lo que rodea la tecnología, la telefonía celular, los computadores, las tarjetas de crédito electrónicas o los satélites, normalmente lee demasiadas revistas y estudia complicados libros y artículos técnicos.

El *hacker* es, entonces, una persona normal, con amplios conocimientos acumulados a fuerza de empeño, y normalmente suele sorprender con su forma de ver la vida.

El ser *hacker* es una actitud, una forma de vida, una tendencia cultural y una forma de acercarse a lo que uno disfruta, de manera alegre, audaz, retadora y curiosa. Por ejemplo, Mozart fue un excelente *hacker* de la música y disfrutaba sus composiciones.

En concepto del filósofo finlandés Pekka Himanem [15], la ética del *hacker* considera varios valores característicos de la sociedad en red; la pasión se constituye en el valor orientador de la vida del *hacker*, a través de la incesante búsqueda de conocimiento cuya realización le colma de energía y gozo. Un elemento esencial de la ética *hacker* es su actitud en relación a las redes o la nética, la cual implica una completa libertad de expresión en la acción, privacidad para proteger la creación de un estilo de vida individual y rechazo de la receptividad pasiva. El *hacker* que vive según esta ética, en estos tres niveles de trabajo, dinero y nética, consigue el más alto respeto por parte de la comunidad.

Personas que parecen hackers pero no lo son

La comunidad informática ha difundido durante muchos años el uso del término *hacker*, para identificar a los atacantes de redes y sistemas informáticos; igualmente, el término *cracker* ha sido empleado para hacer referencia a *hackers* maliciosos, que se infiltran en un sistema para ganar pericia o beneficio propio. Infortunadamente, los términos han evolucionado y se han convertido en sinónimos de criminal informático; no obstante, los términos *hacker* y *cracker* se han establecido para distinguir una línea delgada, trazada entre el bien y el mal de su accionar. Es importante comentar que la mayoría de estudiosos de las ciencias de la computación y de la seguridad de información están usando términos más apropiados para referirse a individuos que no son *hackers*, entre los cuales están: *hacker* malicioso, atacante o intruso [16]. Para clasificar las distintas tendencias y manifestaciones de estos cibergrupos, debemos tener en cuenta sus objetivos, intencionalidad, destrezas, conocimiento y técnicas de ataque. Los principales grupos que han sido distinguidos por varios autores y organizaciones son los siguientes:

Crackers: en realidad son *hackers* maliciosos, cuyas intenciones tienen fines ilícitos, que van más allá de experimentar y conocer. Mediante ingeniería inversa crean seriales, generadores de claves/llaves (*keygens*) y *cracks*, los cuales sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican. El *cracker* viola la seguridad de un sistema informático de forma similar a como lo haría un *hacker*, solo que a diferencia de este último realiza la intrusión con fines de beneficio personal o para hacer daño. Por esa razón se les denomina *crackers*, ya que quebrantan los sistemas de seguridad, la actitud y las éticas *hacker* explicadas anteriormente; quieren demostrar de lo que son capaces, pero han dejado de lado la verdadera filosofía del *hacker*, haciendo primar su lucro económico y el deseo de hacer daño para ser reconocido.

Lammers y *Script Kiddies*: es el grupo más numeroso y con mayor presencia en la red. Son individuos con ganas de efectuar acciones de *hacking*, pero carecen del conocimiento técnico necesario. Son novatos que desean llegar a ser *hackers* y se denominan como tales, sin serlo. Aprovechan todas las herramientas y programas que circulan por la red y las utilizan sin entender su funcionamiento y los conocimientos técnicos empleados en su desarrollo. Este es quizás el grupo que más peligro representa para las redes y sistemas, pues ponen rápidamente en práctica todo el software de *hacking* que encuentran y bajan de Internet. Emplean de forma habitual programas *sniffers* para espiar las redes, interceptan contraseñas y correo electrónico y envían después varios mensajes con direcciones falsas amenazando el sistema. El *lammer* ejecuta programas creados por otros y sus acciones están orientadas a molestar o ganar notoriedad y popularidad en su grupo de amigos.

Newbies o novatos: son los que empiezan a aprender *hacking* a partir de las herramientas disponibles en la web. Inicialmente no hacen nada y aprenden lentamente. Son los aspirantes a *hacker*, que han entendido la verdadera filosofía del *hacking*, su intención es ir aprendiendo y superando retos para llegar a niveles muy altos en el conocimiento de la informática, los computadores, las redes y las TIC. Si tienen tenacidad, inteligencia, paciencia y son creativos, con el tiempo serán *hackers*.

Piratas informáticos: erróneamente y muy a menudo son confundidos con *hackers*; los piratas informáticos son aquellos que copian programas o reproducen software en forma ilegal y venden ilícitamente las copias de todo tipo de programas comerciales, DVD, CD de música, textos, películas y software.

Phreakers: tienen altos conocimientos autodidactas de telefonía y conocen los sistemas telefónicos. Son los *crackers* de las redes de telefonía y comunicaciones. El *phreaking* se refiere a los diferentes procedimientos y técnicas empleadas por determinadas personas para engañar a las empresas de telecomunicaciones y utilizar los servicios sin pagar, mediante el uso de hardware y software.

