

VIII Jornadas Nacionales de Investigadores en Comunicación. Intervenciones en el campo de la comunicación: un debate sobre la construcción de horizontalidades. Facultad de Periodismo y Comunicación Social, La Plata, 2004.

La criminalización discursiva de los hackers en los medios de prensa.

Pablo Gustavo Rodriguez.

Cita:

Pablo Gustavo Rodriguez (Septiembre, 2004). *La criminalización discursiva de los hackers en los medios de prensa. VIII Jornadas Nacionales de Investigadores en Comunicación. Intervenciones en el campo de la comunicación: un debate sobre la construcción de horizontalidades. Facultad de Periodismo y Comunicación Social, La Plata.*

Dirección estable: <https://www.aacademica.org/pablo.gustavo.rodriguez/55>

ARK: <https://n2t.net/ark:/13683/pymh/g6q>



Esta obra está bajo una licencia de Creative Commons.
Para ver una copia de esta licencia, visite
<https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>.

Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite: <https://www.aacademica.org>.

La criminalización discursiva de los hackers en los medios de prensa.¹

Nombre y Apellido: Pablo Gustavo Rodriguez

E-mail: <mailto:pablo.g.rodriguez@argentina.com>

Institución a la que pertenece: Fac. de Ciencias. Naturales, Universidad Nacional de La Plata

Área de Interés: Comunicación e identidades o Discursos, lenguajes, textos

Palabras claves (3 - tres): Estereotipos, discurso, hackers.

Resumen: El análisis crítico de discurso de las notas periodísticas publicadas sobre los hackers, entre los años 1997 y 2000 en las ediciones electrónicas de los diarios argentinos en Internet revela la existencia de un proceso de criminalización de este grupo por los medios de prensa, mediante el uso de estrategias discursivas características del habla racista y la construcción de un esquema de grupo fuertemente negativo y un modelo situacional que asocia a los hackers a la comisión de delitos mediante el uso de computadoras.

Objetivos y metodología.

El presente trabajo forma parte de una investigación en curso desarrollada en el marco de mi proyecto de tesis de doctorado que lleva por título "Una etnografía del Hackerdom en Argentina", bajo la dirección de la dra. Virginia Ceirano, y la co-dirección de la dra. Marta Maffia, en la U.N.L.P.

El objetivo de este estudio es caracterizar la construcción discursiva acerca de los "hackers" en los medios de comunicación social argentinos. Para alcanzarlo se buscaron todas las notas periodísticas publicadas sobre los hackers, entre los años 1997 y 2000 en las ediciones electrónicas de los diarios argentinos en Internet cuya edición en papel es de circulación nacional. Así se constituyó un corpus integrado por 107 documentos que fueron analizados con apoyo del programa NUD*IST©.

El marco metodológico es el análisis crítico del discurso (ACD), en particular los aportes cognitivos de Teun van Dijk respecto de la expresión discursiva de las ideologías y los modelos situacionales y esquemas grupales.

El ACD considera al discurso como una forma de acción social, atravesada por relaciones de poder y realizando una labor ideológica en la que construye a la sociedad y a la cultura a la vez que es constituido por ellas. Por lo tanto el ACD procura realizar un trabajo interpretativo y

¹ Presentada en las "VIII Jornadas Nacionales de Investigadores en Comunicación. Intervenciones en el campo de la comunicación: un debate sobre la construcción de horizontalidades". La Plata. 16 al 18 de Septiembre de 2004.

explicativo de los problemas sociales a través del discurso (Norman Fairclough y Ruth Wodak En: van Dijk, Teun A 2000: 367 - 400). Asimismo van Dijk ha realizado una descripción muy esclarecedora de las macroestructuras y las superestructuras del discurso periodístico que hemos tenido en cuenta (van Dijk T. A. 1978, 1980) y tanto él como varios otros analistas e investigadores que siguen esta línea, han conducido estudios sobre el discurso racista en los medios de comunicación europeos (van Dijk T. A.1997, 2000) que revelan paralelismos interesantes con nuestros hallazgos sobre la construcción de un estereotipo del "hacker" en los medios argentinos.

Optar por el ACD implica aceptar que:

1. La aproximación del análisis del discurso focaliza un problema social, no un problema exclusivamente lingüístico.
2. Las relaciones de poder son elementos discursivos.
3. El discurso constituye a la sociedad y a la cultura así como es constituido por ellas.
4. El discurso realiza una labor ideológica.
5. El discurso es histórico. Todo discurso remite siempre a otros discursos contemporáneos y producidos con anterioridad.
6. El vínculo entre el texto y la sociedad está mediado por la cognición.
7. El discurso es una forma de acción social.

Definición del problema

Comencemos entonces por definir el problema. Muchos autores consideran que la sociedad industrial ha finalizado para dar paso a un nuevo tipo de sociedad que denominan alternativamente "posindustrial", "posmoderna" (B. Sarlo), o incluso "poscapitalista" (P. Drucker). También "sociedad de la información", o "sociedad digital" (N. Negroponte). Se afirma que esta surge como producto de un fenómeno denominado "tercera revolución industrial", "tercera ola" (Alvin Tofler), "revolución científica y técnica", "revolución digital" (Tapscott²) que ha inaugurado una nueva era llamada caracterizada como "la era de la información" (M. Castells) en la cual el conocimiento es el capital más importante y en la que los bits son más importantes que los átomos.

Tres procesos históricos interrelacionados serían característicos de la nueva sociedad:

"a) Una revolución tecnológica, principalmente basada en las tecnologías de la información tan trascendental, al menos, como las dos revoluciones industriales que se basaron en el descubrimiento de nuevas fuentes de energía.

² "La primera década del siglo XXI traerá cambios de largo alcance y grandes transformaciones en la economía, la política, la educación, el entretenimiento, la sociedad y la situación geopolítica"

"A primera vista, afirmaciones de este tipo parecen excesivas. Sin embargo, no es exagerado decir que estamos presenciando los primeros y turbulentos días de una revolución tan importante como cualquier otra en la historia." (Tapscott, 1998:13)

b) la formación de una economía global que representa la estructuración de todos los procesos económicos a nivel planetario...

c) la aparición de una nueva forma de producción y gestión económica: aquella que (...) nosotros llamamos informacional. Está caracterizada por el hecho de que la productividad y la competitividad se basan en forma creciente en la generación de nuevos conocimientos y en el acceso al procesamiento de la información adecuada." (Albornoz, 1998: 21).

Algunos sujetos sociales han contribuido más que otros a estos cambios. Sin duda el desarrollo de la informática, de las redes de computadoras en general y de Internet en particular han contribuido en forma significativa, y el movimiento "hacker" ha sido por casi 40 años el principal impulsor de estos desarrollos técnicos. La masividad que adquirió en los últimos diez años fue posible a partir de que el comercio y la industria del entretenimiento descubrieron que lo que en un principio fue una red militar y luego una red académica podía convertirse en una fuente de ingresos. En este contexto también se fue popularizando la existencia de los hackers. Sin embargo la noción de qué es y qué hace un hacker ha ido cambiando a medida que se popularizaba. Actualmente casi la única fuente de información acerca de este movimiento son los medios masivos de comunicación. Y lo que éstos informan acerca de los hackers está muy lejos del concepto original de programadores prodigiosos.

