A partir de la obra de Stewart, Charles, Smith, Craig, and Denton, Robert E. (1984) Persuasion and Social Movements. Waveland Press: Prospect Heights, Illinois, el autor trata de efectuar un análisis del movimiento social relacionado con las NNTT de la Información y la Comunicación: los denominados hackers, colectivo sobre el que todavía se tiene una imprecisa definición. En este texto se trata de iniciar un estudio del movimiento hacker a la luz del planteamiento teórico de los autores antes citados, como un novísimo movimiento social surgido a finales del siglo XX.

J.R.O, mayo 2001

Introducción al movimiento social Hacker

(Traducción del inglés: Autor desconocido, posiblemente norteamericano)

Desde la introducción del ordenador personal a finales de los 70, la vocación por el *hacking* ha crecido no sólo en amplitud y miembros, sino que también ha cambiado la dinámica de la institución, como resultado del cambio del papel de la tecnología en la sociedad. Por tanto, la imagen publica del "típico" hacker se ha transformado de novato inocuo a tecno-criminal maligno.

Alentado por el sensacionalismo de los medios y los celos colectivos, sus actividades han sido criminalizadas y ahora los hackers están siendo perseguidos por la ley a una escala desproporcionada a la amenaza actual que plantean. Los hackers quieren que sus motivaciones y éticas sean vistas como legitimas, o al menos entendidas, en vez de ser simplemente descritos como tortuosos adolescentes que no tienen nada mejor que hacer que joder cada uno de los ordenadores disponibles.

A pesar de eso, no se han hecho muchas investigaciones sociológicas acerca de los hackers y su cultura. Encuentro esto extraño; la comunidad académica acepta ampliamente el concepto de la "Sociedad de la Información", sin embargo a esta versión futura de sociedad común no se le ha dado su reconocimiento dentro de la disciplina de la sociología. La perspectiva de una sociedad de clase-dual, en la que la población es separada en los rico-informados y los mal-informados, verdaderamente se cualifica como un serio problema social. La comunidad de hackers informáticos, y el importante papel que esta subcultura juega en la Sociedad de la Información, debe así ser estudiada con igual atención.

La mayoría de los estudios disponibles acercan el término desde una de dos perspectivas: una, una perspectiva criminal, empleando teorías desviadas para explicar la formación y organización de la comunidad hacker; dos, un acercamiento civil-libertario que se enfoca en las actuales leyes de crimen informático y como los temidos hackers son privados de sus derechos Constitucionales. (Todos los citados estudios se basan en la ley Constitucional de los Estados Unidos – no se ha hecho aun un estudio amplio similar acerca de los hackers de Canadá.)

Aunque estos acercamientos son esenciales para entender la cultura hacker, debe también ser estudiada desde un número diverso de perspectivas para mostrar correctamente su profundidad y riqueza de contenido. Por ello, este proyecto analizará la subcultura del *hacking* como una forma de colectivo revolucionario organizado, utilizando una teoría de movimientos sociales desarrollada por Stewart, Smith, y Denton (1984). A pesar de sus actividades, esta subcultura juega actualmente un papel vital en la progresión de la tecnología, y también realiza una función reguladora para el control social, protestando, burlando, y sutilmente minando el control estatal y corporativo por medio de los ordenadores y tecnologías relacionadas con los mismos.

Se mostrará que las actividades relativamente inocuas de los hackers son partes de dicha protesta; sin embargo, esto no puede ser "cantado" en público debido a la naturaleza de las actividades, ej., el *hacking* es ampliamente considerado ilegal. Como ocurre con cualquier subcultura revolucionaria, el movimiento hacker es estigmatizado, desacreditado, y perseguido por los medios de comunicación y la cultura corporativa como juvenil, trastornador, y criminal. Y, todo el tiempo, es generalmente malinterpretado. Debido a este problema, es necesario traer la situación del hacker a la atención de sociólogos por medio de un marco teórico; este el propósito primordial de este documento.

Debido a la falta de estudios amplios actuales, este es un proyecto ampliamente exploratorio. Inspeccionando comunicaciones comunes de hackers, los diferentes temas sociales y políticos de sus actividades pueden ser examinados, y formular conclusiones sobre lo que el *hacking* representa para los participantes. Las comunicaciones de hackers en BBSs – bases de transferencia de ficheros y mensajes electrónicos que están conectadas por medio de un ordenador y un módem – son generalmente consideradas "*underground*". Privadas, altamente protegidas, y generalmente de vida corta, estas BBSs son invisibles al público en general, y la mayoría requieren invitaciones privadas. Por tanto ese tipo de comunicados son difíciles de observar y estudiar; se utilizará un canal distinto de comunicados hacker aquí.

Como con cualquier subcultura que ha sido escasamente estudiada, abundan varias definiciones de lo que es un "hacker", y estas definiciones varían de acuerdo con la posición socio-política del grupo o individuo que lo defina. Para los propósitos de este estudio, los hackers son definidos como entusiastas de la informática que tienen un interés ardiente en aprender acerca de los sistemas informáticos y cómo usarlos de formas innovadoras (Denning, 1991:25).

Esta definición, por tanto, no incluye, por ejemplo, a los hackers malignos que deliberadamente rompen sistemas y borran ficheros, sino a esos hackers que exploran sistemas simplemente por el reto intelectual y que no dejan indicios de sus andaduras. Además, hay generalmente malos usos del término, ya que el *underground* informático no sólo esta formado por hackers, sino también por otras clases de entusiastas informáticos – por ejemplo, *phreakers*, piratas de software, y también *carders* (los que hacen un uso ilegal de tarjetas de crédito). Para una completa discusión de la organización y topografía del *underground* informático, mira Meyer, "The Social Organization of the Computer Underground", 1989.

Análisis Literario

Como se ha mencionado antes, la cultura hacker es un fenómeno relativamente nuevo y la mayoría de documentos sobre ella solo han empezado a emerger en los últimos 10 años, comenzando con la publicación en 1984 del trabajo hito de Steven Levy, Hackers: Héroes de la Revolución Informática. Levy examina la evolución de la Ética Hacker, un sexteto de credos que surgieron de las actividades de los hackers "pioneros" de finales de los 50:

- ¡Entrégate siempre al Imperativo de Transmitir! El acceso a ordenadores – y cualquier otra cosa que pueda enseñarte sobre cómo funciona el mundo – debe ser ilimitado y total.
- Toda la información debe ser libre.
- Desconfía de la autoridad – Promueve la descentralización.
- Los hackers deben ser juzgados por su *hacking*, no por criterios falsos como títulos, edad, raza o posición.
- Puedes crear arte y belleza en un ordenador.
- Los ordenadores pueden cambiar tu vida a mejor.

