Práctica y motivación en el entorno hacker: un análisis empírico

Umi hacker rembiapo ha omokyre'ỹva ichupekuéra: ñehesa'ỹjo

Practice and motivation in the hacker environment: an empirical analysis

Anton P. Baron

Universitat Oberta de Catalunya (España)
Universidad Tecnológica Intercontinental (Paraguay)
Investigador, miembro de la Vicerrectoría de Investigación Científica y Tecnológica
Universidad Tecnológica Intercontinental
antonbaron@gmail.com

Resumen

El propósito de este artículo es describir y examinar críticamente las características de una muestra de 30 hackers de habla hispana: analizar los factores demográficos de los mismos, su preparación tecnológica, las principales actividades que realizan en la Red y las motivaciones que los impulsan a su ejecución. El diseño metodológico incluye un estudio de campo de tipo no experimental descriptivo. La estrategia de muestreo es del tipo no probabilístico, en consecuencia la muestra no es representativa de ningún universo previamente establecido. Los datos se obtuvieron a través de cuestionarios enviados vía e-mail o colgados en los foros discusión. Los hackers que participaron del estudio provienen de España y de los países latinoamericanos; son, en su mayoría, varones y su edad oscila entre 14 y 34 años. Son profesionales o estudiantes en el campo de la informática y todos se dedican a la programación de software de fuente abierta. Las motivaciones para la realización del hacking, por lo general, podrían calificarse de "superiores" e intrínsecas.

Palabras clave: Hackers, Sociedad de la Información, Libertad en Internet, Software libre, Las motivaciones de los hackers, Hacking.

Mombykypyre

Ko jehaipy rupive oñemoha'ãngahai ha oñehesa'ỹjose hekópe porã mba'éichapa 30 hackers oñe'ẽva castellano: oñehesa'ỹjo moõguápa hikuái, iñemoarandu tecnología jeporúpe, mba'e ojapovéva hikuái Red-pe ha opa mba'e omomýiva ichupekuéra ojapo haguã ojapóva. Metodología-pe oguereko tembiapokue okapegua experimental descriptivo oñehenóiva. Oñembyaty haguã marandu noñemohendái mamoitéguipa ojeguerúta, upéva rupi muestra ndaha'éi peteĩ hendaguapegua meme. Marandu oñembyaty mba'eporandu ojeguerahaukava'ekue kuatiaveve rupi térãkatu ojehupiva'ekue umi aty ko'ã mba'e rehe omba'apovakuéra apytépe. Umi hackers oñemba'eporandu hague hína España ha tetãnguéra latinomerica-ygua; kuimba'ememe nunga hikuái, imitãvéva oreko 14 ary ha itujavéva katu 34 ary. Umi tapicha oñembokatupyry informáticape térãkatu oñemoaranduvahína ha maymavete omba'apo software opavavépe guarã ñemoheñóipe. Mba'érehapa ojapo hikuái pe hacking oñehenóiva, ikatu oje'e ojapoha hikuái oĩ rehe mba'e ipypeguakuéra omokyre'ỹva ichupekuéra.

Mba'e mba'e rehepa oñe'ẽ: Hackers, Sociedad de la Información, Libertad en Internet, Software libre, Omokyre'ỹva hackers kuérape, Hacking.

Abstract

The aim of this article is to describe and critically examine the characteristics of a sample of 30 Spanish speaking hackers, to investigate their demographic factors, their technological preparation, their main activities on the internet and the motivation that drives the implementation of their activities. The methodology includes a non-experimental descriptive field study. The sampling strategy is not probabilistic therefore the sample is not representative of any previously established population. Data were collected through questionnaires sent via e-mail or posted on discussion forums. The hackers who participated in the study come from Spanish and Latin American countries and are mostly males aged between 14 and 34. They are professionals in the field of Computer Studies and all are engaged in the programming of open source software. Their motivation for carrying out the hacking could usually be described as superior and intrinsic.

Keywords: Hackers, Information Society, Internet Freedom, Free Software, Motivations of hackers, Hacking.

Práctica y motivación en el entorno hacker: un análisis empírico

Puesto que a los hackers se les tilda de "delincuentes informáticos" y que esconden sus actividades de hacking en el anonimato, todavía circulan opiniones y mitos muy dispares acerca de sus verdaderas identidades e intenciones. Los que rechazan el supuesto carácter delictivo de sus actividades, en contrapartida los consideran como unos verdaderos genios de la informática y asiduos defensores de la libertad en la Red Internet. Por eso, en la primera parte de este estudio se pretendió ofrecer una descripción demográfica de los 30 hackers encuestados de habla hispana: sus edades, experiencias laborales e informáticas. También, dado el carácter de sus actividades, me pareció bien indagar la forma en la que actualizan sus conocimientos, la experiencia que tienen en la programación de software y sus preferencias en cuanto a los diferentes lenguajes de programación.

En segundo lugar, se trata de recabar opiniones de los hackers sobre el software comercial o de fuente cerrada. ¿Qué piensan y qué hacen al respecto? ¿Comparten aquella hostilidad que se les imputa hacia los propietarios de software comercial? En caso afirmativo, ¿se limitan a combatirlos en forma indirecta, o sea, colaborando en el desarrollo de software abierto u ocasionalmente, emprenden acciones directamente orientadas a perjudicar las empresas de software de fuente cerrada?

Finalmente, se estudiaron las motivaciones que tienen los hackers para realizar sus actividades y cómo estos factores motivacionales influyen en su forma o estilo de trabajo. ¿Será que se dedican a la programación de software con mucha pasión? ¿Es ésta su principal actividad en la Red? ¿Qué es lo que los motiva a realizar las actividades del hacking?

¿Quiénes son los hackers?

Existe una gran disparidad de criterios a la hora de definir el fenómeno hacker: mientras que algunos medios de comunicación, influenciados probablemente por las empresas transnacionales de software, emplean este apelativo "para calificar a toda persona involucrada en actos que atentan en contra de la propiedad intelectual, seguridad en las redes, autores de virus, intrusos de servidores, interceptores de mensajes de correo, vándalos del ciberespacio" (Machado, 2003), otros autores los perciben como unos románticos luchadores por la libertad en la Internet, que merecen la denominación de los "nuevos filósofos libertarios" (Tuya, 2001) o "magos [...] genios jamás despistados, hermanos traviesos" (Molist, 2003). La tarea de aclarar estas contradicciones se complica aún más cuando los mismos hackers declaran su condena al uso ilícito de los conocimientos informáticos, acuñando términos como "crackers" o "warez" para denominar a los autores de piratería y delincuencia informática y, de esta manera, distanciándose categóricamente de semejantes prácticas.

Si se pretende tener algunas nociones previas fiables de este término y provenientes de la primera fuente, sin duda se debe acudir al *Jargon File* de Eric S. Raymond, documento que se ha convertido en una especie de la "Biblia de los hackers". En él se ofrecen ocho diferentes definiciones, según las cuales, un hacker es:

- Alguien que disfruta explorando los detalles de sistemas y programas y sabe cómo sacarles el máximo provecho, al contrario de los demás usuarios que prefieren aprender sólo un mínimo necesario.
- Alguien que programa con entusiasmo (a veces obsesivamente) o disfruta programando antes que teorizando sobre la programación.
- La persona capaz de apreciar el valor de hackear.
- La persona que es buena programando de forma rápida.
- Un experto en un programa concreto o alguien que frecuentemente al trabajar usa un programa determinado; en este sentido se puede hablar de 'un hacker de UNIX´, por ejemplo [...]

- Un experto o entusiasta de cualquier clase. En este sentido podría hablarse de un hacker astrónomo, por ejemplo.
- Alguien que disfruta con el desafío intelectual de superar las dificultades de forma creativa.
- [definición objetable] Alguien que maliciosamente trata de descubrir información secreta. De ahí que se habla de ´hacker de los password´ y ´hacker de la Red´. El término correcto en este sentido es ´cracker´ (Raymond, 2000).