El "Hacker's Dictionary" (Raymond, 1999), la mayor obra colectiva y anónima de este movimiento, actualizada permanentemente, y reconocida como la recopilación más precisa y completa del vocabulario de este grupo, recoge las siguientes acepciones del vocablo "hacker":

:hacker: n. [originally, someone who makes furniture with an axe] 1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. 2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. 3. A person capable of appreciating {hack value}. 4. A person who is good at programming quickly. 5. An expert at a particular program, or one who frequently does work using it or on it; as in 'a Unix hacker'. (Definitions 1 through 5 are correlated, and people who fit them congregate.) 6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example. 7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

Sin embargo, ninguna de ellas es fácil de hallar en los medios masivos en todo el mundo, quienes, en cambio suelen preferir ésta última:

8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence password hacker', 'network hacker'. The correct term for this sense is {cracker}.

¿Qué concepto de “hacker” usa la prensa argentina?. ¿Por qué la última acepción, precisamente la menos adecuada, ha logrado tanta difusión?

Esquema de grupo

"... propondremos que las ideologías, como otras representaciones sociales, pueden tener una organización esquemática estándar que consiste en un número limitado de categorías fijas [...] tales como identidad/membresía, actividades, metas, normas y valores, posición social y recursos (van Dijk, 1995a, 1995b)." (van Dijk, 1996b:20, ver la Ilustración 1- Categorías del Esquema de grupo).

“Los miembros del grupo tienen un *autoesquema* sobre el propio grupo y esquemas sobre otros grupos sociales o étnicos. Esta es también la manera en que pueden representarse los estereotipos y los prejuicios grupales. Estos esquemas pueden pensarse como información general sobre las características distintivas básicas del grupo (la apariencia, la posición social, etc.), así como sobre sus normas, valores, objetivos e intereses compartidos. Los esquemas personales y grupales explican cómo perciben e interpretan los miembros de un grupo las acciones de otros y cómo se almacena esta información” (van Dijk, 1980 :158-159).

Si bien van Dijk en 1980 desarrolla principalmente el “autoesquema de grupo”, más tarde acepta que los grupos sociales también construyen esquemas sobre los otros grupos, cuya información, en forma análoga a la del autoesquema, podría responder a las siguientes preguntas:

¿quiénes son **ellos**?, ¿cómo son?, ¿quienes (no) pertenecen a **ellos**?

¿Qué hacen **ellos**? ¿Cuáles son **sus** actividades? ¿Qué se espera de **ellos**?

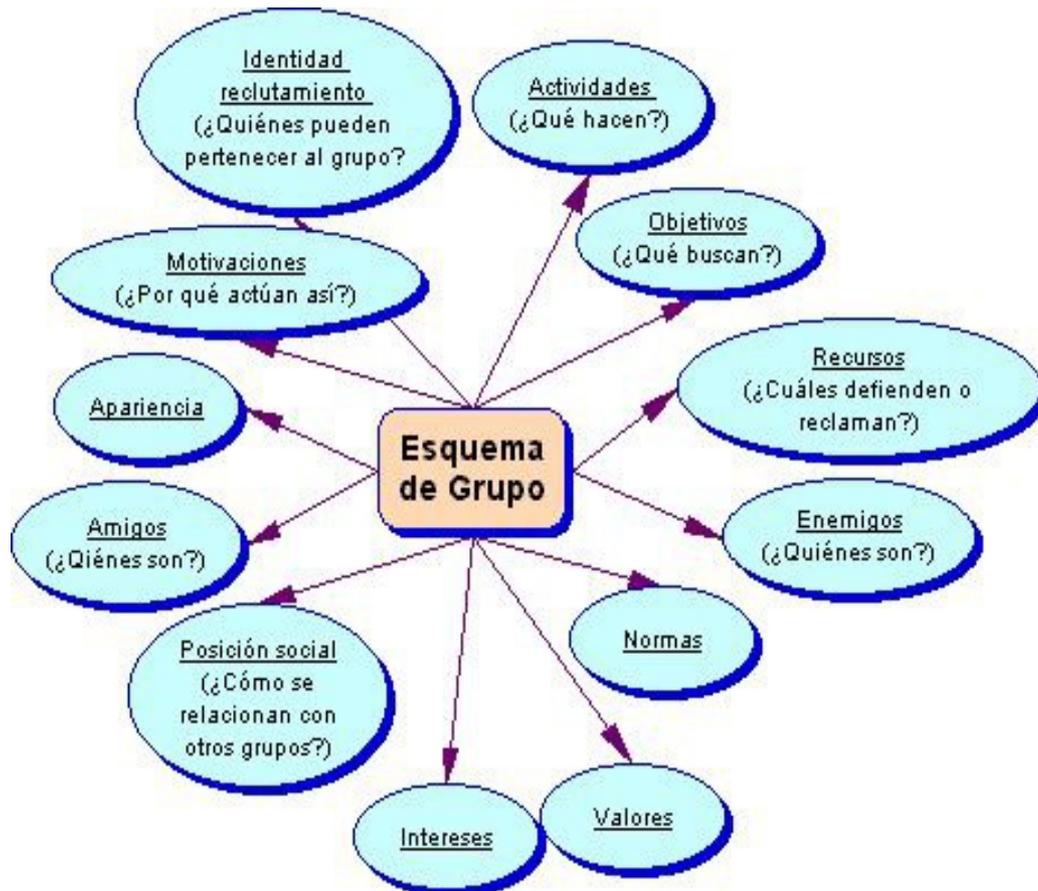
¿cuáles son las motivaciones de estas actividades?

¿Qué normas y valores respetan en tales actividades?

¿Con qué **grupos** están relacionados: quiénes son **sus** amigos y quiénes **sus** enemigos?

¿Cuáles son los recursos a los que típicamente tienen o no acceso (privilegiado)? (van Dijk, 1996b:28).

Ilustración 1- Categorías del Esquema de grupo



“Los esquemas de la memoria caracterizan a las personas con quienes interactuamos y las situaciones sociales en que participamos. Estos esquemas nos proporcionan *estereotipos* sociales, conocimiento sobre las personas y situaciones típicas que esperamos encontrar (...). Pero a pesar del hecho de que la gente real no encaja bien en las clasificaciones simples estereotipadas (...) nuestros modelos del mundo y de las demás personas parecen gobernar nuestras expectativas y nuestras percepciones, aunque las categorizaciones simplifiquen en exceso, aunque en muchos casos sean erróneas.” (Lindsay y Norman, 1983: 702-704).

Los estereotipos y prototipos son sumamente útiles en nuestra vida cotidiana a pesar de que muchas veces resulten erróneos. Ahorran tiempo de procesamiento, permitiendo responder rápida y eficazmente a los acontecimientos. Así ha sido reconocido por los psicólogos cognitivos y por interaccionistas simbólicos como Berger y Luckman, quienes prefieren hablar de “tipificación”.

Los estereotipos se adquieren durante la socialización y no requieren conocimiento de primera mano. Eso los convierte en verdaderos pre-juicios.

“Un problema de los estereotipos sobre la gente es que, una vez aplicados, son difíciles de compulsar y corregir. (...) Debido a que las expectativas guían tan prestamente la percepción y la interpretación y debido a que las motivaciones de la conducta son generalmente ambiguas, los

estereotipos preexistentes sobre los individuos pueden inducirnos automáticamente a percibir esos rasgos, incluso cuando en realidad no están presentes.