(Levy, 1984)

Este original código ético forma la base política de las actividades de los hackers modernos. Aunque los métodos usados por la comunidad hacker han cambiado en cierto modo a través

del tiempo, las motivaciones principales y la ética se han mantenido igual. Este punto es reiterado en varios estudios y comentarios (Felsenstein, 1992; Meyer, 1989; Sterling, 1992). Hay también mucho soporte a la controversia de que la comunidad hacker es rica en diversidad cultural (Ley, 1984; Hafner y Markoff, 1991; Meyer y Tomas, 1990; Wessels, 1990). Sin embargo, hay disponibles conclusiones contradictorias; hay también esos estudios e informes periodísticos que refuerzan la imagen estereotipada del hacker como un adolescente solitario, desprovisto de habilidades sociales, que es casi siempre mezquino y maligno en sus acciones y que no tiene en absoluto morales ni éticas de ningún tipo. (Forester, 1987; Parker, 1991; Stoll, 1989; Turkle, 1983). *Shows* de televisión "de cultura pop" sensacionalistas como Geraldo y NBC Dateline han presentado episodios sobre hackers; dichos episodios son salvajemente exagerados en sus declaraciones y enmarcan al destacado hacker adolescente como brillantes-pero-tortuosos ladrones que pasan sus días robando información de crédito. Estos últimos trabajos son a menudo mal investigados; sus opiniones y "hechos" no vienen de la observación extensa, el contacto con la diversa comunidad hacker, o las investigaciones sobre las motivaciones que hay detrás de las acciones de los hackers, sino más bien por informes periodísticos y/o encuentros con solo una variedad particular de hacker. El basar todo un enjuiciamiento en los resultados de un segmento de una cultura, en vez de un TODO representativo, conlleva a informes incorrectos y ciertamente no hace ningún bien a la comunidad hacker a la hora de que su lado se entienda.

Informes como estos simplemente perpetúan la imagen popular del solitario criminal informático, sin hacer divisiones cruciales entre los anarquistas y los exploradores, por ejemplo. Si, hay hackers que destruyen ficheros y rompen sistemas intencionadamente, pero ciertamente no conforman la abrumadora mayoría de hackers; son de hecho solo un pequeño porcentaje. Muchos hackers, como es su intención primaria, pasan completamente inadvertidos en los sistemas que eligen *hackear* y no son nunca descubiertos. El no dejar rastros o huellas es de lo más importante para los hackers.

Y en este punto, mucha gente asume que entonces procedemos a copiar todo lo que encontramos y a vaciar el sistema para poder entonces vender la única copia disponible de los datos al mayor postor, preferentemente un agente extranjero o el mayor competidor de la compañía.

No tiene sentido. Estamos sedientos de conocimiento e información, y puedes entonces realmente pensar que vamos a destruir eso que es sagrado para nosotros? Para quitarle la oportunidad a otro de tener éxito al entrar como nosotros hicimos? Para echar mas leña al fuego de una ya terrible reputación y aumentar las posibilidades de ser pillados y así efectivamente arruinar nuestras vidas y carreras? ("Toxic Shock", 1990)

Por esta razón, a menudo es difícil estimar el número de hackers activos en un momento determinado de tiempo (Denning, 1990; Landreth, 1989). No sólo el no dejar huellas en un sistema es un reto intelectual y parte del "*hack*", sino que el dejar un rastro hace más fácil el llevar a las autoridades de las fuerzas de la ley directamente hacia ti – y, más importante, cualquier detección hará que la cuenta de usuario robada por el hacker sea borrada o cambiada por el administrador del sistema.

Por otra parte, los estudios y comentarios desde el punto de vista del hacker están normalmente escritos por miembros actuales o ex-miembros del *underground* informático. Esta "visión de dentro" es más probable que presente una imagen mas equilibrada, del tipo que solo un miembro de la cultura estudiada puede producir. Estos estudios explican las motivaciones principales detrás del *hacking* y como el código ético original es adherido en la comunidad informática moderna.

Publicaciones como Computer Underground Digest y 2600: The Hacker Quarterly pugnan por mostrar una visión equilibrada de los hackers que es tanto académica como bien debatida, en contraste con la normalmente errónea de los medios de comunicación.

Además, la literatura apoya fuertemente la noción de que la cultura hacker contiene un duro elemento de rebelión (Denning, 1990; Hollinger, 1991; Levy, 1984; Meyer y Thomas, 1990; Sterling, 1992). Los grupos hacker recopilan normalmente sus propias noticias y diarios electrónicos, al igual que tópicos de debate en BBSs, muchos de los cuales están estrictamente dedicados a aquellos con inclinaciones rebeldes o anarquistas. Dichas publicaciones electrónicas serán discutidas a fondo en Metodología, e incluirán el conjunto de datos para este proyecto.

Acercamiento Teórico

Como se ha dicho antes, la mayoría de los acercamientos para estudiar a los hackers son o bien criminológicos o civil-libertarios. Este documento empleará teoría de movimientos sociales, para así demostrar la existencia de protesta socio-política dentro de la cultura hacker. Stewart, Smith, y Denton (1984) perfilan los seis requerimientos esenciales para la existencia de un movimiento social:

- Un movimiento social tiene al menos una mínima organización.
- Un movimiento social es un colectivo no institucionalizado.
- Un movimiento social propone u opone un programa para cambiar normas sociales, valores, o ambos.
- Un movimiento social es contrario a un orden establecido.
- Un movimiento social debe ser amplio en alcance.
- La persuasión es la esencia de los movimientos sociales.