La definición de Raymond, en primer lugar, descarta categóricamente a cualquier asociación entre el hacker y el delincuente informático y, en segundo lugar, insiste en el entusiasmo con el cual los hacker programan el software. Este entusiasmo fue postulado luego, por otros teóricos (cf. Himanen, 2001), como una manifestación característica de los hackers que describe la relación que habitualmente tienen con su trabajo. Por otro lado, cuando Raymond define a los hackers como programadores de software, se debe precisar que se trata de un tipo específico del mismo, a saber, el software no propietario o el de la fuente abierta.

Los hackers y el software de fuente abierta

Las mayores tensiones surgidas entre el movimiento hacker y los propietarios de software radican en la posición crítica que aquel sostiene frente al consagrado sistema de "copyright" el cual, en la sociedad informacional, se extiende a los derechos del software y permite que los programas de computación tengan propietarios. Esta situación, piensan los hackers, priva al resto del mundo del beneficio potencial que conlleva cada software, convirtiendo a los propietarios en las únicas personas con capacidad de copiarlo y/o modificarlo.

Recordemos que el sistema de copyright nació con la tecnología de la imprenta y mientras fue restrictivo con los copiadores masivos, no impedía que los lectores individuales copiasen sus ejemplares de libros impresos con tinta y pluma, sin afectar por eso, los derechos intelectuales del autor ni los intereses comerciales de la editorial. La aparición de las tecnologías digitales es la causa de que la

copia y la distribución de la información se hagan más flexibles y más fáciles. Precisamente, a causa de esta flexibilidad algunos de los hackers se oponen a que el sistema de copyright sea aplicado también a la información digitalizada.

Richard Stallman (1998), en un artículo muy difundido en la Internet, titulado "Por qué el software no debe tener propietarios" rebate los principales argumentos de los oponentes de la mencionada libertad del software. Denuncia, en primer lugar, los insultos y las exageraciones de los cuales son víctimas quienes abogan por el software abierto: se los llama "piratas" y "ladrones de propiedad intelectual" estableciendo, de esta manera, una identidad simplista y equivocada entre un software y un objeto físico.

Luego, al autor ataca las respectivas legislaciones vigentes calificándolas de perversas y draconianas. Según su opinión, en el caso de software no se puede hablar de "derecho natural" del autor por dos razones: en primer lugar, porque la analogía que se establece entre un programa de computación y un objeto material es muy forzada: cuando se trata de un objeto material cualquiera, sucede que, mientras otra persona se aprovecha de él, disminuye la posibilidad de su aprovechamiento por parte del propietario. Stallman, argumenta que, en el caso de software, la situación es diferente:

> Cuando yo cocino espaguetis, me quejo si otra persona se los come, porque entonces yo ya no me los puedo comer. Su acción me duele exactamente tanto como lo que le beneficia a él; sólo uno de nosotros se puede comer los espaguetis [...] Pero el hecho de que tú ejecutes o modifiques un programa que yo he escrito te afecta a ti directamente y a mí indirectamente. Si tú le das una copia a tu amigo te afecta a ti y a tu amigo mucho más que lo que me afecta a mí. Yo no debería tener el poder de decirte que no hagas estas cosas. Nadie debería (1998).

La segunda razón por la cual resulta impropio hablar del "derecho natural" en el caso del software, se desprende de la

verdadera esencia y el propósito con el cual se estableció el sistema de copyright:

> La idea de los derechos naturales del autor fue propuesta y decididamente rechazada cuando se concibió la Constitución de los EE.UU. Esa es la razón por la cual la Constitución sólo *permite* un sistema de copyright, y no *requiere* uno; por esa razón dice que el copyright debe ser temporal. Establece asimismo que el propósito del copyright es promocionar el progreso -no recompensar a los autores. El copyright recompensa a los autores en cierta medida, y a los editores más, pero se concibe como un medio de modificar su comportamiento (*ibid*.).

Finalmente, Stallman debate el argumento esgrimido con mayor frecuencia por los defensores de la propiedad de software, que es el argumento económico: la existencia de los propietarios de software conlleva a producir más software. El autor reconoce que esto en parte es cierto: la gente producirá más si se les paga bien por ello, pero lo que se incentiva realmente en este caso no es algo que la sociedad realmente necesita. En la producción de cualquier objeto físico no se ve afectada su calidad sólo porque tenga un propietario o no: el bocado, por ejemplo, es igualmente sabroso o nutritivo en ambos casos. Con el software, sin embargo, no sucede lo mismo: permitir la existencia de propietarios del mismo hace que la sociedad se vea privada de que la información esté realmente a disposición de los ciudadanos (o sea que el software se pueda leer, arreglar, adaptar y mejorar, y no solamente ejecutar); se ve privada de la libertad de ejercer el control sobre una parte de sus propias vidas y, finalmente, queda despojada del espíritu de cooperación entre los ciudadanos. Por otro lado, siempre polemizando con el argumento económico, Stallman trae a colación el caso de "La Fundación para el Software Libre", una entidad sin ánimo de lucro y el de los colaboradores que desarrollan el software libre, para demostrar que esta actividad puede generar ganancias, resguardando los derechos intelectuales de los programadores y, al mismo tiempo, no caer en la venta de los programas cerrados. Se establece de esta manera, una diferencia clara

entre el software de fuente cerrada y la comercialización del mismo, diferencia que no siempre está tenida en cuenta hasta por los mismos hackers, tal como se desprende de algunas respuestas del presente estudio que se podrán ver más adelante.

El estilo de trabajo y las motivaciones de los hackers

Uno de los autores, al que le llama la atención la apasionada relación de los hackers con su trabajo es el analista finlandés, Pekka Himanen. Según este autor, las ocupaciones profesionales de los hackers a menudo trascienden las barreras consideradas tradicionalmente laborales y hasta se confunden con los espacios del ocio (2001). Himanen considera que en el pleno de nuestra sociedad informacional se está construyendo una nueva ética del trabajo la cual "desafía la actitud que durante tanto tiempo nos ha tenido esclavizados, a saber, la ética protestante del trabajo, tal como la expuso Max Weber" (2010, p. 11), haciendo referencia al célebre estudio del sociólogo alemán sobre *La ética protestante y el "espíritu" del capitalismo*.

El "espíritu capitalista", para Max Weber, es un tipo de mentalidad relacionado con el ámbito económico y que requiere del individuo una entrega absoluta al trabajo, desafiando, de esta manera, la mentalidad anterior "tradicional" (dentro de la semántica weberiana, esto equivaldría a la mentalidad "medieval" para nosotros), según la cual el hombre trabajaba para vivir y no al revés. El hombre de la mentalidad pre-capitalista, cuando llegaba a acumular alguna riqueza significativa, dejaba de trabajar o al menos lo evitaba, dedicándose a actividades muy diferentes, como la caza, el juego, la diversión y otras que hoy llamaríamos comúnmente, ociosas. La "nueva" mentalidad capitalista obligaba al hombre a vivir para trabajar. El trabajo llegó a tener su propio fin: ganar el dinero. De esta manera, el dinero dejaba de ser un simple medio para satisfacer los fines hedonistas y eudeimonistas del individuo y, en cambio, la obtención del mismo devenía como una obligación moral, un deber absoluto. Todo esto sucedía, según el análisis del sociólogo alemán, precisamente debido a la influencia socializadora de la ética protestante. La frase de San Pablo "quien no trabaja que no coma" adquiría una validez absoluta.

Las pocas ganas de trabajar fueron síntomas de la carencia del estado de gracia (cf. Weber, 2001, p. 202).