“Si el individuo o grupo es valorado positivamente, estos problemas pueden no ser serios. Sin embargo, surgen dificultades si el prototipo del caso es valorado negativamente, como ocurre con los prejuicios o el racismo” (Lindsay y Norman, 1983:705. El énfasis es mío).

En términos generales la estrategia básica del discurso sobre los otros es la combinación de una autopresentación positiva y una heteropresentación negativa, es decir el grupo al cual el enunciador pertenece, su “grupo de pertenencia” o *ingroup* es presentado en términos elogiosos, destacando sus virtudes y minimizando sus defectos e, inversamente, el grupo de “los otros” o *outgroup* se describe en términos críticos, peyorativos, destacando lo que a los ojos del grupo de pertenencia del enunciador tienen de cuestionable o indeseable y minimizando sus rasgos positivos.

En Psicología cognitiva esto recibe el nombre de Teoría de la atribución. El modo como una persona se comporta depende tanto de la situación como de las características particulares de esa persona. Esencialmente la conducta puede reconocer dos causas: la situación y la persona. Las causas debidas a la situación se llaman *situacionales, condicionales, externas o extrínsecas*. Las causas debidas a la persona se llaman *rasgos de personalidad, disposicionales, internas o intrínsecas*.

“Es típico suponer que la conducta de los demás es principalmente causada por factores personales, rasgos o valores perdurables, en vez de los aspectos específicos de la situación misma (...). Las personas hacen atribuciones casi automáticamente sobre las causas de la conducta. Pero la atribución de causas a un acontecimiento singular es arriesgada. Lleva a errores”.

“Es bastante interesante que las personas tiendan a atribuir su propia conducta buena a sus propias personalidades virtuosas, y su mala conducta a la situación. Pero tienden a atribuir la mala conducta de las demás personas a esas personas. En parte vemos que las auto observaciones de una persona sufren una carencia de amplitud y de distanciamiento de la situación. Al fin y al cabo, cuando perdemos los estribos o nos enfadamos percibimos que el acontecimiento es directamente responsable. Pero cuando observamos que se enfada otra persona en sucesos similares -o, lo que es más importante, otra persona se enfada con nosotros (...), tendemos a censurar a la otra persona.” (Lindsay y Norman, 1983:708, 711)

En su artículo de 1996b, van Dijk identifica una serie de estrategias de presentación de ellos y nosotros que puede resumirse en el siguiente cuadro:

Tabla 1 Estrategias de presentación nosotros/ellos

Descripción/atribución de acción positiva	
Grupo de pertenencia (ingroup)	Grupos ajenos (outgroup)
• Énfasis	• Sin énfasis

<ul style="list-style-type: none"> • Aserción • Hipérbole • Topicalización <ul style="list-style-type: none"> ➤ oracional (micro) ➤ textual (macro) • Alta, posición prominente • Poner en encabezado, resumir • Descripción detallada • Atribución a la personalidad • Explícito • Directo • Ilustración narrativa • Soporte argumentativo • Control sobre la imagen 	<ul style="list-style-type: none"> • Denegación (disclaimer) • Subestimación • De-topicalización • Baja, posición no prominente • Marginación • Vaguedad, descripción general • Atribución al contexto • Implícito • Indirecto • Sin narración • Sin soporte argumentativo • Sin control sobre la imagen
Grupos ajenos (outgroup)	Grupo de pertenencia (ingroup)
<i>Descripción/atribución de acción negativa</i>	

La lista anterior se aplica a las diferentes niveles y dimensiones del texto y el habla (niveles fonológico, gramatical, semántico y pragmático y dimensiones estilística y retórica) generando estructuras particulares características. En este trabajo, debido a las limitaciones de espacio y de competencia del autor, nos limitaremos a los aspectos léxicos y a algunas estrategias discursivas relacionadas así como a sus implicancias cognitivas para la construcción de esquemas de grupo y modelos situacionales sobre los hackers.

1. Lexicalización negativa. ¿Quiénes son los hackers?. ¿Cómo los designan los diarios?

Aparte del mismo vocablo "hacker", utilizado en 98 de los 107 documentos analizados, los lexemas con los que se designa a los hackers, en orden de frecuencia son:

Nodo	Concepto	Docs.
(2 2 1)	Piratas, piratas informáticos, piratas cibernéticos, ciberpiratas. NOTA: Cabe recordar que la definición del diccionario de pirata incluye el concepto de ladrón ("ladrón que roba en el mar"), así como el de "clandestino" y "sujeto cruel y despiadado".	67

(2 2 3)	cibercriminales, delincuentes cibernéticos, delincuentes tecnológicos	13
(2 2 2)	terroristas cibernéticos	7
(2 2 5)	vándalos informáticos	3
(2 2 4)	CiberRobin Hoods	1
(2 2 6)	alimañas informáticas	1
(2 2 7)	programadores	1
(2 2 8)	nueva guerrilla	1
(2 2 9)	diablos cibernéticos	1
(2 2 10)	saboteadores informáticos	1

Como puede apreciarse, todos ellos, con la sola excepción de "programadores" tienen connotaciones negativas.

2. Topicalización negativa: ¿Qué tipo de acciones de los hackers salen en los diarios?. ¿Qué dicen los diarios que hace un hacker?

Lo siguiente es un listado de las acciones que las notas periodísticas atribuyen a los hackers, también por orden de frecuencia de mayor a menor.

Nodo	Nombre y definición	Docs.
(2 3 9)	atacar, agredir, dañar; computadoras, redes, sistemas.	53
(2 3 8)	ingreso o penetración ilegal o no permitida en computadoras, redes o sistemas informáticos.	48
(2 3 2)	robar (dinero, tarjetas de crédito, códigos o información)	34
(2 3 1)	invadir o violar sistemas (computadoras o redes)	22
(2 3 3)	Falsificar, modificar o alterar datos o información.	19
(2 3 12)	provocar pérdidas económicas o gastos de dinero a terceros	17
(2 3 17)	realizar espionaje, espiar, fisgonear, curiosear, acceder a información ajena confidencial.	16
(2 3 31)	bloquear sitios web	14
(2 3 20)	destruir sistemas o información	14
(2 3 23)	hacer daño	9
(2 3 4)	demostrar la vulnerabilidad de los sistemas	9
(2 3 29)	atacar a usuarios comunes	8
(2 3 11)	realizar sabotajes	7
(2 3 13)	desestabilizar a las grandes empresas	7
(2 3 32)	expresar consignas políticas	7
(2 3 6)	cometer fraudes	6

(2 3 10)	estafar	6
(2 3 27)	ordenar o intentar ordenar acciones militares	6
(2 3 16)	crear programas dañinos	5
(2 3 22)	tomar venganza	5
(2 3 21)	extorsionar	3
(2 3 7)	delinquir	2
(2 3 18)	realizar una guerra informática	2
(2 3 19)	engañar	2
(2 3 33)	control remoto de computadoras	2
(2 3 5)	bloquear centrales telefónicas	1
(2 3 15)	piratear software y venderlo	1
(2 3 24)	trabajar a sueldo para criminales	1
(2 3 25)	burlarse de Bill Clinton	1
(2 3 26)	crackear	1
(2 3 28)	llamar la atención mediática	1
(2 3 30)	traficar con información robada	1
(2 3 34)	crear virus	1
(2 3 35)	efectuar escuchas telefónicas	1
(2 3 50)	Legales: Actividades permitidas por la ley, no delictivas y no dañinas.	25