A través de la aplicación de este criterio, la subcultura hacker puede claramente ser considerada un movimiento social:

- Organización mínima: la cultura hacker tiene un numero significativo de miembros "seguidores", y un numero de "lideres". Dichos lideres pueden ser "gurús" - expertos en programación que son legendarios por su conocimiento y su útil pericia (Raymond., 1993) - o abiertos miembros de la comunidad, tales como "Emmanuel Goldstein" (editor y redactor de 2600: The Hacker Quarterly). Los hackers a menudo forman pequeños grupos propios, con redes de conexión a otros grupos por varios canales de comunicación; este tipo de organización sirve eficientemente a las necesidades de la comunidad sin la necesidad de una organización única de gran escala.
- Colectivo sin institucionalizar: El movimiento social es siempre un "grupo marginal" y es criticado por no manejar la controversia por los canales y procedimientos normales y adecuados - incluso cuando los canales y procedimientos le son negados al movimiento. El movimiento no tiene virtualmente poderes de recompensa y castigo por encima del reconocimiento personal y la expulsión, y la expulsión casi siempre conlleva a organizaciones competidoras creadas por los exiliados. (Stewart, Smith, y Denton, 1984: 5)
- Los hackers siempre han sido considerados un "grupo marginal", en los colegios (donde los hackers son simples "novatos") y en la sociedad (donde se les etiqueta como "criminales"). No son considerados parte de ninguna institución social. Adicionalmente, se les niega a menudo la opinión personal en los medios de masas, que normalmente aprovechan cualquier oportunidad para desacreditar y minar a los miembros de la comunidad hacker.
- Propone u opone cambios: esto es de lo que va la cultura hacker. Los hackers desean cambiar las actitudes del público masivo hacia la tecnología, y creen por encima de todo que el conocimiento es poder. Si la gente no esta deseando aprender todo lo que puede sobre tecnología, están permitiéndose ser controlados por el Estado y el poder corporativo; luego, sus actividades tanto se oponen a las normas actuales como proponen unas nuevas.

- Contrario a un orden establecido: El enemigo de los hackers son aquellos que tratan de oprimirles todo lo que pueden - el Estado y las grandes corporaciones. El *hacking*, como una forma de protesta socio-política, es por tanto difamado y denunciado en los medios por estas dos instituciones. El innato conocimiento de esto por los hackers se manifiesta en varias formas: en colectivos anarquistas, en acciones *anti-establishment* colectivas (Meyer y Thomas, 1990), y el hecho de que los ordenadores estatales y corporativos son la mayoría de las veces los blancos intencionados de los hackers
- Amplio en alcance: Como se ha mencionado antes, normalmente es difícil estimar el número de hackers operativos actualmente debido a la falta de rastros que dejan en los sistemas. Sin embargo, ha habido varias estimaciones acerca del numero de BBSs sobre hacking operando actualmente - otro análisis difícil por que la mayoría de las BBSs hacker son "*underground*" y los números de teléfono no están disponibles ampliamente - Meyer y Thomas (1990) estiman que actualmente hay unos pocos cientos solo en los Estados Unidos, comparadas con las miles BBSs no *underground*. El hacking es un fenómeno internacional, y sus miembros van mas allá de las líneas étnicas, raciales, de sexo, y vocacionales. Por ejemplo, ha habido muchos informes documentados de extensa actividad hacking en Europa (Hafner y Markoff, 1991; Stoll, 1990).
- Persuasión: El típico movimiento social sin institucionalizar, mínimamente organizado hace uso de pocas formas de recompensa o castigo necesarias bien para coaccionar a la gente a que se una o para mantenerse leal a una causa o para forzar el orden establecido para capitular todas o alguna de sus demandas. ...

La persuasión es penetrante cuando un movimiento trata de ofrecer o negociar algo. Por ejemplo, un movimiento social que decide llegar a un acuerdo debe convencer tanto a los que lo apoyan como a los que se oponen de que es serio, que está operando desde una posición fuerte, y de que tiene algo de valor que cambiar por concesiones. (Stewart, Smith y Denton, 1984: 11)

La persuasión, en este caso, está también presente. Para la primera parte de la definición, la cultura hacker lo cumple ofreciendo un sutil sistema de recompensa o castigo a sus miembros. Por ejemplo, el código ético está duramente impuesto; si un miembro lo burla y deliberadamente borra algunos ficheros, por ejemplo, otros hackers se burlaran de él a cambio. El chivarse, delatar, y el entregar uno a otro a las autoridades no es poco común (Hafner y Markoff, 1991; Sterling, 1992). Esto es hecho primordialmente sin temor y desconfianza de la autoridad y la ley - que si no ofrecen información, serán perseguidos como asociados en el crimen - más que sin rencor a un colega hacker.

Como un chip de ofrecimiento con poderes estatales y corporativos, los hackers dan la explicación de que les están haciendo un favor sacando a la luz agujeros de seguridad en sus sistemas (Denning, 1990; Goldstein, 1990; Hittinger, 1991; Landreth, 1989.) Con las palabras de un hacker:

Un grave problema en el Cyberespacio es la falta de comunicación entre hackers y no-hackers. Las corporaciones tienen derecho a su privacidad, y por ello se sienten amenazadas por la "amenaza" hacker... Si hackers y corporaciones y compañías de seguridad y compañías de Software, etc., superasen sus diferencias se podría hacer mucho. Cambiando "partes y piezas" de conocimiento, los dos grupos opuestos pueden desarrollar juntos avances revolucionarios en informática que beneficiarían a todos. ("The Dark Adept", 1990)

Así, por este modelo de construcción de movimiento social, se puede afirmar que la comunidad hacker de hecho comprende dicho movimiento. Un análisis de datos relevantes apoyara mas adelante esta conclusión.

Datos y Metodología

Este proyecto utiliza un acercamiento etnográfico, usando datos cualitativos y análisis de documento, para estudiar la cultura hacker. Analizando varios documentos electrónicos y comentarios de hackers, se puede encontrar un apoyo a la teoría del *hacking* como un movimiento social, empleando protesta socio-política. Como se ha discutido previamente, las comunicaciones "*underground*" tales como las que se encuentran en BBSs proveen medios más ricos y representativos para estudiar; Las revistas y comentarios de hackers son mayormente representativos de sólo los miembros más conocidos y comentados de la cultura. Sin embargo, hay varios problemas metodológicos propios de recoger información de BBSs. Primeramente, las BBSs hackers están muy bien guardadas, y difíciles para un extraño (incluso para un buen investigador) de acceder. Hay cuestionarios a rellenar para el "nuevo-usuario", y dichos cuestionarios casi siempre incluyen preguntas técnicas, para así comprobar la valía potencial del nuevo usuario (Meyer y Thomas, 1990). Algunas veces al nuevo usuario se le hace un pequeño test, como encontrar el numero de teléfono no listado de cierto ordenador, o se le pide que de cierta información como un nombre de cuenta y un *password* de algún sistema corporativo bien seguro.