Consecuentemente, de acuerdo con la alegoría de Pekka Himanen, la Reforma protestante "desplazó el centro de gravedad de la vida desde el sábado hacia el viernes" (2001, pp. 35-36), elevó el trabajo a lo más importante de la vida del hombre e hizo que hasta el cielo venga representado como un taller (cf. Ibídem). Es precisamente en este punto donde la ética de los hackers deviene como una alternativa para el hombre de la nueva sociedad informacional: los hackers ponen en tela de juicio aquellas virtudes vigentes en la sociedad capitalista respaldadas por la ética protestante y proponen un nuevo estilo de vida y de trabajo. Siguiendo la misma alegoría de Himanen, podríamos decir que, proponen desplazar la vida desde el viernes hacia el domingo.

Como ya se señaló anteriormente, Himanen no está sólo en considerar esta característica del estilo de trabajo de los hackers: en la definición del hacker, anteriormente citada y extraída del *Jargon File* de Eric S. Raymond, a menudo se utilizan conceptos que indican la relación afectiva que el hacker mantiene con su trabajo: se habla de alguien que *disfruta* explorando los detalles... que programa con *entusiasmo*... *disfruta* programando... es un experto o *entusiasta* de cualquier clase... Alguien que *disfruta* con el desafío intelectual..., etc.

Por otro lado, Jorge Machado también nos proporciona un concepto de hacker muy significativo al respecto:

> La palabra hacker aplicada en la computación se refiere a la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía. El hacker es alguien que se apasiona por las computadoras y se dedica a ellas más allá de los límites (2003).

El mismo autor, cuando narra la historia de la Almirante de la Marina Norteamericana Grace Hooper, considerada por algunos como

la primera hacker, indica que cuando ésta "realizaba sus labores en la computadora Mark I**,** durante la Segunda Guerra Mundial, se daba el tiempo para sus investigaciones y experimentos, inclusive fuera del horario de trabajo o hasta en días feriados" (2002).

Este entusiasmo, característico del estilo de trabajo de los hackers, como todo fenómeno social debe ser un producto de algunos determinados incentivos o impulsos motivacionales. De ahí que, los estudios sobre las motivaciones que guían a los hackers a tomar determinadas posturas ocupan un lugar prominente en los intentos por comprender dicho fenómeno. De hecho, Linus Torvalds uno de los principales gurúes de este movimiento, y el que inició el desarrollo del sistema operativo Linux, tan preferido por los hackers, al intentar explicar quiénes son ellos realmente, lo hizo remitiéndose exclusivamente a los aspectos relacionados con la motivación. A propósito, expuso una sencilla teoría motivacional, la cual autodenominó, la Ley de Linus (cf. Torvalds, 2001 en Himanen, 2001, pp. 15-19). Según ella, todos los motivos humanos podrían agruparse en tres categorías básicas, que son la supervivencia, la vida social y el entretenimiento, categorías que se constituyen en fases de un mismo proceso evolutivo (Ibid., pp. 16-17). La teoría en sí no difiere mucho de las clásicas consideraciones de Maslov (1954) que dieron inicio a los estudios científicos sobre la motivación humana y que también siguieron unos criterios parecidos: las necesidades fisiológicas y de seguridad de su famosa "Pirámide" corresponderían a la fase de supervivencia que propone Torvalds. Luego, lo que Maslov llamaba la "necesidad social" y la "estima" podría identificarse con la fase de la "vida social", según la Ley de Linus y finalmente, el "entretenimiento" de la versión del informático finlandés, se relacionaría con la cúspide de la Pirámide de Maslov, es decir, con la autorrealización (claro está, que el entretenimiento no se entiende aquí en un sentido estrecho como diversión y pasatiempo, sino algo mucho más amplio: cualquier intento apasionado por explicar el universo). Finalmente, ambos también consideran que las diferentes categorías motivacionales tienen un carácter jerárquico y progresivo.

Otras teorías actuales sobre la motivación reagrupan aquellos elementos de la Pirámide de Maslov de diferentes maneras. Por ejemplo, Clayton Alderfer (1969) considera que existen tres grupos de necesidades humanas: la existencia, la relación y el crecimiento (teoría conocida como la ERG de las siglas inglesas: Existence - Relatedness – Growth), mientras que para McClelland (1989) estas necesidades son las del logro, el poder y la afiliación. No obstante, todas ellas, incluida la de Linus Torvalds, parecen indicar la insuficiencia del modelo conductista de la motivación, el cual centraba su explicación en el concepto de impulso y otorgaba una excesiva importancia a las necesidades de supervivencia y a todas aquellas que fueran originadas en los estímulos del medio, o sea extrínsecamente. Ahora, sin embargo, se apunta a la existencia de numerosas fuentes de motivación que están al margen de los estímulos e impulsos, y son intrínsecas al individuo. Precisamente, en este punto se coloca el aporte principal del análisis motivacional de los hackers, quienes inician y continúan sus acciones, ejerciendo grandes niveles de esfuerzo para lograr sus metas, impulsados por móviles "superiores":

> Para ellos, la supervivencia no es lo principal [...] Un hacker es una persona que ha dejado de utilizar su ordenador para sobrevivir ("me gano el pan programando") y ha pasado a los dos estadios siguientes. Él (o, en teoría aunque en muy contadas ocasiones, ella) utiliza el ordenador para sus vínculos sociales: el correo electrónico e Internet son las grandes vías para acceder a una comunidad. Pero para un hacker el ordenador es también entretenimiento. No me refiero a los juegos, ni tampoco a las bellas imágenes que circulan por la red. El ordenador mismo es entretenimiento (Torvalds, 2001 en Himanen, 2001, pp. 18-19).

Método

En este estudio ha participado un grupo de 30 hackers de habla hispana de diferentes comunidades españolas y latinoamericanas. Dado el carácter peculiar de estos grupos, la escasez de estudios empíricos previos, como también el hermetismo con el que tiene que

enfrentarse el investigador y la consecuente imposibilidad de establecer, aunque sea aproximadamente, un número fiable de la población, la estrategia de este muestreo es no probabilística y la presente muestra no pretende ser representativa de ningún universo previamente establecido. Por esas mismas razones, el nivel de este estudio es eminentemente descriptivo.

Desde un principio, se procuró mantener también un aspecto cualitativo en el análisis de los resultados. Por esa razón, fue escogida la entrevista libre focalizada como el instrumento para el abordaje empírico del tema. La intención fue contactar con algunos de los hackers y procurar entrevistarlos en línea utilizando los espacios como chats, foros de debates y otros. No obstante, esta intención primaria debió ser abandonada pronto, en vista de la muy escasa respuesta y el nulo interés, por parte de los hackers, en ser entrevistados. Se utilizó entonces la técnica de la "bola de nieve": pude contactar primero con algunos hackers del lugar de mi residencia y conseguir que ellos, a su vez, me comunicaran y recomendaran a sus colegas de otros países. Así pude contactar personalmente con 31 personas de las cuales 30 participaron del presente estudio. Ninguno, sin embargo, estaba dispuesto a realizar las entrevistas en línea, por lo que tuve que optar por enviarles un cuestionario con preguntas abiertas para poder mantener un cierto grado cualitativo de los datos construidos y para que los encuestados tuvieran una mayor libertad para expresar sus opiniones.

Finalmente, los datos en parte fueron analizados con la ayuda de la estadística descriptiva, en concordancia con el carácter de este estudio, ya que en él, no se plantearon hipótesis ni tampoco se correlacionaron las variables estudiadas. Pero, por otro lado, fui ilustrando este análisis con las expresiones más significativas de los encuestados.