Las actividades "Legales" (Actividades permitidas por la ley, no delictivas y no dañinas) que se les atribuyen son las siguientes:

Nodo	Nombre y definición	Docs.
(2 3 50 13)	Consultor privado en seguridad informática.	13
(2 3 50 11)	Colaborar con las autoridades, con la policía o el gobierno para detener a otros hackers o mejorar la seguridad de los sistemas informáticos.	10
(2 3 50 6)	Contribuir a defender o incrementar la seguridad, inviolabilidad o invulnerabilidad de los sistemas informáticos.	6
(2 3 50 1)	Evitar que otros hackers ingresen a los sistemas.	4
(2 3 50 2)	Encargados de la seguridad, Contratados por empresas u organismos estatales como auditores o como responsables de la seguridad de sus sistemas.	4
(2 3 50 3)	Dirigir organismos o fundaciones	2
(2 3 50 12)	Evitar la fuga de datos	2
(2 3 50 4)	Realizar Congresos	1

(2 3 50 5)	Defensa de privacidad	1
(2 3 50 7)	Detectar los puntos vulnerables de un sistema	1
(2 3 50 8)	Solidarias (crear páginas web para org. de DDHH)	1

Como vemos, la gran mayoría de las actividades atribuidas a los hackers son delictivas. Menos de un 25% de los documentos hacen alguna referencia a la realización de actividades no delictivas, y aún éstos no constituyen una reivindicación de los hackers sino que estas actividades legales son presentadas como una rareza, como algo fuera de la norma, o como un indicio de que los sujetos que las realizan han "sentado cabeza" y se han "pasado al bando contrario" abandonando el hacking, o sea que son realizadas por "ex-hackers".

Además de definirlos por la realización de acciones a las que se señalan como delitos, a pesar de que no están legalmente prohibidas ni penalizadas, y además de referirse a ellos como cibercriminales y ciberdelincuentes y de señalar entre sus actividades el robo de dinero y de información se criminaliza a los hackers utilizando un vocabulario policial o militar para describir sus actividades y la respuesta a ellas por la policía.

Uso de vocabulario militar:

Por ejemplo, al describir las actividades de los hackers se las refiere como "ataques masivos", "ataques coordinados", "el golpe más audaz de toda su historia", "invasiones cibernéticas", "atentados", "una nueva forma de guerrilla". Para restar importancia a los ataques de denegación de servicio sufridos en febrero del 2000 a varios sitios de comercio electrónico el entonces pte. de los EEUU, Bill Clinton dijo que no eran "un Pearl Harbor electrónico".

A ellos se los identifica como "el enemigo" y como "un ejército subterráneo relacionado con los anarquistas que se enfurecieron tan espectacularmente con la Organización Mundial de Comercio en Seattle". Se los considera un "riesgo" o "amenaza para la seguridad nacional". Cuando un sistema resulta infectado por un virus se dice que "cayó en las garras del enemigo".

Las computadoras que utilizan son denominadas "plataforma de ataque" o "engranajes de un arma". Las ciudades donde viven o las empresas donde trabajan son llamadas su "centro de operaciones". Las computadoras que atacan son denominadas "blancos", "objetivos" o "víctimas".

Sus "ataques" son considerados como un problema de seguridad nacional que motiva "reuniones cumbre" del presidente de los EEUU, con asesores en seguridad nacional con miras a definir "estrategias de defensa", "declarar una ofensiva", "dar batalla" o "declararles la guerra".:

"La Agencia de Defensa Nacional comenzara la construcción de un sofisticado sistema de seguridad para prevenir las invasiones cibernéticas" (CD_De Japón hasta Perú...UT2)

"Pero la fuerte ofensiva del gobierno norteamericano parece no atemorizar a los piratas de la red, que AYER VOLVIERON A ATACAR" (CD_El FBI dice que los hackers... UT11)

Dichos "ataques" consisten en "el BOMBARDEO DE GRAN CANTIDAD DE INFORMACIÓN". SUS "armas" son troyanos, gusanos, cookies y computadoras.

Los programas y medidas de seguridad informática como los firewalls y antivirus son llamados "artillería contra los hackers".

Uso de vocabulario policial o penal

Frecuentemente se habla de los hackers en la prensa en relación a procesos judiciales o persecuciones policiales, por lo que abunda en estos casos el vocabulario policial, reforzando su imagen de delincuentes aún cuando no se los llame así abiertamente.

Por ejemplo se dice que "dieron un golpe" o se los menciona perseguidos por la policía, o el FBI, en procesos judiciales, con causas pendientes, en libertad condicional, prófugos de la justicia, siendo interrogados por la policía, recibiendo condenas de prisión, pagando fianzas o multas, siendo condenados a realizar servicios comunitarios, a tomar cursos de ética, o a verse privados del uso de computadoras.

A pesar de que reiteradamente se menciona al hacking como un delito en ocasiones se aclara que legalmente no está tipificado como tal y que por lo tanto la única manera de encarcelar a un hacker es esperar a que cometa algún otro delito tipificado, como robo de tarjetas de crédito, de líneas telefónicas, de dinero, fraude, estafa, extorsión, falsificación de información o privar a terceros de su derecho de acceso a la información.

3. ¿Por qué lo hacen? (Motivaciones atribuidas y declaradas)

Las motivaciones declaradas por los individuos citados como hackers o especialistas son las siguientes:

- No es para ganar dinero.
- No es para impedir las ganancias de las empresas.
- La intención es hacer una demostración de poder.
- Demostrar lo inseguros que son los sitios de comercio electrónico.
- Es por el desafío de vencer los sistemas de seguridad informáticos supuestamente inviolables. Para ver si son capaces de superar las vallas que un experto en seguridad informática puso.
- Satisfacer la curiosidad.
- Aprender cosas nuevas.

- Buscar la vulnerabilidad de los sistemas de computación "no para aprovecharse de ellos, sino para señalarles a los expertos en seguridad informática los flancos débiles, para que puedan arreglarlos".
- Descubrir fallas en Internet con la intención de prevenir al público.

Las motivaciones atribuidas por los autores de las notas son:

- Por diversión. "Su desafío es vencer sistemas de seguridad informáticos supuestamente inviolables, y divertirse espionando, alterando o destruyendo DATOS DE ACCESO RESTRINGIDO".
- Cobrar venganza por las investigaciones que lleva a cabo el FBI sobre los hackers o contra un antiguo empleador.
- Como un juego.
- Ver hasta qué punto llegan sus habilidades.
- Demostrar que no existe un sistema infalible.
- Un deporte de moda.
- Lucrar con la venta de información robada en sus accesos no autorizados.

Adicionalmente, en la nota "CZ_Guerra desde los teclados" se presentan tres hipótesis, sin abogar por ninguna de ellas en forma especial:

- Se trata de unos jóvenes fascinados por desplegar su anónimo poder, hoy seguramente muertos de risa
- Una versión aggiornada de los luddistas, esos antiindustrialistas que rompían las máquinas
- Un ensayo general y a gran escala de gangsterismo y guerra comercial

En este punto es importante observar el uso que se hace de las comillas y de diversos mecanismos para establecer distancia enunciativa y descalificar las opiniones que no se comparten. Más abajo describiré más en detalle estas estrategias.