Dichos tests sirven como filtros de nuevos miembros potenciales merecedores y no merecedores; es imperativo que los nuevos usuarios sean seleccionados correctamente. Si un operador de sistema (llamados "*sysop*" - el que mantiene las BBSs) no selecciona a los usuarios correctamente, cualquier clase de usuario de ordenador podría ganar acceso - incluso un oficial de policía o agente del gobierno. Es primordial para el *sysop* echar a miembros inadecuados, ya que si el usuario no va a contribuir compartiendo información en la BBS, no hay necesidad de mantenerlos; si todo lo que hacen es llevarse constantemente información o ficheros y no contribuyen con nada igual en valor (son llamados "*sponge*"="esponjas/gorrones"), son ridiculizados y su cuenta es borrada de la BBS.

Segundo, hay una desconfianza innata hacia los nuevos usuarios en la comunidad hacker. Esto está alimentado por el hecho de que oficiales de la policía o agentes del gobierno a menudo tratan de ganar acceso a la BBS bajo falsas pretensiones - y algunos pocos lo consiguen. A cualquiera, descubierto, alegando ser simplemente un amigable reportero o investigador, será instantáneamente echado, y puesto en la lista negra de otras BBSs de hackers - se corre la voz muy rápido. El modo de las comunicaciones entre ordenadores, donde no puedes ver, oír, o hablar físicamente con otra persona, hace fácil el disfrazarse como otra persona.

La gente de las fuerzas de la ley con unos conocimientos técnicos excelentes de informática y algunos conceptos de la cultura *underground* pueden pasar fácilmente como un hacker. Por esta razón, los números de teléfono de las BBSs de hackers están muy bien guardados y no son de distribución pública. Listas de números de otras BBSs de hackers son normalmente mantenidas y están disponibles en dicha BBS; pero estas listas están normalmente anticuadas, debido a que las BBSs son extremadamente volátiles y casi siempre tienen una vida muy corta (Meyer, 1989).

Por estas razones, he decidido emplear como datos *underground* las publicaciones y cartas de hackers en vez de los comunicados de BBSs. Aunque no tan representativas de la diversa comunidad hacker como los datos de BBSs, los análisis de las publicaciones y cartas evitan los problemas intrínsecos en investigación etnográfica, tales como el ganarse la confianza y cooperación de los miembros del *underground* para así obtener acceso a la cultura - que, debido a su justificable naturaleza paranoica, llevaría mucho tiempo. También, esta el problema de ser intrusivo en la cultura.

Es importante evitar el meterse en la forma de funcionar habitual del grupo. Nada hunde más rápidamente un proyecto que el interferir en la manera de pensar y hacer las cosas de un

grupo. Al final, dicha intrusividad cambiara la situación que has venido a estudiar; en el peor de los casos, llevará a tu expulsión. (Northey y Tepperman, 1986: 71)
Utilizando análisis documental, sin embargo, se evitan estos problemas, sin diferencia en la calidad de los datos. Muchos debates apasionantes en BBSs *underground* están resumidos por individuales y son mandados a publicaciones hacker, que (con una habilidad técnica limitada, búsqueda, y acceso a Internet) pueden ser encontradas en varios *sites* de archivos públicos. Están son aún las palabras de hackers, sin embargo no es completamente necesario para este estudio el meterse en la cultura en sí misma como observador.
Como se mencionó, varias publicaciones y *newsletters* de hackers comprenden el conjunto de datos. Cada publicación o *newsletter* esta constituido por artículos, normalmente en un tópico tipo how-to (ej., "Hacking Answering Machines", by Predat0r; "The Improved Carbide Bomb", by The Sentinel), como también comentarios, escritos por varios autores. Como en las BBSs *underground*, las publicaciones y *newsletters* de hackers tienden a brotar y desaparecer en muy poco tiempo, sin explicaciones. Las usadas para este estudio, sin orden en particular, son:

- PHRACK: (Una contracción de las palabras Phreak/Hack) Esta publicación es generalmente reconocida como la publicación electrónica "oficial". (La otra publicación "oficial", 2600: The Hacker Quarterly, esta disponible solo en forma impresa.) Phrack es la publicación hacker más antigua que existe, con su primera publicación en 1985.
- COMPUTER *UNDERGROUND* DIGEST: Conocida como CuD. Esta *newslette*r electrónica semanal tiene tanto artículos académicos como comentarios de miembros de la comunidad *underground*, y comenzó su publicación en Marzo de 1990.
- DIGITAL MURDER: Su primer capitulo es de Octubre de 1991. Una *newsletter* de hacking/phreaking en general.
- FBI (Freaker´s Bureau Incorporated): Newsletter general, que comenzó en Septiembre de 1991.
- HACKERS UNLIMITED: Comenzó en Diciembre de 1989.
- INFORMATIK: La publicación de Información Privilegiada, 1992.
- MAGIK: (Master Anarchists Giving Illicit Knowledge), 1993
- THE NEW FONE EXPRESS: Junio de 1991
- P/HUN:(Phreakers/Hackers *Underground* Network) Una de las más conocidas y duraderas publicaciones, comenzó en 1988.
- NARC:(Nuclear Phreakers/Hackers/Carders) Otra publicación Duradera, comenzó en 1989
- TAP ONLINE: (Technical Assistance Party) Se estableció primero en 1972 como YIPL (Youth International Party Line) por Abbie Hoffman, y poco después cambió su nombre a TAP. Reconocida como la "abuela" de las publicaciones de hackers (Meyer, 1990).
- TPP:(The Propaganda Press) Con apenas un año, y una de las *newsletters* de pasada.
- NIA:(Network Information Access) Otra publicación relativamente nueva, portando el lema "Ignorancia, No Hay Excusa".
- H-NET: Comenzó en Junio de 1990
- LOD/H TECH JOURNALS: Estas son las publicaciones técnicas de LOD/H - el grupo de *élite* de Legión of Doom. Este conjunto de cuatro partes fue sacado en Enero de 1987 como una publicación única.

Estas publicaciones constituyen una rica muestra representativa de la cultura informática *underground*, Los autores de artículos que aparecen en estas publicaciones y *newsletters* son generalmente considerados los hackers más de "*élite*" o con más conocimientos en la cultura,

especialmente aquellos que escriben los artículos del tipo *how-to*. Así, estas publicaciones se pueden considerar bien representativas de las éticas, creencias y valores de la cultura.
Las secciones siguientes proveerán y discutirán datos, sacados de estas publicaciones, apoyando cada una de las seis características de los movimientos sociales descritas por Stewart, Smith, y Denton (1984). Estos seis puntos fueron dados como un marco teórico para este estudio - por favor vuelve a Acercamiento Teórico para recordar este modelo.