Resultados y comentarios

Datos demográficos

Los hackers encuestados en este estudio fueron conformados, en su gran mayoría por los hombres (97%), habiendo solamente una mujer hacker. Por más que en la historia del movimiento hacker algunos autores destacan el rol de quien fuera Almirante de la Marina

Norteamericana durante la Segunda Guerra Mundial, Grace Hooper, desarrolladora del software y creadora del lenguaje de programación COBOL, e independientemente del hecho que en la actualidad uno de los personajes más influyentes en este ámbito es la periodista catalana Merce Molist, no obstante, el mundillo de los hackers es considerado casi exclusivamente como "cosa de hombres" y la presencia femenina en dicho entorno se estima como escasa. Nuestra muestra no va en contra de esta opinión.

Los encuestados provenían principalmente de España (50%). La otra mitad de la muestra se distribuía entre los países latinoamericanos: México (17%), Venezuela (13%), Paraguay (10%) y Argentina (7%) y Perú (3%). La distribución geográfica de los respondientes denota una presencia mayoritaria de los hackers españoles frentes a los de otros de países latinoamericanos. Dado que el estudio no es representativo en cuanto que la muestra no responde a ninguna población previamente determinada, este dato lejos de ser fundamento idóneo para afirmar o concluir algo al respecto, sólo puede llamar la atención a una posible y lógica relación que podría existir entre el grado de desarrollo económico-tecnológico de un país determinado con su respectivo número de hackeractivistas. Esta es una tendencia que se observa también en un otro estudio en el cual, de los 526 encuestados solamente 13 (unos 2,5%) pertenecen a los países latinoamericanos (A Hacker Survey, 2002).

La mayoría de los hackers (40%) tiene entre 21 y 25 años, seguidos por los del rango de entre 16 a 20 (23%), luego aparecen los hackers de entre 31 a 35 años (17%). Los hackers menores de 15 y los comprendidos en el rango de entre 26 a 30 años, conforman los grupos más pequeños de 3 personas cada uno (10% respectivamente). En cuanto a esta variable, puede llamar la atención la presencia de personas muy jóvenes, lo cual induce a plantear la siguiente pregunta: ¿pueden existir hackers de 14, 15 o 16 años? Por más dudas que pueda haber en cuanto a la preparación tecnológica de estas personas o su suficiente conciencia y madurez para poder identificarse plenamente con un movimiento tan complejo, existen sin embargo, al menos dos indicadores que permitirían responder afirmativamente a dicho

planteamiento. El primero consiste en el testimonio de algunos de los encuestados, programadores experimentados quienes se iniciaron en la programación en una edad sorprendentemente corta: por ejemplo, un hacker quien programa ya hace 23 años, afirma haberse iniciado a los 9 años de edad; otro empezó en la misma edad y cuenta actualmente con una experiencia de 10 años de programación. En línea general, existen dentro de la muestra de nuestro estudio, varias personas que afirman tener entre 6 y 23 años de programar y que empezaron haciéndolo a la edad de entre 8 a 13 años.

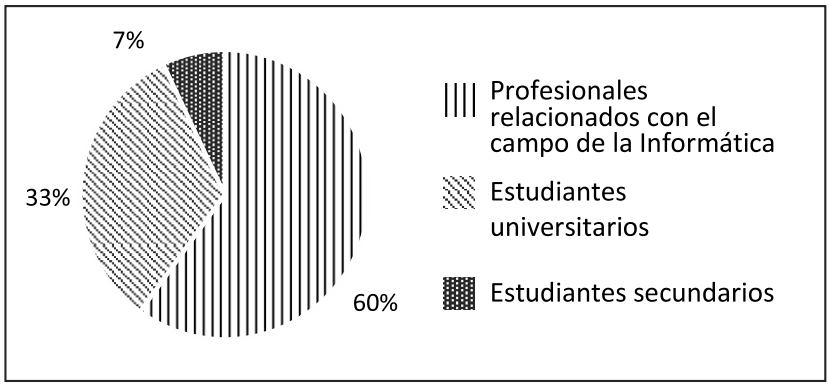
El segundo indicador que permitiría considerar como hackers a algunos adolescentes, es la opinión que al respecto expresan los hacker experimentados. Al ser consultados sobre la posibilidad de la existencia de los compañeros tan jóvenes, en general respondían afirmativamente. Uno de ellos, por ejemplo, acepta esta posibilidad pero agrega que esto sucede "en muy contadas ocasiones; yo, de esa edad y buenos, sólo he conocido a uno, genios a los 15 años hay pocos" (Hacker 01). Otro encuestado también responde positivamente en estos términos: "Si, varios de mis amigos (ahora más grandes) comenzaron a partir de los 14 años (me incluyo). Si bien no había Internet, utilizábamos mucho las BBS's" (Hacker 04). Cada caso es diferente, pero si se tienen en cuenta ciertos matices y algunas salvedades, se podría aceptar, en líneas generales, la existencia de los hackers de una corta edad. Dichas salvedades, expresa en forma elocuente uno de los testimonios:

> Si podrían existir hackers con 13 años de edad es muy relativo. Cuando comenzamos a escribir eDIV, por ponerte mi caso, todos teníamos 13 y 14 años pero no mucha experiencia ni soltura en el manejo de lenguajes de programación: era un auténtico caos, cada uno queríamos hacerlo de una forma distinta y usando una forma de programar diferente. Sin embargo a partir de los 15 la cosa cambiaba, todos sabíamos qué hacer y cómo. Con el paso del tiempo y según la edad vas madurando y pensando de una forma que harás las cosas cada vez mejor. Tenemos, por otra parte, los chicos entre 12-18 años que se creen hackers, sin previo reconocimiento por

> parte de la comunidad y que se autoproclaman como tales al usar un exploit de X bug en Y programa. Son los llamados 'Script Kiddies', simplemente se limitan a usar programas que explotan vulnerabilidades, pero no saben siquiera si lo que han hecho ha sido un desbordamiento de buffer, copiar una cadena en X segmento de memoria o qué; saben que rompen cosas y punto, no les interesa saber el por qué ni el cómo de estas :-). Volviendo al principio, el verdadero 'hacker' se empieza a formar con 15 años, los otros entre 12 y 13 están 'en proceso' (Hacker 22).

Otro encuestado culpa precisamente la existencia de estos hackers adolescentes del cierto sensacionalismo mediático con el que se trata el mundillo hacker: "A los 14 o 15 años, hay un desajuste hormonal tremendo que causa comportamientos poco lógicos, lo que explica la tendencia existente a que estos chavales aparezcan en las noticias" (Hacker 28). No obstante, el mismo no acepta de que esto sea alguna señal de genialidad, más bien cree que con la edad, ellos se vuelven más responsables y "saben distinguir entre el bien y el mal, incluso en la red. Normalmente estos chavales utilizan vulnerabilidades sobradamente conocidas, documentadas y parcheadas".

Figura 1. Características laborales/estudiantiles de la muestra



En primer lugar, resalta el nivel de la preparación educativa superior de la muestra de los hackers, el cual, siendo claramente superior a la media de la población en general, tanto en España como

en Latinoamérica, hace que estos grupos sean mucho más cultos, especialmente en cuanto a la cultura tecnológica se refiere. Por más que muchos expresan opiniones negativas sobre la preparación tecnológica que se imparte en la universidad, casi todos han pasado por ella.

Lo destacable es que todos los encuestados que se encuentran insertos en el mercado laboral manifiestan estar trabajando en áreas directamente relacionadas con la informática. Se encuentran entre ellos: Consultores de sistemas, Consultores de Seguridad Informática, Ingenieros en Telecomunicaciones, Diseñadores y Desarrolladores de Sistemas Automáticos para líneas de producción, Robótica y Acción Artificial, Administradores de Sistemas y otros. Por otro lado, todos los estudiantes universitarios, como era de esperar, cursan carreras que también están directamente relacionadas con la Informática. Hasta los dos de los cuatro hackers más jóvenes que aún están en el colegio, afirman haber seguido algún tipo del colegio técnico con la especialización en computación.