4. ¿A quiénes atacan? (Blancos, enemigos)

(2 3 9 1) Los hackers son noticia por atacar los sistemas informáticos de Bancos, tarjetas de crédito, aerolíneas, grandes empresas (Yahoo!, Amazon, Excite, E-Bay, CNN, eTrade y Buy.com.), sitios del gobierno (Pentágono, CIA, FBI, Dto. de Defensa de los EEUU, ejército, marina y Fuerza Aérea, ministerios, Senado, Casa Blanca, Centro Nacional de Protección de la Infraestructura, NASA), ediciones electrónicas de los diarios más importantes del mundo y proveedores de Internet.

Por otra parte con frecuencia se señala que éstos son los "blancos" preferidos por los hackers. Sin embargo las notas también sugieren que pueden atacar a cualquier usuario. Incluso un

artículo que comienza afirmando explícitamente que es altamente improbable que la PC de un usuario común resulte atacada por hackers dedica todo el resto de su espacio a alertar a esos usuarios sobre las diferentes formas en que su sistema podría ser atacado y recomienda protegerse usando antivirus y firewalls. Esta nota lleva por título precisamente "Cómo defenderse de los hackers". Los títulos de las otras notas que sostienen que "cualquier PC" puede ser atacada por los hackers son:

"Hábitos que cuidan"; "Tengo un hacker en mi teléfono celular" ; "Un atento centinela contra virus y hackers"; "A prueba de hackers"; "Espionaje.com"; "Peligro en el disco rígido" y "Según un hacker, es como enfrentarse a un Goliat".

Estructuras y estrategias discursivas del habla racista

Entre estructuras y estrategias discursivas implicadas en la descripción ideológicamente construida de los hackers hemos hallado la mayoría de las que menciona van Dijk en (1996b:36-39) y algunas más, que describimos a continuación (Todas la definiciones de las estrategias están tomadas del mencionado texto de van Dijk):

a) Hipérbole: "La descripción de un acontecimiento o acción en términos muy exagerados".

"Pero Serial Killer no es su verdadero nick, aunque ilustra bastante bien un tipo de comportamiento compulsivo que le hizo verter sangre de computadoras hace un par de años. Doscientas o trescientas víctimas borradas a cero." (LN_Peligro en el disco rígido, UT:56)

b) Móvil de compasión: "El mostrar simpatía o afinidad hacia víctimas (débiles) de las acciones de los **otros**, de tal modo que se resalta la brutalidad del **otro**".

"Los "piratas" han encontrado un medio estupendo para conseguir su objetivo SIN CORRER PELIGRO. Así, crece el "robo de identidades" o la recopilación de datos personales de los usuarios, incluidas sus cuentas bancarias y sus tarjetas de crédito. La víctima no se da cuenta de lo que está ocurriendo hasta que el hacker comienza a usar esa información para concretar CUALQUIER TRANSACCIÓN A SU FAVOR. Maureen Mitchel, una enfermera de Ohio, sufrió el robo de sus documentos de identidad y, además de haber PERDIDO TODOS SUS AHORROS, tuvo que dedicar más de 400 horas de su tiempo haciendo gestiones en los bancos para que le volvieran a conceder un crédito." (CD_Un hacker buscado por el FBI, UT:13-15)

c) La comparación negativa: "Para acentuar los atributos negativos del **otro** se compara a la persona-objeto o al *outgroup* con una persona o con un *outgroup* reconocidos generalmente como "malos"."

"Cuando fue fiscal de estado en Illinois, y después, cuando entró a la policía de investigaciones, le tocó lidiar contra temibles delincuentes de acción: secuestradores, asaltantes de bancos, traficantes de droga. Hoy, Andrew Black, agente especial de la oficina del FBI de San Francisco,

vive detrás de una especie absolutamente distinta. Es cazador de piratas informáticos, esos personajes de fin de siglo contra quienes goza disputar "apasionantes partidas de ajedrez". (CD_Fue de los mejores, UT:1).

"Pero anoche todavía no había sospechosos. "Es como encontrar una aguja en un pajar", admitieron funcionarios del FBI, que también siguen la pista del terrorismo internacional, "porque podría ser una manera de golpear a los Estados Unidos". (CD_Lanzan una fuerte ofensiva, UT:9)

d) Concretización. "Para acentuar sus actos negativos, otro motivo bien conocido es describirlos en detalle, y en términos concretos, visualizables."

"El navegante pasea plácidamente por la Web, pero inesperadamente la pantalla cambia de imagen y el lector de CD-ROM se abre y se cierra en forma incontrolada. La escena no pertenece a una película de terror, se trata sólo de la vivencia de un internauta que tiene UN INTRUSO EN SU DISCO RÍGIDO. Sin demasiado esfuerzo, HACKERS, CRACKERS, LAMERS y otras variedades de PIRATAS INFORMÁTICOS pueden entrar en la compu a través de Internet y CONTROLARLA A SU ANTOJO." (CI2_0 Cómo defenderse, UT:1).

"La casa de Spock queda en algún lugar del conurbano. Es más de la medianoche y por las paredes de la habitación de techo alto chorrea un disco de Pink Floyd. Ahí está Spock. Acaba de meterse en la máquina de un usuario que dice llamarse Federico y que, inocente o desprevenido, acepta conversar con Spock a través del chat. Spock saca los colmillos. Se retuerce de risa. Tiene control absoluto de la computadora de Federico. Le espía el disco rígido: fotos, cartas, juegos. Spock dice: -Si a mí me llega a pasar esto me muero... me sentiría violado. Mi postura es: yo lo hago, pero odiaría que me lo hicieran a mí." (LN_Peligro en el disco rígido, UT:78).

e) Aliteración.

"El sistema de redes está en jaque. O en "hacker". Pero, al menos por ahora, el rey goza de buena salud." (FUTURO-Guerrilleros y piratas en la red, UT:70).

f) Advertencia. "De modo general, aún sin la evidencia de las probables consecuencias, los artículos de opinión enfatizan las amenazas *posibles* y el terror: abundan los escenarios catastrofistas orientados generalmente ya sea a satanizar a los *otros* o bien a mover a la acción a aquellos de nosotros (y especialmente los políticos) que no toman las cosas con la debida seriedad. (...). Hay que señalar que la lexicalización negativa, la hipérbole, la generalización, el prejuicio religioso y la concretización pueden formar parte de esta representación persuasiva de la amenaza." (van Dijk, 1996b:38). Tenemos muchos ejemplos, pero el siguiente me parece especialmente destacable, puesto que la advertencia se lanza incluso después de que el "experto" consultado ha descartado de plano la existencia del peligro que se denuncia.

“Stanton Mac Candysh, de Electronic Frontier Foundation, opina que "es importante que se tomen medidas precautorias para evitar que ataques como los de la semana pasada se vuelvan habituales". Pero advierte que "lo ocurrido no debe sobredimensionarse." El experto de este centro californiano dedicado a garantizar que los principios constitucionales estadounidenses se protejan en las nuevas tecnologías dijo a Página/12 que no había que reincidir en un pánico semejante al que cundió en algunos grupos por el llamado Y2K, la pronosticada y nunca acaecida caída de los sistemas de computación al comenzar el año 2000. (...) Mac Candysh observó que la terminología utilizada en Estados Unidos para definir los ataques es alarmista. "Se habla de terrorismo cibernético, criminales, sabotaje. En realidad, se trata de unos chicos de colegio secundario o de universitarios que se están divirtiendo". Reconoció, sin embargo, que los actos delictivos pueden escalar y comprometer, por ejemplo, los sistemas militares de seguridad.”
(P12_El riesgo real, UT:1,3)

g) La violación de la norma y los valores. “La forma más elemental de establecer una distinción entre *ellos* y *nosotros* no es solamente describirnos a nosotros mismos en términos benevolentes y a ellos en términos negativos, sino enfatizando el hecho que los *otros* violan aquellas normas y valores que para nosotros son tan preciados.” (idem). En nuestra base contamos con 175 UT, provenientes de 49 documentos en los que se menciona a los hackers como desviantes de algún tipo, siendo el calificativo más frecuente el de “delincuentes” con algún modificador como “informáticos” o precedidos por el prefijo “ciber”. Bastará recordar las acciones que se les atribuyen para tener una idea.