Característica #1: Mínima Organización

Gordon Meyer (1989), en "Social Organization of the Computer Underground", provee un completo estudio sobre como los hackers y los miembros del *underground* informático se organizan por medio de BBSs y otros canales ilícitos de comunicación, tales como bases de *voice-mail* corporativas y "puentes" telefónicos. Estos métodos permiten a los hackers compartir información vital como quien ha sido arrestado o buscado, que sistemas se han cerrado, nuevos números que probar, agujeros de seguridad que han sido descubiertos, etc.
Aunque el *hacking* es primordialmente una actividad solitaria, los hackers necesitan conectarse entre si, a través de BBSs y otros canales de comunicación, en grupos para compartir información y técnicas, y también para dar una sensación de comunidad.
Estos grupos normalmente no tienen lideres en sentido real (Meyer, 1989), pero algunos miembros están destinados a saber más que otros, y los veteranos del grupo actúan como "hermanos mayores" y guías para los hackers novatos. Por ejemplo:

Aprendí todo lo que pude todo lo rápido que pude, y después de varios meses de *hacking* intensivo y de "comercio" de información, el *Cracker* dejó de ser un novato. Sabía un montón acerca de *hacking* por entonces, y ya que me gustaba compartir lo que sabía, me gane la reputación de ser uno al que acudir si tenías problemas. ... A medida que la reputación del *Cracker* creció, el responder dichas peticiones se convirtió en una cuestión de orgullo. (Bill Landreth (alias "The Cracker"), 1989: 16)

Además, los hackers se reúnen regularmente en sociedad, o bien en pequeños grupos, o en grandes concentraciones nacionales llamadas "*cons*" (convenciones). Las *cons* son organizadas por grupos de *élite* y tienden a atraer a un buen número de gente.
Las cons presentan a interlocutores invitados, que son casi siempre hackers de *élite* y muy conocidos, y también ocasionalmente académicos o profesionales en el campo de la informática. Una vez planeadas, las *cons* son anunciadas en BBSs underground y a través de publicaciones de hackers. Cada convención tiene un nombre único - la *HoHoCon* en Houston, *SummerCon*, *PumpCon* en *Halloween*, y *DefCon*, por nombrar unas pocas principales. Las convenciones como concentraciones sociales, sin embargo, tienen su propio conjunto de problemas:

Viernes, 30 de Octubre de 1992, comenzó *PumpCon*, en el patio del Marriot, en Greenburgh, Nueva York. Considerándolo todo, aparecieron unos 30 hackers, y lo pasaron muy bien. Al menos hasta la noche del 31 de Octubre, cuando 8 ó 10 miembros de la policía de Greenburgh irrumpieron e hicieron una redada en el Con. Unos pocos hackers que habían estado dando una vuelta en coche mientras ocurría la incursión volvieron unas horas después, y cuando fueron vistos por la policía, fueron inmediatamente llevados a 255 e interrogados. (Estaban cruzando el hall, cuando un poli apareció, y les dijo que pasasen a una habitación.) Los polis les preguntaron si eran hackers, y cuando estos no contestaron, un oficial de policía llegó al bolsillo del abrigo de uno de ellos, y sacó un *auto diales*. Esto por si solo era suficiente para mandar a los tres a la habitación 255, donde el resto de los hackers estaban detenidos para ser interrogados. Mi pregunta es -¿no es eso un poco ilegal? Búsqueda y captura sin una causa probable u orden judicial? Oooops - se me olvidaba - ¡somos HACKERS! Somos TODOS MALOS! Estamos SIEMPRE violando la ley. ¡No tenemos DERECHOS!. ... En una de las habitaciones, había unas dos docenas de revistas informáticas que aparentemente estaban confiscadas, aunque la orden no especificaba que las revistas pudiesen ser cogidas.

Pero, cuando estás cazando HACKERS, supongo que puedes llevarte todo lo que quieras. Después de todo, los hackers son genios malignos, y no tienen los mismos derechos que tienen los criminales NORMALES. (por "Someone")

Característica #2: Colectivo sin Institucionalizar

Los hackers han sido considerados siempre un grupo "marginal" en la sociedad. En los colegios, los hackers son vistos como *"novatos/lerdos*" y "solitarios" sin habilidades sociales (Levy, 1984; Turkle, 1983); en la gran sociedad, son perseguidos por aquellos que están en el poder. En palabras de un hacker:

"Soy un hacker." Si alguna vez le digo eso a alguien, inmediatamente se asumirá que soy maligno, vandálico, ladrón, un pseudo-terrorista que sale para tomar los ordenadores del mundo en beneficio personal o probablemente para cosechar alguna satisfacción morbosa borrando megas y megas de datos valiosos.

"Se me asocia con el *underground* informático." Si alguna vez le digo eso a alguien, habría un flujo destellante de asociaciones estúpidas en la mente de esa persona entre yo y La Mafia, con Saddam Hussein, Siria, Libia, Abu Nidal, y quién sabe qué más.

Casi universalmente, entre la mayoría ignorante, nosotros los hackers somos considerados como gamberros peligrosos cuyo único propósito en la vida es el de causar tanto daño como nos sea posible en el menor tiempo posible al mayor número de gente.

Seguro, hay esos pequeños críos (física y mentalmente) que se hacen llamar "hackers" y que concuerdan con las descripciones de arriba. Hay también gente que se hacen llamar "seres humanos" que violan, asesinan, engañan, mienten y roban cada pocos minutos (o son segundos ahora?). Significa eso que todos los "seres humanos" deberían ir a la cárcel ("Toxic Shock", 1990).

Como con cualquier grupo minoritario, los hackers son juzgados como proscritos, y como resultado de ello los recursos sociales, económicos, y políticos les son abstenidos. El suceso de la redada policial en la convención *PumpCon* (mira más arriba), como también el comentario de arriba, son reflejos del enfado de los hackers por ser constantemente burlados y mirados por encima del hombro como una amenaza despreciable. La cultura hacker definitivamente no es parte de ninguna institución establecida. Sin embargo, los hackers a menudo expresan un deseo de trabajar con una institución establecida, tal como la policía, por propio beneficio (menos oportunidades de ser perseguido) y por el bien del movimiento (los hackers piensan que la policía debería emplear su tiempo y sus recursos en perseguir a los verdaderos criminales informáticos, tales como los malversadores corporativos).

