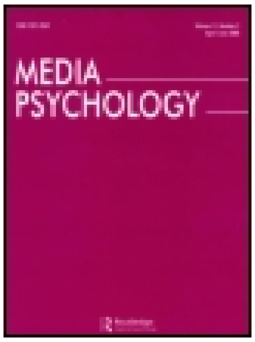

Routledge
Taylor & Francis Group

Media Psychology

ISSN: 1521-3269 (Print) 1532-785X (Online) Journal homepage: https://www.tandfonline.com/loi/hmep20

Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages

Hyung-jin Woo , Yeora Kim & Joseph Dominick

MEDIA PSYCHOLOGY, *6,* 63–82

Hackers: Militants or Merry Pranksters? A Content Analysis of Defaced Web Pages

Hyung-jin Woo
Yeora Kim
Joseph Dominick
Grady College of Journalism and Mass Communication
University of Georgia

Web defacement by hackers has been an emerging topic of concern among those in the online community. Hackers with different psychological motivations may produce different types of defacement. In this study, we content analyzed 462 defaced Web sites to describe how they were changed. In addition, we used social identity theory to predict the severity of the defacement according to the presumed motivations (political vs. personal) of the hackers.

About 70% of the defacements could be classified as pranks, whereas the rest had a more political motive. Moreover, the findings suggest that hackers are not the lonely, isolated individuals sometimes portrayed in the media but are members of an extensive social network who are eager to demonstrate their reasons for hacking and often leave calling cards, greetings, and taunts on Web pages. Text is the preferred means of defacement. Those sites hacked by individuals with a political motivation contained more aggressive expressions and greater use of various communication channels than those sites that were hit by people whose hacking was primarily for fun or self-aggrandizement.

In September of 1999, FBI agents arrested a 19-year-old for maliciously altering the Web page of the U.S. Army (Dickey, 1999). That same year, the home page of the White House was defaced (Hartman & Gerstein, 1999). A year later, a Houston man agreed to plead guilty in a case involving a hacker group that caused more than $1.5 million in damages to U.S. government and corporate Web sites ("A 19-Year-Old," 2000). These are just three examples from a long list of hacking in-

Requests for reprints should be sent to J. Dominick, Deparment of Telecommunication, University of Georgia, Athens, Georgia 30602. E-mail:joedom@uga.edu

cidents from the past few years. Hacking is a growing problem. The U.S. government's Computer Emergency Response Team reported more than 17,000 cases of corporate hacking in 2000. The actual number is probably much higher because many companies do not report attacks to avoid negative publicity (Zetter, 2001). The problem will only grow worse. The Internet is filled with Web sites that offer tips and tool kits for would-be hackers.[1]

Hacking can take many forms: Web page defacement, denial of service attacks, deletion of files and data, theft of private information, viruses, and so forth. In this research study, we looked at the most simple but probably the most obvious form of hacking: Web page defacement. Attrition.org is a group that tracks this kind of hacking and reported about 8,000 page defacements in 2000. (Again, these are reported cases; the actual number is probably higher.) Coca-Cola,® Microsoft,® the U.S. court system, and many other organizations have had their Web sites altered.

Hackers deface Web sites for numerous reasons. Sometimes the motivation is political. Dunn (1999) wrote that the Kosovo conflict was "turning cyberspace into an ethereal war zone where the battle for the hearts and minds is being waged through the use of electronic images, online discussion group postings, and hacking attacks." Conflicts in the offline world often trigger online battles. This phenomenon is seen in the conflict between Israelis and Palestinians ("Waging War Online," 2001), between Koreans and Japanese ("Japanese Textbook Dispute," 2001), and between Chinese and Americans (Cha, 2001). In other cases, patriotism catalyzes hacking on behalf of the hackers' country (Denning, 2001). As Taggart (2001) pointed out, "Various transnational groups of hackers and defacers split along nationalistic, religious, and ethnic lines have joined the conflict" (p. 1).

Other hackers hack to further a cause. One such group is Ethical Hackers Against Pedophilia (E.H.A.P.; http://www.ehap.org), a group of hackers whose goal is to stop the exploitation of children on the Internet. Other hackers want to keep cyberspace free from the monopolistic power of transnational corporations. These individuals try to maintain cyberspace as an anticommercial, deregulated realm where information is shared without monetary compensation.[2] In short, promoting social norms and values are the key motives behind their activity. The term *hacktivist* has been coined to describe this type of hacker.

In contrast, many hacker groups and individual hackers disrupt Web sites and servers with little regard for the sites' political, national, religious, or ethnic identity. Rather, they focus on personal issues, making a game of taunting other Web sites or breaking into other computer systems merely for the fun of it, or for peer recognition, or to impress a significant other, or for the sense of personal accomplishment that comes with cracking a complicated system. Their hacking might be described as a prank or as mischief. According to Rist (1998), a prime motivational factor for hacking is simple ego. Rist (1998) pointed out that "a big chunk of a true hacker's mind-set is ego: I am smarter than you are, just check your Web page" (p. 1). Not surprisingly, hackers often brag and show loopholes in the site to Webmasters, thus proving that they are better technocrats than those who manage the Web site. Raymond (2001) maintained that to be a hacker, a person must get a thrill from solving problems, sharpening skills, and exercising intelligence. One hacker (Emmanuel Goldstein, interviewed by CNN.com; "Q & A with Emmanuel Goldstein," 2001) claimed his reason was "to seek knowledge, discover something new, be the first person to find a particular weakness in a computer system or the first to be able to get a certain result from a program." Denning (2001) reported that the thrill of illicit behaviors, excitement, and challenge was the main reason for hacking. Yet another reason for hacking is to gain peer recognition by informing other hacker communities about information, techniques, and sources. Finally, some hackers put words and images on others' Web pages to impress their boyfriends/girlfriends (http://www.Itworld.com Web site). To summarize, the prime motivation for the types of hacking mentioned previously is personal aggrandizement or achievement.