Pero también se les describe como desviantes por naturaleza, por sus inclinaciones incluso previas a su actividad de hacker. En uno de los artículos más extensos (LN_Peligro en el disco rígido), el estereotipo del hacker, diferente a los jóvenes "normales", es construido como presentando una personalidad enferma, trastornada, caracterizada por los siguientes rasgos:

- **COMPORTAMIENTO ANTISOCIAL:** en su mayoría son adolescentes pero consideran a su novia como su peor enemigo, al revés que el adolescente normal y prefieren las relaciones mediatizadas por computadora a las relaciones cara a cara.
“Vander tiene 23 años y dos amigos a los que nunca les conoció la cara: prefiere su letra a través de la pantalla, porque los velos de la cibernética son más dulces.”
- **COMPORTAMIENTO OBSESIVO:** quieren tener el 100% del tiempo para dedicarlo a la computadora. *“(...) mezcla de técnicos anarquistas y científicos obsesivos”;*
- **SADISMO:** Se divierten "espiando, alterando o destruyendo DATOS DE ACCESO RESTRINGIDO"

“Se llama Lobo. Es un tierno hacker de 16 años, que empezó a los 10. Se siente un bicho raro en el colegio. No entiende por qué a sus compañeros no les apasionan los secretos que

guarda un teléfono celular. Por qué ver el animalito destripado, estirando la antenita, no les produce un cosquilleo de emoción”

- **PREPOTENCIA:** "La información debe ser libre y gratuita, dicen, prepotentes"
- **IDOLATRÍA Y FETICHISMO:** "y rinden culto al mismo dios: un disco rígido -no siempre el propio- preñado de información jugosa, que se abre como un durazno maduro".
- **COMPORTAMIENTO DESTRUCTIVO COMPULSIVO:** "*Pero Serial Killer no es su verdadero nick, aunque ilustra bastante bien un tipo de comportamiento compulsivo que le hizo verter sangre de computadoras hace un par de años. Doscientas o trescientas víctimas borradas a cero.*"

” Spock es una criatura de pesadilla. Muchas de sus noches las pasó enterrado hasta las narices en computadoras ajenas, con una orden de borrar todo en la pantalla y jugando con sus amigos a acertarle con una goma de borrar a la tecla de Enter. El destino de un servidor dependía de la trayectoria de una goma de borrar, brotado de lujuria informática.”

- **PARANOIA:** "*Caminan mirando por encima del hombro. No le dan su número telefónico a cualquiera. Madre Paranoia, esa señora con las muelas repletas de cámaras de video, vela por su tribu de adeptos.*"

Algunos de estos rasgos se ilustran extensamente mediante relatos de carácter literario con predominancia de secuencias descriptivas muy subjetivas y expresivas con abundancia de comparaciones, metáforas e hipérboles. Las secuencias descriptivas se intercalan con otras narrativas y dialogales subordinadas a la descripción, con carácter ilustrativo. “Todo el despliegue sintáctico nominal – aposiciones, oraciones adjetivas, complementación - se pone al servicio de la construcción de cuadros y retratos que manifiestan la propia visión del locutor a través de la selección ...” de adjetivos valorativos precisos y sugerentes (Calsamiglia y Valls, 2001:281).

h) La presuposición. “Un dispositivo semántico bien conocido para enfatizar indirectamente nuestros atributos buenos y sus malos; esto es, se supone que estos son bien conocidos por todos como si dependieran del sentido común y por tanto no requirieran formularse explícitamente.” (p. 36-39).

“Ya saben: hackers. Curiosos eternos de las redes informáticas, fisgones de sistemas operativos propios y ajenos. Mezcla de técnicos anarquistas y científicos obsesivos que se rebelan contra la información oculta. La información debe ser libre y gratuita, dicen, prepotentes, y rinden culto al mismo dios: un disco rígido -no siempre el propio- preñado de información jugosa, que se abre como un durazno maduro”. (LN_Peligro en el disco rígido, UT:1).

h) Descalificación retórica: Denomino así en realidad al uso de diversos recursos como la ironía, burla, parodia, antífrasis y similares, al citar otros discursos. En el corpus estudiado suele aparecer combinado con la siguiente estrategia.

i) Distanciamiento enunciativo: Entiendo por ello la cita entrecomillada de las opiniones que no se comparten. En nuestro corpus las declaraciones de hackers u otros “especialistas en informática” que atribuyen motivaciones altruistas, románticas o no-delictivas a los hackers, son citadas entre comillas para, seguidamente, refutarlas, contradecirlas o ponerlas en duda mencionando información supuestamente factual que las contradicen, y/o que siembra dudas sobre la sinceridad o la moral del entrevistado, citando opiniones contrarias de otro “experto serio y respetable” o bien mediante simples comentarios irónicos o burlones (descalificación retórica).

Al citar las palabras de hackers y de personas que los cuestionan el cronista guarda una apariencia de equidad, por permitir que “suenen las dos campanas”. Pero el trato diferencial que hace de las citas y la distancia que toma de algunos discursos a favor de otros, así como la selección que efectúa de los hechos a relatar, evidencia la toma de posición ideológica contraria a los hackers. Algunos ejemplos:

“Sabén muchísimo de computación pero, sobre todo, conocen a fondo la tecnología de las telecomunicaciones. Por lo general "trabajan" por la madrugada y aprovechan una línea telefónica de otra persona, que a esa hora está desocupada, o varias líneas.” (CD_Los piratas de la modernidad, UT:3)

“Aquí en Argentina, la edición de Clarín Digital fue hackeada en la madrugada del 2 de diciembre de 1998, cuando un grupo denominado Fö.EvE. Te4M and XTeam entró violando la seguridad de su sitio web impartiendo consignas por la libertad de expresión, el derecho "a conocer la verdad" o frases como "por una tarifa telefónica plana" e inclusive "no se olviden de Cabezas". El golpe tuvo su efecto y provocó una interesante inversión en equipamientos para mejorar la seguridad de la página de Clarín Digital. Las empresas encargadas del mejoramiento seguramente estarán agradecidas.” (FUTURO-Guerrilleros y piratas en la red, UT:31-32).

“IBM, pionera en la afiliación de estos "ciberrobínhoods" a la buena causa, lanzó al mercado a mediados de los 90 el concepto de "hackers éticos", que aparecían en las fotos vestidos de blanco al mejor estilo médico cirujano. Ellos iban a ser los "chicos buenos", encargados de cuidar la seguridad de "su" empresa.” (idem, UT:62).