No podemos permitir, NO PERMITIREMOS que esta tiranía continúe! El Gobierno de Los Estados Unidos ha ignorado la voz de la Comunidad Electrónica mucho tiempo! Cuando dijimos al gobierno que lo que estaban haciendo no era correcto, se negaron a escuchar! Cuando formamos grupos de acción políticos para llevar nuestros casos a la corte y ante el Congreso, se nos dijo que estábamos usando pretextos legales para librarnos del crimen!!! Hemos dado a nuestro gobierno, de forma respetuosa y pacifica, mas que razonables peticiones para que se nos libre de nuestra injusticia, pero más que nada la situación ha empeorado!

Las administraciones Gubernamentales usan el crimen informático como un arma en batallas internas con la jurisdicción. Los oficiales del gobierno, que tienen solo un conocimiento mínimo de ciencias informáticas, usan el crimen informático como una herramienta para el éxito laboral. Los diputados electos, que no tienen ni idea de ordenadores, usan las "superautopistas de la información", el crimen informático, y la criptografía para obtener dinero del contribuyente y apoyo del votante! La Comunidad Electrónica, el único grupo que entiende en su totalidad los hechos aquí involucrados, y el único grupo afectado por las decisiones que se toman, ha sido completamente ignorado. ("The White Ninja", 1994)

Característica #3: Propone o se opone al cambio

Aquí, los hackers satisfacen los requisitos de este criterio. Como se ha dicho antes, una ética primordial del hacker es que la información y el conocimiento es poder (Denning, 1990; Landreth, 1989; Levy, 1984). De hecho, el lema de la publicación electrónica de hackers NIA (Network Information Access) es "Ignorancia, No Hay Excusa". Hay una llamada general al público para educarse a sí mismos en el tema de la tecnología, de modo que no sea usada para controlarles:

Como podemos ver, éste no ha sido el caso. El sistema informático ha estado solamente en las manos de grandes negocios y del gobierno. El maravilloso aparato pensado para enriquecer nuestra vida se ha convertido en un arma que deshumaniza a la gente. Para el gobierno y las grandes empresas, la gente no es mas que espacio en el disco, y el gobierno no usa los ordenadores para disponer ayuda para los pobres, sino para controlar mortales armas nucleares. El Americano medio solo puede tener acceso a un pequeño microordenador que tan solo es una fracción de lo que pagan. Las empresas mantienen sus equipos de lujo fuera del alcance de la gente detrás de una pared de acero de valor y burocracia increíblemente alto. Fue por estos asuntos por lo que nació el *hacking*. ("Doctor Crash", 1986)

Muchos, si no todos, de nosotros creemos que la información debería ser intercambiada libremente... Si todo el mundo se mantiene al día sobre las nuevas tecnologías, técnicas, entonces todos se pueden beneficiar... Cuanto más sepamos cada uno, menos errores del pasado repetiremos, mayor base de conocimientos tendremos para los desarrollos futuros. ("Toxic Shock", 1990)

Muchos hackers comparten una visión utópica común - la de una sociedad electrónica donde la información es libre e incontrolada, donde la democracia reina en la "autopista de la información", y la creatividad e ingeniosidad son características veneradas:

Los hackers son necesarios de nuevo. Podemos resolver problemas, terminarlo, y hacerlo divertido. ¡El público general tiene un interés personal en esto! El público tiene interés personal en la privacidad electrónica, en los sistemas personales seguros, y en el e-mail seguro. A medida que todos aprenden más, el encanto y brillo de los misteriosos hackers se desvanecerán. Los profanos están teniendo una idea más clara de lo que esta pasando. ("Johnny Yonderboy", 1990)

Para mayor referencia, ver el trabajo de Steven Levy, Hackers: Heroes of the Computer Underground.

Característica #4: Contrario a un orden establecido

Como se vio en la sección previa, los hackers están enfadados por el modo en que se les encasilla en los medios de comunicación. En este caso, el "orden establecido" incluye a muchos de esos - las autoridades legales, las corporaciones, el gobierno - que tienen un interés innato en mantener a los hackers y a sus mensajes socio-políticos en la estacada.

Este es nuestro mundo ahora... el mundo del electrón y el interruptor, la belleza del baudio. Hacemos uso de un servicio que ya existe sin pagar por lo que podía ser jodidamente barato si no fuese dirigido por glotones capitalistas, y tú nos llamas criminales. Exploramos... y nos llamáis criminales. Buscamos el conocimiento... y nos llamáis criminales. Existimos sin distinciones de piel, sin nacionalidad, sin influencias religiosas...y nos llamáis criminales. Construís bombas atómicas, libráis guerras, asesináis, engañáis, y nos mentís y nos hacéis creer que es por nuestro bien, y seguimos siendo los criminales. Si, soy un criminal. Mi crimen es el de la curiosidad. Mi crimen es el de juzgar a las personas por lo que dicen y piensan, no por su apariencia externa. Mi crimen es el de ser mas listo que tú, algo por lo que jamás me perdonarás. Soy un hacker, y este es mi manifiesto. Podrás detener a éste en concreto, pero no podrás detenernos a todos...después de todo, somos todos parecidos. ("The Mentor", 1986)

Los hackers son muy prolíficos a este tópico, y ciertamente no tienen pelos en la lengua cuando se da la oportunidad de vociferar su ira hacia aquellas instituciones que les oprimen:

Pero, incluso cuando escribo esto, empiezo a darme cuenta de por que somos un grupo de gente tan temido...
Somos incomprendidos por la mayoría...
No puedes entender a alguien que juzga a los demás por lo que dicen, piensan, y hacen, en vez de hacerlo por su apariencia externa o por lo grande que es su salario. No puedes entender a alguien que quiere ser honesto y generoso, en vez de mentir, robar, y engañar.
No puedes entendernos por que somos diferentes. Diferentes en una sociedad donde el conformismo es el estándar demandado. Buscamos alzarnos por encima del resto, y después ayudar a subir a los demás a la misma nueva altura. Tratamos de innovar, de inventar.
Nosotros, seriamente, tratamos de ir donde nadie ha ido antes.
Somos incomprendidos, malinterpretados, desvirtuados.
Todo por que simplemente queremos aprender. Nosotros simplemente queremos aumentar el flujo de información y conocimiento, para que TODOS puedan aprender y beneficiarse. ("Toxic Shock", 1990)
Dicha opresión, sin la apropiada descarga de enfado y frustración, puede llevar a la anarquía - y muchos hackers tienen una inclinación anarquista/rebelde por esta misma razón (Meyer y Thomas, 1990).
Hay una última modalidad de esta guerra contra de los abusadores informáticos. Esta es menos sutil, una modalidad menos electrónica, pero mucho más directa y hace entender el mensaje. Estoy hablando de lo que se llama Anarquía. La anarquía como la conocemos no se refiere al sentido literal de la palabra (sin clases dirigentes), sino al proceso de destruir físicamente edificios y establecimientos gubernamentales. Esta es una parte muy drástica, y vital de esta "tecnorrevolución". ("Doctor Crash", 1986)
Muchos boletines y publicaciones anarquistas comenzaron su circulación en 1989 y 1990, que fueron los años del comienzo de masivas medidas drásticas contra los hackers en los Estados Unidos. Las casas de hackers sospechosos fueron asaltadas, equipos confiscados (y hasta el momento, muchos no se han devuelto), y varias acusaciones impuestas.
Varios procesos de alta reseña fueron llevados a audiencia, tales como el de *"Knight Lightning*". Una de las redadas mas paranoicamente alimentadas fue llevada a cabo en Steve Jackson Games, una compañía que producía juegos de rol de simulación. El libro que acompañaba a uno de estos juegos, GURPS Cyberpunk, fue reprendido por las autoridades legales como "un manual para el crimen informático" (Sterling, 1992: 142). Para una completa discusión acerca de estas redadas acompañadas de los follones legales a que los hackers se tuvieron que enfrentar, consulta The Hacker Crackdown de Bruce Sterling (1992). Estos arrestos y juicios fueron también controlados de cerca por la Electronic Freedom Foundation, un grupo de presión que se fundo como respuesta a estas medidas de presión. Varios comentarios, respuestas, y manifiestos de ira referentes a estas redadas son también publicados regularmente en The Computer Underground Digest (CuD).

Característica #5: Amplio en alcance

Como se ha mencionado, la cultura hacker no es única de Norte América; muchos hackers en otros países han sido igualmente perseguidos y acosados por los medios. El caso mas conocido de esto es de los hackers de Europa. Un grupo, el Chaos Computer Club, tiene miembros en Francia y Alemania. Holanda tiene su propio grupo destacado, HACK-TIC. Estos grupos, al igual que otros de alrededor de Europa, se reúnen cada año para la conferencia anual del Chaos Computer Club en Alemania.
Contrariamente a su nombre, el CCC esta bien organizado, publica sus actas de las conferencias anuales, y es generalmente considerado una base de recursos para otros hackers Europeos. El más famoso de los hackers Alemanes es Markus Hess, cuyas exploraciones de larga distancia en los sistemas americanos fueron documentadas por Cliff Stoll, en su libro The Cukoo´s Egg de 1989. Otro ejemplo de organización a gran escala son

las convenciones de hackers en los Estados Unidos. También, el numero de BBSs hacker solo en los Estados Unidos, que afirmamos anteriormente que estaban alrededor de unos pocos cientos, son un testamento a la amplia escala de este fenómeno.
Los hackers mantienen que hay otros iguales que todos ellos alrededor del mundo, y cuando se dan cuenta de que son intelectual y mentalmente diferentes que la mayoría de la demás gente, es como una revelación.
Y entonces ocurrió... una puerta abierta al mundo... pasando velozmente por la línea telefónica como heroína por las venas de un adicto, un pulso electrónico es enviado, se divisa un refugio a las incompetencias del día a día... una BBS es encontrada.
"Esto es... aquí es donde pertenezco... “Conozco a todo el mundo aquí.... incluso si nunca me he encontrado con ellos, hablado con ellos, o nunca mas vuelva a oír de ellos... os conozco a todos...
Soy un hacker, y este es mi manifiesto. Puedes parar a éste en concreto, pero no puedes pararnos a todos.... después de todo, somos todos parecidos. ("The Mentor", 1986)

Característica #6: Persuasión

Como se ha discutido antes en Acercamiento Teórico, la cultura hacker a menudo emplea la recompensa y el castigo para mantener su grupo unido. Los hackers que desafían las éticas y valores del *underground* son castigados, y se corre rápidamente la voz del ofensor y su acto a través de la red social.
Por ejemplo, en Out of the Inner Circle, de Bill Landreth (alias "The Cracker") se documenta el desarrollo del Inner Circle, un grupo de hackers de elite que el ayudo a crear. El Inner Circle tenía tradiciones similares a la Ética del Hacker, y dichas reglas estaban estrictamente impuestas:
El hecho de que tratamos de invitar solo a aquellas personas que reunían esos dos requisitos resulto rápidamente en un "código ético" que fue, y sigue siendo, la filosofía que mantuvo al Inner Circle unido. ....Tenemos muchas buenas razones para seguir estas reglas básicas. Pero lo mas importante, por lo que al *Inner Circle* se refería, tenía que ver con el principio básico del respeto a la propiedad e información de otra gente. Éramos exploradores, no espías, y para nosotros, el dañar archivos de ordenadores era no sólo chabacano y poco elegante - era incorrecto. (Landreth, 1989: 18)
Algunos hackers creen que ha llegado la hora - que aquellos que están en el poder están finalmente deseando escucharles:
¿Cuán lejos debe llegar el gobierno para proteger a las compañías y sus datos? ¿Cuáles son exactamente las responsabilidades de una compañía con datos sensibles y de valor en sus sistemas informáticos? Hay una clara sensación de que las compañías del sector privado deberían hacer mas para protegerse. Los hackers pueden dar un punto de vista importante acerca de estos temas, y de pronto hay gente deseando escuchar. ("Johnny Yonderboy", 1990)
Otros se hacen activistas, y un hacker busca activamente el sector corporativo enviando artículos técnicos de seguridad al Computer Underground Digest, una publicación que es ampliamente leída por ambos: hackers y profesionales informáticos:
....Espero romper esta barrera de resentimiento cruzando las líneas del *underground* al mundo "real" y dando información de valor sobre sistemas, seguridad, *interfacing*, etc. Espero que otros sigan el ejemplo, y que el sector privado sea recíproco permitiendo que la información técnica fluya por el *underground*. Finalmente, espero que haya una armonía entre los hackers y los miembros del sector privado para que podamos aprender unos de otros y hacer el mejor uso posible del más grande de los inventos, el ordenador. ("The Dark Adept", 1990)
Aplastantemente, parece que la visión de The Dark Adept no se ha hecho realidad todavía. Los hackers siguen siendo atacados y condenados bajo nuevas leyes de crimen informático que en el mejor de los casos son imprecisas, e inapropiadas constitucionalmente en el peor

de los casos. Esta cultura ampliamente incomprendida está extendiendo su mano a la industria corporativa, ofreciéndose a compartir sus conocimientos y habilidades para crear una mejor tecnología para todos.
Sin embargo, la cultura corporativa rechaza constantemente este ofrecimiento. Experimentos preliminares han sido hechos en los Estados Unidos, haciendo contrataciones de hackers por parte de compañías para comprobar sus sistemas, y los resultados han sido abrumadoramente positivos (Denning, 1990). ¿Por qué, entonces, no se adopta esta práctica ampliamente? Una discusión de las implicaciones de esto, incluyendo relaciones de poder y control económico-político, podría fácilmente comprender otra tesis; por esta razón, no se ahondará aquí.