Independientemente del grado de la preparación tecnológica formal, los hackers se caracterizan por un constante esfuerzo de capacitación y actualización. Absolutamente todos confirman que lo hacen frecuentemente: algunos todos los días y otros especifican hasta el número de horas promedio que dedican a este quehacer (5 a 8 horas diarias). En cuanto a la forma de estas actualizaciones, llama la atención que prácticamente nadie considera apropiados para este fin los estudios formales, como la Universidad o el Colegio. En vez de eso, la mayoría se actualiza directamente en la Red a través de los sitios especializados o en forma autodidacta, leyendo manuales y aplicándolos a las tareas diversas, siguiendo de alguna manera una máxima expresada por uno de los encuestados: “en la universidad no te enseñan a ser hacker”. Las maneras de la actualización de los hackers están representadas en la siguiente Tabla.

Tabla 1. Formas, a través de las cuales los hackers actualizan sus conocimientos

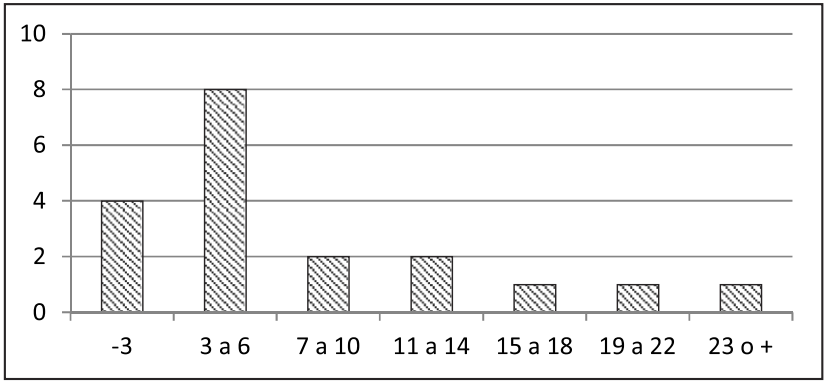
Medio de actualización		Frecuencia
Internet		**26**
	Sitios especializados	15
	Foros, listas de correo, grupos de noticias	9
	Ezines	2
Actividades prácticas		**4**
	Leyendo documentos y probando	2
	Sorteando problemas a medida que aparezcan	2
	Practicando en la mesa de trabajo	1
Libros técnicos		**4**
Revistas técnicas		**1**
Conferencias		**1**

La consideración de la Internet como la manera de la actualización por excelencia es abrumadora, aunque la misma no indica que las otras modalidades sean excluyentes, ya que se puede observar que varios de los encuestados utilizan diferentes maneras de actualización, dejando en claro, sin embargo, su preferencia por la Red.

Todos los encuestados son programadores, aunque no todos se dedican a esta actividad profesionalmente. Solamente dos de los hackers respondieron que no eran programadores, pero luego afirmaron sin embargo, haber utilizado lenguajes como C, C++ y Pearl lo que confirma lo expresado anteriormente. En cierto sentido, nuestra muestra no va en contra de la idea generalizada que se tiene sobre lo que son realmente los hackers. Así, por ejemplo, cuando Eric S. Raymond en la definición citada anteriormente enuncia las ocho características principales de los hackers, la que se relaciona con la programación de software denota una persistencia especial; recordémos que para él, el hacker era alguien que disfrutaba explorando los detalles de sistemas y programas, programaba con entusiasmo y disfrutaba programando, era bueno programando rápido y un experto en un programa concreto, entre otros. De manera que, todos nuestros encuestados responden positivamente a esta asociación: hacker - programador de software, incluyendo también a aquellos que aún son

adolescentes. Lo expresado anteriormente, requiere sin embargo de ciertos matices, ya que en nuestra muestra, la experiencia en la programación es muy variada, tal como se puede observar en la Figura 2.

Figura 2. Años de experiencia con los que cuentan los encuestados en la programación de software



Esto nos da una media de 8,1 y mediana de 7 años de experiencia en la programación, lo cual es considerable aunque quizá, debido a la asimetría de los datos extremos, los cuales varían desde un año hasta 23 años de experiencia, sería más representativa la mediana, o sea, unos 7 años de programación promedio.

Una variable significativa sobre la preparación tecnológica de los hackers, aparte de la experiencia misma en la programación, podría ser el tipo o los tipos de lenguajes que usan con más frecuencia, los lenguajes que recomiendan, los que no recomiendan y las razones por las cuales lo hacen, lo cual se analiza a continuación[1].

[1] Mis agradecimientos, en esta parte del escrito, al Señor Oscar Vayreda, mi compañero del Programa de Doctorado en la Sociedad de la Información y el Conocimiento impartido en la Universitat Oberta de Catalunya, quien me ayudó a interpretar los datos referentes a lenguajes de programación.

Tabla 2. Lenguajes de programación recomendados y menos recomendados por los hackers

Lenguaje	Más recomendado en %	Menos recomendado En %
C	53%	-
C++	43%	-
Pearl	40%	7%
Java, Appletscripts	40%	-
PHP	33%	-
Python	23%	-
ASM (Assembler)	20%	-
Visual Basic	13%	13%
Shell Scripts	13%	-
Bash	10%	-
HTML	7%	-
ASP	3%	3%
CSH	3%	-
Smalltalk	3%	-
Squeak	3%	-
Mysql	3%	-
TCL	3%	-
Ruby	3%	-
.NET	-	7%
Access	-	3%
Delphi	-	3%
Pascal	-	3%
Multiplataforma	-	3%
No responde	-	50%

Siendo el C++ una evolución del lenguaje C, podría decirse que una absoluta mayoría (un 96%) expresa la preferencia por este lenguaje, el cual por lo demás, es un lenguaje mulptiplataforma, es decir que no depende de un sistema operativo determinado. Esto debería interpretarse también como una expresión lógica de los presupuestos libertarios de los hackers. Lo mismo podría decirse cuando se analiza la preferencia de los lenguajes PHP y ASP, respectivamente: siendo la función de ambos básicamente la misma, pues ambos sirven para interpretar las instrucciones de la página web en el

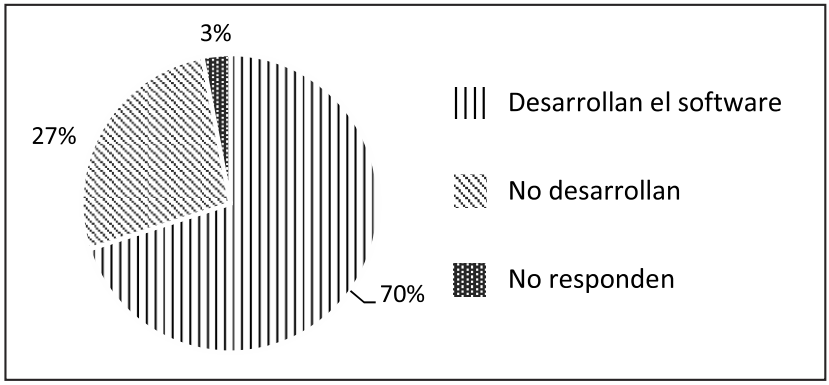
servidor para luego enviarlas al navegador. La preferencia por el primero se debe a que no tiene propietario, mientras que la escasa aceptación del segundo, por ser patrimonio de Microsoft.

Si bien, para recomendar los diferentes lenguajes de programación los hackers tienen bien clara su preferencia personal, no es así cuando se les consulta sobre los lenguajes que consideran poco recomendables: la mitad de los encuestados no responde a esta pregunta dando a entender que cada uno posee algunas ventajas. Entre las respuestas sobre los lenguajes menos recomendados aparecen tres, bastante confusas, hecho que quizá denote poca experiencia de algunos encuestados en el campo de la programación: en primer lugar, Delphi no es precisamente un lenguaje sino un entorno que facilita la programación en el lenguaje Pascal, especialmente en su variante orientada a objetos; en segundo lugar, Access tampoco es un lenguaje sino una base de datos sencilla de Microsoft que funciona sólo en Windows; finalmente, la Multiplataforma lejos de ser un lenguaje específico, es un tipo de lenguaje que habilita al programador a "correr" sus productos en diferentes sistemas operativos.