“-`Pero la nuestra fue una conducta totalmente antihacker. Un hacker no dice: Entré a tal lugar. Por eso inventamos el nombre del grupo, porque lo que hicimos nosotros no lo hacen los hackers. Lo hacen los idiotas´.

“Xteam siguió sacrificando el prestigio y el 24 de marzo de 1998 (aniversario del golpe militar de 1976) hackeó la página de la Fuerza Aérea Argentina, poniendo una poesía sobre desaparecidos.” (LN_Peligro en el disco rígido, UT:39-40).

Modelos situacionales

Podríamos preguntarnos ¿por qué los medios se expresan de este modo sobre los hackers?. Tal vez sea muy prematuro esbozar una respuesta, pero por lo pronto pensamos que puede tener que ver con los valores periodísticos. Nos referimos con ellos a los que determinan la posibilidad de que un hecho sea seleccionado para ser formulado como noticia y publicado. En primer término están los formulados en términos económicos: las creencias y opiniones de poderosos actores de la noticia (las fuentes), de los anunciantes, los suscriptores, etc. Por las razones que hemos explicado sucintamente más arriba los hackers representan una nueva forma de trabajo característica de lo que se ha denominado la “Nueva economía” que es contradictoria en muchos sentidos con las formas de trabajo y relaciones de propiedad de la economía industrial. Eso los vuelve indeseables para gran parte del *establishment*, que controla el *acceso* a los medios de comunicación.

En segundo lugar están las rutinas sociales de recopilación de las noticias y la producción organizativa, derivada de la periodicidad de publicación, accesibilidad de las fuentes, etc. Estos hacen que se favorezca la selección y producción de relatos periodísticos sobre las elites y que reflejan los valores económicos, sociales e ideológicos de esas elites. Pero en tercer lugar tras haber pasado por los filtros anteriores hay toda una serie de limitaciones cognitivas más específicas que definen los valores periodísticos sobre lo que es digno de ser considerado una noticia y publicado. Los estudios europeos mencionados más arriba señalan que entre éstos valores están la novedad, la actualidad, la presuposición, la consonancia, la relevancia, la proximidad, la desviación y la negatividad.

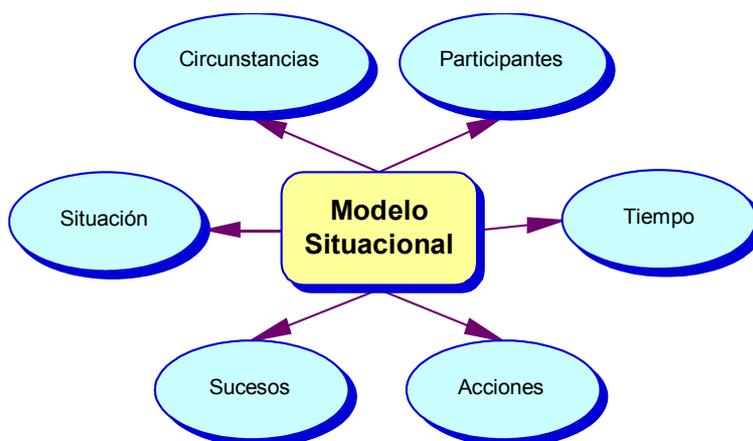
Varios estudios de comunicación, semiótica, cognición y discurso destacan la importancia que la prensa tiene en la formación de estereotipos sociales, esquemas mentales o modelos situacionales y, consecuentemente, de actitudes sobre grupos minoritarios o en algún sentido "diferentes" a la mayoría, como podría ser el caso de los hackers.

“(…) El objetivo último del procesamiento informativo es el establecimiento de un *modelo situacional* (MS) en la memoria episódica. Este MS es una representación de la situación del texto y se asemeja a las categorías esquemáticas generales como el tiempo, la situación, las circunstancias, los participantes, las acciones y los sucesos, cada uno de ellos con su(s) posible(s) modificador(es). [Nota: véase Ilustración 2 - Modelo situacional]. Para el discurso periodístico, la comprensión frecuentemente implica la recuperación y la actualización de modelos existentes (...). Dado que cada situación, estrictamente hablando, es única, sus modelos cognitivos, son asimismo únicos y consisten en una mezcla de información recuperada a partir de MS previos, posiblemente algo generales, nueva información. Esto también posibilita la combinación de diferentes MS.” (van Dijk, 1980:209).

Su MS es también lo que el periodista desea transmitir a los lectores a través de sus artículos (van Dijk, 1980:256).

Comprender un texto, entonces, significa construir un modelo situacional sobre el mismo. en éste modelo se integran conocimientos previos sobre acontecimientos similares al relatado por el texto, que a su vez derivan de otros modelos y esquemas de grupo, que incluyen creencias evaluativas tanto como información factual y experiencias subjetivas. Cuando evocamos un texto, más que recordar sus palabras, lo que hacemos es recuperar el modelo que construimos sobre él, el cual al mismo tiempo dice más que el texto y menos que él.

Ilustración 2 - Modelo situacional



Un acontecimiento nuevo tendrá más probabilidades de ser evocado con posterioridad y por más tiempo cuanto más se preste a ser asimilado a un modelo situacional preexistente. Las personas recuerdan mejor lo que ya conocen y lo que se ajusta mejor a sus expectativas. En otras palabras, muchas veces lo que se “evoca” no es nada que se haya leído, sino una información que “se deduce” del modelo. La noticia que se acomoda a la estructura esquemática canónica de estos modelos será mejor evocada. “Los resultados experimentales confirman que los individuos recuerdan mejor aquello que ya conocen, es decir, la información que recupera viejos modelos, o que simplemente puede situarse en el interior de esos modelos. Asimismo, los sucesos emocionales más destacables, como los crímenes, desastres o conflictos, suelen recordarse bien, especialmente si se adecuan a una creencia existente (estereotipada, prejuizada) o a un esquema de actitud (como la supuesta participación de los negros en los crímenes).” (van Dijk, 1980:258).

De este modo, una vez instalado el estereotipo del hacker como aquel que ingresa en sistemas informáticos violando las barreras de seguridad para producir daños o robar, toda acción anónima ocurrida en este sentido será atribuida a un hacker, reforzando con ello el estereotipo.

Esto nos lleva nuevamente al problema del *acceso*. Según van Dijk es una tarea del ACD el estudio de las estrategias y estructuras cognitivas involucradas en los procesos de que afectan la cognición social de diferentes grupos. El define el Poder social (por oposición al individual) en

términos del *control* que algunos grupos u organizaciones ejercen sobre las acciones o pensamiento de otros, limitando su capacidad de acción o influenciando su conocimiento, actitudes e ideologías. “ (...) lo que está en juego aquí es la manipulación de *modelos mentales* de eventos sociales a través del uso de estructuras discursivas específicas, tales como estructuras temáticas, titulares, estilo, figuras retóricas, estrategias semánticas y otras. A menos que los lectores u oyentes tengan acceso a información alternativa o recursos mentales para oponerse a tales mensajes persuasivos, el resultado de esta manipulación puede ser la formación de *modelos mentales preferenciales* de situaciones específicas (así, por ej. la “revuelta racial”), que a su vez puede generalizarse en conocimientos, actitudes e ideologías preferenciales más amplios (por ej. acerca de los negros o de los jóvenes)” (van Dijk, 1996a:85-86).