En otras clasificaciones se incluyen otras categorías, entre las cuales sobresalen los *sneakers*, que son espías informáticos y utilizan sus conocimientos informáticos para espiar. El *snuffer* es una variante del anterior. Se limita a averiguar claves de acceso a sistemas y describe agujeros y errores en los programas. Otro término utilizado es el de *rider*, que alguna vez estuvo en las categorías anteriores, pero que después empezó a trabajar legalmente y usar sus conocimientos.

Conclusiones

La nueva sociedad de la información, denominada cibersociedad, considera la información como un recurso económico fundamental, el cual se constituye en la base del desarrollo actual. Los recursos teleinformáticos, incluyendo las redes de alta velocidad, facilitan los medios a través de los cuales se localiza y comunica dicha información. Los cambios producidos en esta cibersociedad se manifiestan en todos los ámbitos: económico, político, cultural, académico y social.

En la actualidad, la masificación de la computación personal y la conectividad a través de Internet han favorecido el cambio de los hábitos de los individuos, relacionados con sus pasatiempos, la educación y la cultura. Destaca la ampliación del entorno de una cultura informática o cibersociedad, a la cual pertenecen

jóvenes con amplia imaginación, conocimiento informático y curiosidad, que disfrutan la exploración de los nuevos componentes teleinformáticos disponibles y sacan el máximo provecho a sus posibilidades.

Desde los tiempos del Club del Ferrocarril del MIT, las técnicas de *hacking* y la propia tecnología han cambiado mucho; sin embargo, el espíritu *hacker* de investigación, conocimiento, colaboración y anonimato sobrevive, a pesar de la estigmatización y mala información de los medios masivos.

Muchos de los avances de las tecnologías de la información, las comunicaciones, la computación, la inteligencia artificial, la nanotecnología han sido logrados, influenciados, impulsados y mejorados por ellos; incluso los símbolos más conocidos de nuestra era, Internet, las redes, el computador personal, las herramientas de desarrollo de software, el software, los sistemas operativos (entre ellos, los más destacados, Unix y Linux) y los componentes de seguridad, no fueron en realidad creados por empresas o gobiernos, sino por individuos entusiastas, curiosos, inteligentes y disciplinados que pusieron en práctica sus ideas.

La proliferación de herramientas en Internet, la facilidad de uso de estas herramientas y la disponibilidad de sitios web y libros que describen exactamente cómo explotar las vulnerabilidades han aumentado considerablemente la población de *crakers*, *script kiddies*, *lammers*, piratas informáticos, delincuentes y atacantes. A medida que más vulnerabilidades son descubiertas cada día, muchas más personas están interesadas en tratar de explotarlas. Algunos solo quieren satisfacer su curiosidad, quieren alardear ante los demás, mientras que otros tienen distintos objetivos, destructivos o monetarios, en mente.

El hacking también puede ser considerado como un continuo desafío a la sociedad de la informática para crear mejores productos, prácticas y procedimientos. Si los *hackers* no estuvieran continuamente tratando de *hackear* los productos, estos no podrían seguir evolucionando en la forma que lo están haciendo. Seguramente, los productos seguirían creciendo en funcionalidad, pero no necesariamente en seguridad.

Referencias

[1] E. Raymond. "The Jargon File, version 4.4.7". 29 de diciembre de 2003. [En línea]. Disponible en: http://catb.org/jargon/

[2] L. Joyanes. *Cibersociedad. Los retos sociales ante un mundo digital*. Madrid: McGraw-Hill, 1997.

[3] R. H. Ríos. *La conspiración* hacker. Buenos Aires: Longseller, 2003.

[4] Wikipedia. [En línea]. Disponible en: http://es.wikipedia.org/wiki/Hacker

[5] Wikipedia. [En línea]. Disponible en: http://en.wikipedia.org/wiki/Xerox_Parc

[6] H. Hahn. *Unix sin fronteras*. México: McGraw-Hill, 1995.

[7] T. Nelson. *Project Xanadu*. [En línea]. Disponible en: http://www.xanadu.net/

[8] Defcon. *Jeff Moss in the news*. [En línea]. Disponible en: https://forum.defcon.org/showthread.php?p=98012

[9] S. Levy. *Hackers: Heroes of the Computer Revolution*. Nueva York: Penguin Books, 1994.

[10] Free Software Foundation. Disponible en: http://www.fsf.org/.

[11] L. Torvalds. *Bio*. 7 de septiembre de 2007. Disponible en: http://www.linux.org/info/linus.html.

[12] Eric Raymond. *Breve historia de la cultura* hacker. *La gran explosión de la web*. Disponible en: http://www.wikilearning.com/monografia/breve_historia_de_la_cultura_hacker-la_gran_explosion_de_la_web/7955-8.

[13] C. Pérez, J. Agudín, A. García. *La Biblia del* hacker. Madrid: Anaya, 2003.

[14] E. S. Raymond. *How to Become a Hacker*. 2001. [En línea]. Disponible en: http://www.catb.org/~esr/faqs/hacker-howto.html

[15] P. Himanem. *La ética del hacker y el espíritu de la era de la información*. Barcelona, 2001.

[16] M. Castells. "*Hackers*, *crackers*, seguridad y libertad". Lección inaugural del curso académico 2001-2002". UOC. [En línea]. Disponible en: http://www.uoc.es/web/esp/launiversidad/inaugural01/hackers.html