Los hackers y el software de fuente abierta

Otra actividad en la Red considerada propia de los hackers, en tanto su expresión ideológico-libertaria, es el desarrollo del software de fuente abierta. La Figura 3 demuestra que la mayoría se dedica a esta tarea con frecuencia.

Figura 3. Porcentaje de los hackers que desarrollan o no el software de fuente abierta



De los 21 encuestados que afirman haber desarrollado este tipo de programas, 15 agrega además, haberlo convertido en su principal actividad dentro del hacking (8 de ellos afirman que lo hacen con mucha frecuencia sin especificar detalles y 7 lo hacen diariamente). Los demás encuestados dedican a dicha tarea entre 5 a 30 horas semanales.

El tema del software de fuente abierta tiene también su lado negativo, quizá el más expuesto en los medios masivos de información, y se refiere a emprender acciones en contra de los propietarios de software. Sin embargo, no todos los integrantes de la muestra de las comunidades hackers están directamente en contra del software cerrado y las opiniones expresadas al respecto son muy variadas. Por un lado, están los que directamente no encuentran nada malo en esto y hasta creen que el software comercial, por lo general, es de buena calidad: "para ser objetivo tengo que admitir que en general el software propietario de uso masivo es muy bueno. Es mentira decir que los productos de Microsoft son malos porque no lo son en lo absoluto" (Hacker 01). Otros, aceptan el derecho de su existencia pero lo condicionan diciendo, por ejemplo, que "Debería ser más barato", que "A veces se exagera con las restricciones" o que:

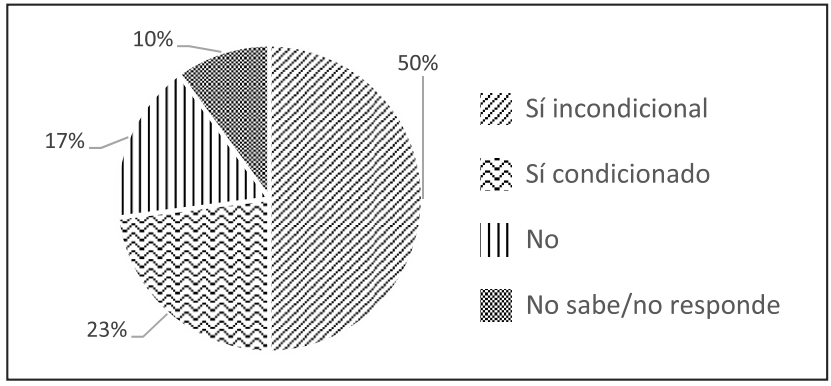
> Es aceptable en los primeros estadíos de vida del producto software (entre 1 y 3 años), luego debe pasar a ser libre para que la comunidad mundial lo enriquezca y lo comparta con todos sin tener en cuenta la escala de ingresos... El problema es

cuando empiezan a surgir monopolios mal intencionados. Esto afecta la competencia y la mejora del software" (Hacker 12).

La opinión de la mayoría, sin embargo, está directamente en contra de este tipo de software. Los argumentos más frecuentes señalan que el mismo se vuelve obsoleto muy rápidamente, que entorpece el desarrollo de la tecnología y que está lleno de bugs (fallos). Algunos creen en su inevitable desaparición e indican lo ilógico de su existencia: "me costaría, pero podría creerlo, que se pague por algo que se cuelga. Ahora bien, lo que no me entra en la cabeza es que se pague esas cantidades por algo que se cuelga existiendo una alternativa mejor y de menor coste" (Hacker 14).

Al ser directamente indagados sobre si el software debería ser libre el acuerdo es casi unánime y está representado en la siguiente Figura.

Figura 4. Opiniones de los hackers sobre si debería ser libre el software



Los que decididamente y sin condicionamientos están a favor del software libre esgrimen una gran variedad de argumentos que podrían ser resumidos en cuatro categorías: (1) *razones didácticas***:** los demás podrán aprender del trabajo de programador, (2) *razones económicas***:** en los países subdesarrollados se podrá investigar sin limitaciones; el software se vuelve más barato para el consumidor final, (3) *razones prácticas***:** la comunidad mundial puede mejorar un

software y adaptarlo a las necesidades específicas; nadie tendrá que empezar a programar desde cero; en caso de fallos la comunidad mundial los elimina rápidamente, y (4) razones éticas**:** la informática es una forma de conocimiento y como tal toda limitación a su acceso en inmoral; es patrimonio de la sociedad.

Por otro lado, las condiciones que algunos encuestados ponen a la existencia del software libre se reducen a las siguientes:

- que se asegure un mínimo de ingresos a las empresas para su futuro y para posibilitar el pago de los trabajadores o que se cobre el servicio de soporte;
- que sean libres, al menos, los sistemas operativos;
- que sea libre, al menos, el software de las oficinas públicas.

Sobre este último caso, una persona argumenta cuanto sigue:

> Al menos debería ser libre todo el software usado en los organismos públicos. No tiene sentido que me den un .doc al bajar una instancia, me están obligando a pagar una licencia de MS Word (o a tenerlo ilegalmente) para poder acceder a esa información. Es como si me obligaran a llevar una marca de zapatillas para entrar en sus oficinas: inadmisible (Hacker 20).

Finalmente, los que están en contra de software libre recurren al único argumento económico-comercial, que es el funcionamiento del mercado y la defensa de los derechos comerciales del programador. No obstante, según lo expuesto en la Introducción del presente estudio, la idea del software libre no es necesariamente incompatible con la comercialización del mismo ni con los derechos intelectuales de los programadores, por lo cual estos argumentos, como también algunos de los condicionamientos expuestos anteriormente, pierden su fuerza argumentativa.

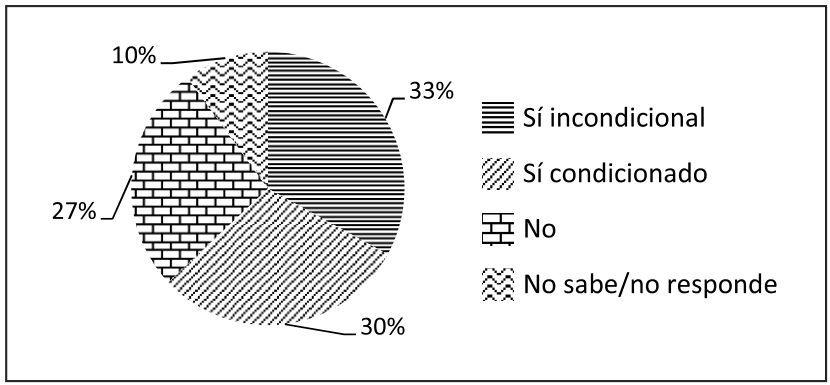
En general, las opiniones sobre Bill Gates y otros propietarios de empresas de software de fuente cerrada son muy desfavorables. Esta forma de pensar es expresada por las dos terceras partes de los

encuestados. Algunas de las acusaciones se formulan de la siguiente manera:

- Muy buen empresario: vendiendo mucho de poca calidad (Hacker 03);
- Frenó la tecnología de software (Hacker 05);
- Ha demostrado su inhumanidad al haber dejado en bancarrota a muchas empresas que disponían de los mejores productos (Hacker 09);
- Oportunista visionario, su filosofía es más o menos si no puedes comprarlo, hackealo (Hacker 11);
- Son especuladores y cobardes, no se ven preparados para competir con la comunidad libre (Hacker 12);
- Capitalista, que por su filosofía económica no va a cambiar a fuente abierta (a no ser que sea negocio :)) (Hacker 14)
- Que son como niños que no entran en razón por mucho que les enseñes que así no prosperarán (Hacker 16);
- Patentar algoritmos, como el de mp3, y luego cobrar royalties por su uso: es como si tuviéramos que pagar a Newton cada vez que usamos la constante G (atracción gravitatoria de la Tierra). Igualmente ridículo es el tema de las patentes de software (y de las patentes en general, muchas veces) (Hacker 20)
- Siento desprecio (Hacker 28).