Por lo que hemos visto los hackers, como grupo, tienen restringido el acceso a los medios masivos. Su voz, cuando se expresa, es manipulada por medio del manejo de las comillas, el uso de recursos como la ironía, la burla y otras formas de descalificación retórica y nunca es citada sin ser contrastada con la de otro experto que expresa una opinión contraria. Aunque tienen sus propias publicaciones, no son de alcance masivo y cuando la prensa las menciona, pasan por los mismos filtros descalificativos (puede verse aquí un ejemplo de una nota periodística breve³).

Que el control del *acceso* se haya convertido en un mecanismo importante de poder no es tampoco extraño a los cambios económicos revolucionarios que comentamos al comienzo de este trabajo. Precisamente, Jeremy Rifkin, en su más reciente trabajo, señala que en esta Nueva Economía se observa una transición del control de la propiedad de los medios de producción al control del acceso a la información: “En la era de las redes los suministradores que acumulan un valioso capital intelectual comienzan a ejercer el control sobre las condiciones y los términos en que los usuarios se aseguran el acceso a las ideas, el conocimiento y las técnicas expertas, que resultan decisivas. (...) Después de todo, el acceso es algo que hace referencia a distinciones y divisiones, que se refiere a quien está incluido y a quien queda excluido. El acceso aparece como una potente

³ Título: ¿Hackers o crackers?

NOTA PRINCIPAL: Lanzan una fuerte ofensiva contra los piratas informáticos

“Los piratas informáticos estadounidenses, llamados hackers, salieron a defenderse. En un comunicado difundido por Internet a través de la revista virtual 2600, afirmaron que no son criminales y advirtieron que la ofensiva del gobierno estadounidense puede terminar en una "limitación de la libertad individual".

Hasta el más legendario de los hackers, Kevin Mitnick (que purgó cinco años de cárcel y salió libre el mes pasado) declaró que "un verdadero hacker no dañaría jamás intencionalmente ningún sistema".

Lo que los hackers quieren es diferenciarse de aquellos a quienes llaman crackers (en inglés, el verbo to crack se utiliza para aquellos que rompen o decodifican un sistema). Los crackers serían aquellos que asaltan un sistema informático para destruirlo, sustraer información, recaudar o extorsionar por dinero.

Claro que diferenciar a un hacker "bueno" de uno "malo" (cracker) no es simple. Pero el sistema empleado para el bloqueo que realizaron el lunes a sitios como Amazon.com puede dar una pista. Conocido como Deamons, es el mismo que utilizaron los hackers para bloquear las comunicaciones durante la última reunión de la Organización Mundial del Comercio que tuvo lugar en Seattle en noviembre de 1999, cuando 50.000 personas protestaron en contra del rostro deshumanizado de la globalización. Si las misteriosas manos que inutilizaron el lunes al portal Yahoo! comulgan de algún modo con el ideal libertario de aquella protesta, no cabrían ya dudas: se trata de hackers y no de crackers.” (Clarín digital, Viernes 11 de febrero de 2000)

herramienta conceptual para reconsiderar nuestras concepciones del mundo y de la economía, como la metáfora más potente de la próxima era.” (Rifkin , 2000:15, 27).

Conclusiones

Hemos intentado responder a varias de las preguntas que un análisis crítico busca responder en el estudio de los textos informativos, a saber: “¿Quiénes son los actores (protagonistas y secundarios) de las noticias?, (...) ¿Qué acciones se describen, se subrayan o se ignoran?, ¿Qué fuentes se citan y cómo se legitiman?, ¿A quién se cita (o no) y con qué formulación estilística?” (van Dijk, 1997: 61). Aún es mucho lo que podría hacerse en el trabajo de análisis. No hemos analizado la macroestructura semántica. Los titulares por lo general coinciden con la macroproposición de primer nivel, expresando la idea central de la nota periodística, que es simultáneamente la que mejor se evoca, o incluso la única que se evoca pasados unos tres meses, según estudios empíricos. Tampoco hemos analizado la superestructura de las noticias. Aún así pensamos que el análisis de los aspectos léxicos de las noticias desde la perspectiva del ACD con énfasis en el enfoque sociocognitivo de van Dijk arroja suficiente luz sobre la existencia de un proceso de criminalización de los hackers por los medios argentinos, a través de la construcción de un esquema de grupo fuertemente negativo, y un modelo situacional que los asocia a la comisión de delitos mediante el uso de computadoras, todo ello vehiculizado en un discurso que se caracteriza por el uso de abundantes estrategias y mecanismos de presentación del otro típicos del habla racista.

Bibliografía

- Albornoz, Mario, "Cómo leer desde la periferia las nuevas relaciones entre tecnología y sociedad".
En: Finkleleevich, Susana y Ester Schiavo (comp), *La ciudad y sus TIC's (Tecnologías de Información y comunicación)*. pag. 19-25. Un. Nac. de Quilmes, Bernal, 1998.
- Calsamiglia Blancafort, Helena y Amparo Tusón Valls, *Las cosas del decir. Manual de análisis del discurso* Ed. Ariel, Barcelona, (1999 [2001])
- Castells, M. Y P. Hall, *Las tecnópolis del mundo. La formación de los complejos industriales del siglo XXI*. Ed. Alianza, Madrid, 1994.
- Drucker, Peter, *La sociedad poscapitalista*. Ed. Sudamericana. Bs. As. 1993.
- Lindsay, Peter H. y Donald A. Norman, *Introducción a la Psicología Cognitiva*. Ed. Tecnos, Madrid, 1983.

- Michael Stubbs, "British traditions in Text analysis: Firth, Halliday and Sinclair". In: *Text and corpus analysis*. Blackwell Publishers Inc., pag 23-50.
- Pozo, Juan Ignacio, *Teorías cognitivas del aprendizaje*. Ed. Morata. 2º ed. Madrid, 1993.
- Raymond, Eric S., *The new hackers's dictionary*, VERSION 4.1.4. Disponible en: <http://www.tuxedo.org/~esr/writings> , Accedido: 17 JUN 1999.
- Rifkin, Jeremy, *La era del acceso. La revolución de la nueva economía*. Ed. Paidós, Bs. As. 2000.
- Tapscott, Don, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. McGraw-Hill, New York, 1998.
- Tischer, Meyer, Ruth Wodak y Vetter, Two approaches to Critical discourse Analysis. En: *Methods of text and discourse analysis*. Cap. 11 (pág. 145-170). Sage Publications, 2000.
- van Dijk T. A. (comp.), *El discurso como interacción social*. Ed. Gedisa, Barcelona, 2000.
- van Dijk T. A., "Análisis del discurso ideológico". En: *Versión nº 6*, pag. 15-43, UAM-X, México, 1996b.
- van Dijk T. A., "Discourse, power and access". In: Caldas-Coulthard and Malcolm Coulthard, *Texts and practices. Readings in Critical Discourse Analysis..* Ed. Routledge, London, 1996a.
- van Dijk T. A., *Ideología. Una aproximación multidisciplinaria*. Ed. Gedisa, Barcelona, 2000.
- van Dijk T. A., *La noticia como discurso. Comprensión, estructura y producción de la información*. Ed. Paidós, Barcelona, 1980.
- van Dijk T. A., *Racismo y análisis crítico de los medios*. Ed. Paidós. Barcelona, 1997.
- Wodak, Ruth, "¿La sociolingüística necesita una teoría social?. Nuevas perspectivas en el análisis, crítico del discurso. En: *Revista Iberoamericana de Discurso y Sociedad*, p. 123-147. 2000