Conclusiones y Sumario

En este documento, se ha explorado la concepción del fenómeno del *hacking* informático como un movimiento social. Trabajando con un modelo teórico sobre movimientos sociales desarrollado por Stewart, Smith, y Denton (1984), varios documentos sobre hackers han apoyado la idea de la existencia de una colectividad social. Como la cultura hacker es relativamente nueva y esta asombrosamente poco estudiada, estas conclusiones se pueden tomar como preliminares. Espero que este estudio haya asentado una base para posteriores estudios sociológicos sobre el underground informático.
Como la proliferación de tendencias hacker anarquistas sugiere, esta cultura necesita desesperadamente alguna comprensión, así como un oído amigable. Hemos visto que la industria corporativa rechaza los conocimientos y habilidades técnicas de los hackers; ¿no se podría hacer realidad un mayor nivel tecnológico si estas dos partes trabajasen juntas? La respuesta a esto se encontrará en el futuro. A medida que la posibilidad de una Sociedad de Información global se ve más cercana, la gente debe estar deseando traerse a sus manos su educación técnica. Todos podemos aprender una valiosa lección de los hackers: que el apetito intelectual y la búsqueda del conocimiento debe ser central en nuestra sociedad.
La llegada de la Sociedad de la Información ha sido anunciada por académicos y no-académicos del mismo modo. La noción de una sociedad electrónica libre y democrática ha sido advertida como una especie de utopía, donde la información fluye sin trabas y la libertad de expresión es esencial. Sin embargo, hay igualmente un lado oscuro en esto. Cada vez más la información se esta haciendo privada, y mucha gente teme que la Sociedad de la Información sea en realidad una especie de sociedad tipo Orwelliano de “1984”- en vez de eso: Hay algo que no está bien en la Sociedad de la Información. Hay algo mal en la idea de que la "información" es una comodidad como una silla o un escritorio....El conocimiento es poder. El crecimiento de las redes informáticas, de la Sociedad de la Información, está haciendo cosas raras y desbaratadas a los procesos por los que el poder y el conocimiento están actualmente distribuidos.
No creo que la democracia prospere en un entorno donde imperios vastos de datos son encriptados, restringidos, apropiados, confidenciales*, top secret*, y sensibles. Yo temo por la estabilidad de una sociedad que construye castillos de arena a partir de bits de datos e intenta parar una corriente global con regios mandatos. (Sterling, 1992)
El debate continúa; podemos sentarnos, esperar pacientemente, y ver cómo resulta todo; o podemos actuar, autoeducarnos y educar a cada uno, y estar preparados para lo que venga. Terminaré este proyecto con una apropiada cita de un hacker:
Si necesitas un manual sobre cómo llevar a cabo cualquiera de los métodos arriba expuestos, lee un fichero acerca de ello por favor. Y sea lo que sea lo que hagas, continúa la lucha. Lo sepas o no, si eres un hacker, eres un revolucionario. ("Doctor Crash", 1986)

Bibliografía

- Doctor Crash (1986) "The Techno Revolution". Phrack 1:6, 10 Junio, 1986.

- Sterling, Bruce (1992) "A Statement of Principle". Computer Underground Digest 4:47, 30 Septiembre, 1992.
- Denning, Dorothy (1990) Concerning Hackers Who Break Into Computer Systems. In Proceedings of the 13th National Computer Security Conference, October 1990.
- The Dark Adept (1990) "The Ultimate Interface: Hackers and the Private Sector". Computer Underground Digest 2:9, October 23, 1990.
- Johnny Yonderboy (1990) "A Hacker's Perspective". Computer Underground Digest 1:13, June 12, 1990.
- Landreth, Bill (1989) Inside the Inner Circle. Microsoft Press: Redmond, WA.
- The Mentor (1986) "The Conscience of a Hacker". Phrack 1:7, January 8, 1986.
- Stoll, Cliff (1989) The Cuckoo's Egg. Simon and Schuster: New York.
- Sterling, Bruce (1992) The Hacker Crackdown. Bantam: New York.
- Meyer, Gordon and Thomas, Jim (1990) "The Baudy World of the Byte Bandit: a Postmodernist Interpretation of the Computer Underground". Forthcoming in F. Schmalleger (ed.), Computers in Criminal Justice, Wyndham Hall: Bristol, Indiana.
- Toxic Shock (1990) "Another View of Hacking: The Evil that Hackers Do". Computer Underground Digest 2:6, October 6, 1990.
- Levy, Steven (1984) Hackers; Heroes of the Computer Revolution. Dell: New York.
- The White Ninja (1994) "A Declaration of Complaints and Grievances of the United States Electronic Community". Phrack 5:45, File 6/28, March 30, 1994.
- Turkle, Sherry (1984) The Second Self: Computers and the Human Spirit. Simon and Schuster: New York.
- Someone who has been there but wishes to remain anonymous (1992) "A Bird's-Eye View of the PumpCon Problem". Computer Underground Digest 4:60, November 22, 1992.
- Meyer, Gordon (1989) The Social Organization of the Computer Underground. Unpublished Master's Thesis, University of Northern Illinois.
- Stewart, Charles, Smith, Craig, and Denton, Robert E. (1984) Persuasion and Social Movements. Waveland Press: Prospect Heights, Illinois.
- Hafner, Katie and Markoff, John (1991) Cyberpunk : Outlaws and Hackers on the Computer Frontier. Simon and Schuster: New York.
- Wessells, Michael (1990) Computer, Self, and Society. Prentice Hall: Englewood Cliffs, NJ.
- Northey, Margot and Tepperman, Lorne (1986) Making Sense in the Social Sciences. Oxford University Press: Toronto.

  Parker, Donn (1991) "Response to Dorothy Denning", in The United States vs. Craig Neidorf: A Debate on Electronic Publishing, Constitutional Rights and Hacking. Communications of the ACM 34:3, March 1991, p. 34.