Al constatar esta actitud tan desfavorable hacia los propietarios de software de fuente cerrada y siguiendo los estereotipos circulantes sobre el mundillo hacker es lógico que surjan las siguientes preguntas: ¿se traduce esta opinión crítica generalizada en algunas actividades directamente dirigidas en contra de los mismos propietarios de software o de sus productos? ¿Sería correcto, para los hackers por ejemplo, apropiarse de estas licencias para darlas a conocer al público y fomentar, de esta manera, su uso gratuito? Las respuestas a esta última pregunta se pueden observar en Figura 5.

Figura 5. Opiniones de los hackers sobre si es correcto utilizar los conocimientos tecnológicos para apropiarse de las licencias del software de fuente cerrada



Los hackers que incondicionalmente asumen la eticidad de estas actividades argumentan que las mismas son tan sólo una respuesta a una situación abusiva ya existente: "Se trata solamente de una respuesta a algo que no debe ser. Como dice la tercera ley del movimiento de Newton, para cada acción hay una reacción. Esa reacción a software comercial no es legal, pero es natural. Es simplemente lo que debe suceder, y por eso es legítimo" dice uno ellos (Hacker 13). Les parece que ésta sería una forma de evitar poner barreras al conocimiento y además una manera de tener el control sobre la tecnología (Hacker 7 y 14, respectivamente).

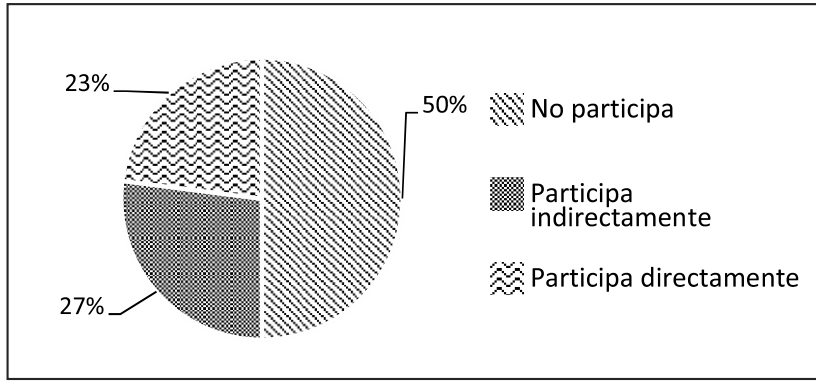
Otros, los que aprueban también estas actividades, las condicionan de diferentes maneras:

- con tal que sea para el uso privado, no comercial;
- cuando los productores de software se "aprovechan demasiado" o cuando los precios son exorbitantes o las empresas abusan de su posición en el mercado;
- en el caso en que las empresas desarrolladoras no ofrecen información sobre sus procesos, formatos, protocolos o algoritmos, o
- mientras no se viole ninguna ley.

Los que no aprueban este tipo de actividades argumentan, generalmente, que las mismas atentarían en contra de los intereses de las empresas, de los programadores y del sistema económico en sí, aunque cabe también un argumento diferente según el cual, la actividad misma carece de sentido debido al bajo nivel tecnológico que implica un software propietario: "Me parece una mierda. Yo no uso software propietario para mis desarrollos, por principio. Además, le compruebo al mundo que puedo desarrollar cosas tremendas sin usar ni un solo pedacito de software propietario" (Hacker 01).

En cuanto a las actividades que en la práctica emprenden nuestros encuestados en contra de los propietarios de software, la muestra se divide en dos partes exactamente iguales (ver la siguiente Figura): mientras que una mitad niega categóricamente haber promovído acción concreta alguna, la otra mitad sí, reconoce haberlas emprendido, por más qué algunos no lo hacen de forma directa.

Figura 6. Participación de los hackers en actividades dirigidas en contra de los propietarios de software



Los que no lo hacen, suelen atribuir estas actividades a los crackers o a otras personas que lo hacen por ellos. En este último caso se percibe cierto grado de aceptación y justificación implícitas de estas acciones aunque se deslindan responsabilidades propias. Y en cuanto a los actúan en este caso, lo hacen de diferentes formas, entre las cuales destaca:

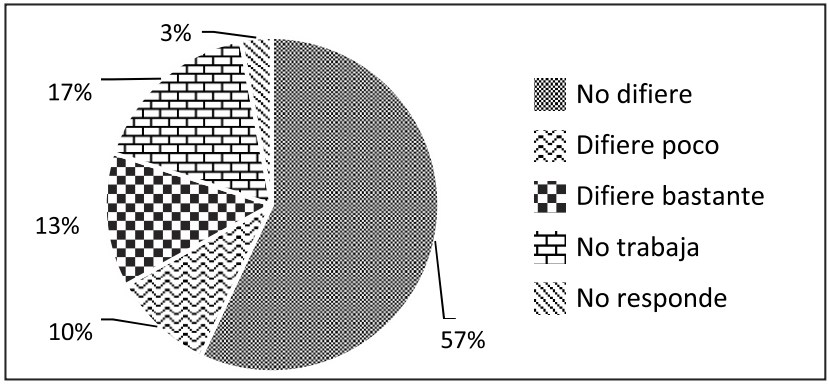
- la recolección de firmas contra las patentes de software, como las que se recabaron para la declaración contra las patentes de software en la Unión Europea;
- la utilización del software criptográfico seguro y de fuente abierta (como GnuPG) protestando, de esta manera, contra el Tratado de Wasenaar[2];
- haciendo abogacía en pro del software libre;
- crackeando los programas propietarios (Hacker 17).

Resultan especialmente interesantes las actividades indirectas, como la creación de modelos económicos y viables de software libre, apoyo a los programas contrarios y/o alternativos a los propietarios de baja calidad, en vez de atacarlos directamente. Algunos consideran que hasta su esfuerzo y afán continuos por aprender lo máximo en el campo de la informática, constituye una forma alternativa de lucha en contra del software propietario (Hacker 12).

La forma de trabajo y las motivaciones

En la muestra de los hackers, llama la atención un alto porcentaje de personas cuyo trabajo remunerado no difiere en nada o difiere poco de sus actividades de hacking las cuales, por lo demás, son su pasatiempo favorito (Ver Figura 7).

Figura 7. Relación entre el trabajo remunerado de los hackers y su hackactivismo.



[2] EE.UU. impide a sus ciudadanos y a empresas exportar software criptográfico fuerte a menos que se proporcione a la Agencia de Seguridad Nacional una puerta trasera para poder romperlo. Programas como GnuPG no están sujetos a estas restricciones.

Si se tuviera en cuenta solamente a los encuestados que poseen algún trabajo remunerado y que no son sólo estudiantes (25 personas) el porcentaje de aquellos cuyo trabajo no difiere de sus actividades preferidas de hacking asciende a 68% y, por más que la presente muestra no pretende ser representativa de ningún universo, el número es sorprendentemente alto en comparación con la visión tradicional sobre el trabajo que fue considerado siempre como una "pesada carga" en la sociedad industrial capitalista. En este sentido, uno podría suscribirse a la tesis de Himanen, según la cual, el estilo de trabajo en la sociedad informacional estaría destinado a romper con las viejas divisiones entre el "trabajo" y el "ocio", entre el "viernes" y el "domingo". He aquí algunas justificaciones de este estado de cosas expresadas por los mismos hackers:

- Mi trabajo no difiere en nada... estoy investigando, desarrollando software y haciendo auditorias de seguridad y todo legalmente y pagándome, ¿¡que más quiero?! Para mí esto es el *carpe diem* de mi vida :) lo que soñé años atrás :) (Hacker 05);
- En ambos ámbitos realizo tareas de investigación, desarrollo e ingeniería inversa (Hacker 04);
- No difieren en nada, trabajo con el mismo ímpetu como hago mis actividades extralaborales (Hacker 06);
- No, en nada... Generalmente en mis ratos libres hago cosas parecidas (Hacker 07);
- Me dedico completamente a mi área específica y de hecho tengo acceso a los recursos del trabajo sin problema (Hacker 18);
- Considero que la mayoría de quienes somos buenos en esto lo somos porque nos gusta, y por tanto nuestras actividades de tiempo libre están muy ligadas a nuestro trabajo. Esto es lo que nos convierte en buenos: amamos lo que hacemos (Hacker 20);
- Básicamente la mayoría de lo que aprendo en mi tiempo libre, acabo aplicándolo de una u otra forma a mi trabajo (Hacker 29);

Si bien no todos corren la misma suerte y hay quienes odian lo que hacen en su trabajo (Hacker 01) el número elevado de los que

dicen lo contrario indica la necesidad de estudios posteriores orientados en esta dirección.

Por último, se indagó a los encuestados acerca de los motivos que los inducen a hacer el hacking. Los resultados de esta pregunta se ven reflejados en la Tabla 3.

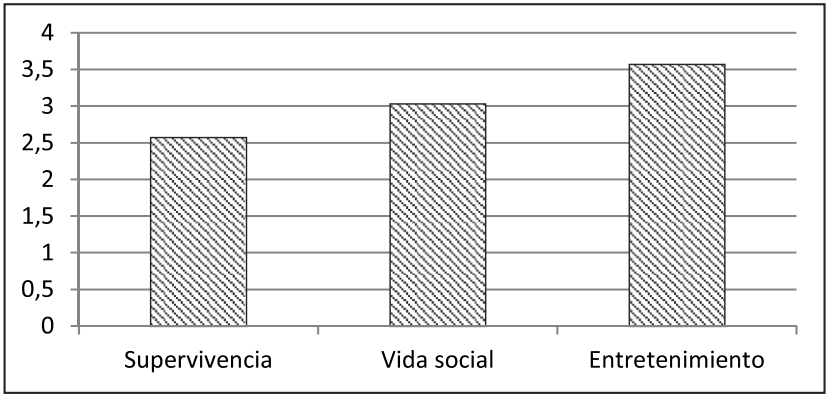
Tabla 3. Motivaciones de los hackers para realizar las actividades del hacking

Reactivo	**Media**
Me estimula intelectualmente	4,80
Simplemente me lo paso bien	4,52
Lo divertido me es útil para mi formación profesional	4,40
Me permite colaborar con el software de fuente abierta	4,04
Me permite luchar por los ideales libertarios	3,56
Me gratifica saber que puedo romper las medidas de seguridad de las grandes corporaciones	3,32
Me ayuda a combatir a los propietarios de software	3,24
Me proporciona un estatus social dentro de la red	3,12
Para mejorar mi situación laboral	3,08
Me divierte el desafío de crackear los programas pagos, aunque luego no las use	2,64
Me proporciona herramientas para violar la seguridad de los sitios web de personas e instituciones odiosas	2,24
Me permite ganar más dinero	2,16
Me permite crackear programas pagos y compartirlos con la gente para que pueda usarlos gratis	2,00
Me permite divertirme creando virus informáticos	1,76
Me permite ahorrar dinero crackeando los programas pagos y usarlos sin licencia	1,76

Estos reactivos aparecían en el cuestionario en orden aleatorio, siendo que cada uno de ellos correspondía a una de las tres categorías de niveles motivacionales propuestos por Linus Torvalds. Siguiendo su "Ley de Linus", podría intentarse la agrupación de los

mismos dentro de estas categorías, cuyo resultado está representado en la Figura que viene a continuación.

Figura 8. Media aritmética de las clases de motivaciones de los hackers ordenadas según las categorías de la "Ley de Linus"



Al menos en la muestra que nos tocó a estudiar, el postulado de Linus Torvalds se cumple perfectamente, ya que denota claramente la prevalencia de las motivaciones "superiores" frente a los básicos, de supervivencia. Y en aquellos de orden superior, es precisamente el entretenimiento el que lleva la punta, superando inclusive a las motivaciones relacionadas con la vida social.

Es digno de resaltar, entonces, el hecho, según el cual nuestros hackers forman parte de aquel feliz y selecto grupo de la sociedad actual cuyo trabajo remunerado difiere muy poco o incluso no difiere de forma alguna, de lo que están acostumbrados hacer en su tiempo de ocio, en este caso, en sus actividades de hacking. De alguna manera, esta privilegiada situación debe relacionarse con sus niveles motivacionales. Efectivamente, tanto Linus Torvalds como los resultados de nuestra encuesta sugieren que los hackers, lejos de guiarse por motivos de supervivencia tienen, en su mayoría, motivaciones de orden "superior". Quedaría solamente por estudiar de qué manera estas dos variables se relacionan: si el hecho de no tener tanto en cuenta los motivos de orden inferior es lo que les ayuda a conseguir trabajo dentro de su área específica (quizá también, aunque sea

indirectamente, el alto grado de competitividad profesional que manifiestan) o más bien, si el hecho de trabajar en lo que les apasiona, aumenta sus niveles motivacionales. Puesto que el fenómeno motivacional de los hackers relacionado con su trabajo y ocio es tan sólo un síntoma del cambio generalizado que está ocurriendo hoy en día dentro de la Sociedad del Conocimiento y la Información, en la cual nos ha tocado vivir, debería apuntarse ahora a la realización de estudios posteriores orientados hacia la obtención de una muestra más representativa de los hackers; una muestra de esta envergadura, proporcionaría un marco referencial que permitiera interpretar mejor este fenómeno tan fascinante y propio de la sociedad actual.

Referencias

A Hacker Survey: Investigating the Dynamics, Motivations, and Practices of Open Source/Free Software Programmers. The Boston Consulting Group. (2002). Recuperado de http://www.osdn.com/bcg/

Alderfer, C.P. (1969). An Empirical Test of a New Theory of Human Needs en *Organizational Behavior and Human Performance*. Mayo de 1969, pp. 142-175.

Himanen, P. (2001). *La ética del hacker y el espíritu de la era de la información*. Barcelona, España: Destino.

Machado, J. (2003). *Hackers, crackers, piratas, phreakers y delincuentes informáticos*. Recuperado de http://www.perantivirus.com/sosvirus/general/hackers.htm

Machado, J. (2002). *Grace Hooper, ¿la primera hacker de la historia de la computación?* Recuperado de http://www.perantivirus.com/sosvirus/hackers/gracehoo.htm

McClelland, D.C. (1989). *Estudio de la motivación humana*. Madrid, España: Narcea.

Molist, M. (2003). *Entrevista* Recuperado de http://ww2.grn.es/merce/molist.htm

Raymond, E.S. (2004). *Jargon File 4.4.8*. Recuperado de http://www.catb.org/~esr/jargon/

Stallman, R. (1998). *Por qué el software no debe tener propietarios*. http://sindominio.net/biblioweb/telematica/why-free.es.html

Tuya, M. (2001). *De hackers, crackers y demás familia*. Recuperado de http://z14.invisionfree.com/Anbu_Studios/index.php?showtopic=37

Weber, M. (2001). *La ética protestante y el "espíritu" del capitalismo*. Madrid, España: Alianza.