Furthermore, there is a social dimension to hacking. Taggart (2001) suggested that this tendency is reflected in their language, specific to the hacker/defacer undergrounds—"Fuckz" are given to opponents as hackers taunt their rivals. "Greetz" are given to those individuals and groups with which they align themselves (Taggert, 2001, p. 2). These greetings for friendly hackers or negative statements toward rival groups on defaced Web pages are evidence that some hackers try to align themselves with or against other hackers depending on their ideology, agenda, or favorite issues.

What are the characteristics of Web pages defaced by hackers? Dominick (1999) noted that people use a personal homepage as a way of self-presentation by including features such as a feedback mechanism, links to other sites, likes/dislikes, opinions, and so forth on their Web pages. In turn, hackers use other people's Web sites as a way of adverse presentation against others by defacing the original Web pages and replacing them with images and texts of the hacker's choice. In that connection, the major purpose of this study was to describe defaced Web pages. By content analyzing defaced Web sites, we might find clues that help us better understand the hacking phenomenon, the tools that hackers use, and the psychological motivations of those who hack.

THEORETIC RATIONALE

Social Identity Theory

Because little is known about hackers and their efforts to deface Web pages, this study was by necessity exploratory and primarily descriptive. Nonetheless, there is an existing theoretical framework that might be useful in suggesting two preliminary hypotheses. Although it was never developed to deal with hacking, a theory from social psychology called social identity theory seems relevant.

Social identity theory (Leyens, Yzerbyt, & Schadron, 1994) suggests that people have an innate and powerful tendency to organize themselves into groups. The extent to which persons associate themselves with groups establishes their social identities. These groups might be political (liberals, conservatives), religious (Christian, Muslim), ethnic (Jews, Arabs), or even social (Cubs fans, Mets fans). Moreover, these social identities serve to distinguish in-groups (those groups one belongs to) from out-groups (those that others belong to). Those in the in-group define themselves as what the out-group is not. Group members try to maximize the esteem of their group by various methods. They might, for example, emphasize the positive attributes of the in-group while downplaying or denigrating the achievements or abilities of the out-group. Members of the in-group are often mistrustful of people from other groups, particularly those groups that may pose a threat to the stability or integrity of the in-group. This process has been used to describe the development of many phenomena including racial prejudice, gang rivalry, and criminal identity.

Of interest to this study is what happens when competition for resources (power, land, money, status, etc.) occurs between in-groups and out-groups. In this situation, social identity theory suggests that one reaction of the in-group would be to somehow hinder the out-group in some aggressive way. This phenomenon was demonstrated in the classic Robbers Cave experiment (Sherif, Harvey, White, Hood, & Sherif, 1961), in which young boys were divided into two groups and had to compete for rewards. The conflict between the groups began with verbal abuse and eventually escalated into aggressive behavior.

Based on this rationale, we may infer that some hackers might feel threatened by out-groups who compete with them or differ from them in their politics, religion, nationality, or ethnicity. For example, hackers involved in the political conflicts in the Middle East, South America, and Asia might be threatened by the existence of sites containing the opposing viewpoint (e.g., an enemy government's Web site, other religious Web sites, or transnational corporations' Web sites). One way to react to this threat is to respond aggressively against the menacing source. Thus, defacing the out-groups' Web sites with aggressive messages or violent threats may strengthen the feelings of identification or self-esteem the hackers have with their own group. Hackers whose activities are prompted not by threat but by some other motivation would not feel the need to make an aggressive response. Hence, the following hypothesis (H):

H1: Hackers whose inferred motivation for defacing Web sites is a reaction against some opposing political, social, ethnic, religious, or racial out-group will express more aggression against target Web sites than hackers who deface pages for some other reason.

Furthermore, Branscombe and Wann (1994) found that threats to the value of a social identity prompted an in-group to encode more derogatory messages about an out-group. Similarly, Elsbach and Kramer (1996) examined members' responses to a threat to their organizational identity. They found that group members responded to the threat by engaging in more communication activities that highlighted the positive aspects of the in-group. Both of these studies suggest that threats to a group's social identity are met in part by an increase in communication. Thus, after defacing the out-group's Web sites, hackers may feel the need to further reinforce their own group's esteem by putting messages on the target pages that strengthen their own group's viewpoints or repudiate opposing viewpoints. This should translate into increased communication activity (longer messages, using more channels to convey the message such as audio, animation, and video files, and including hyperlinks and e-mail addresses.) This tendency should not be present among those whose hacking is for more personal reasons. Accordingly, the following hypothesis was tested:

H2: Hackers whose inferred motivation for defacing Web sites is a reaction against some opposing political, social, ethnic, religious, or racial out-group will leave longer messages on the defaced pages and use more Web-based channels of communication than those who hack for some other reason.

METHOD

Sampling

There is no existing sampling frame that lists all defaced Web pages. The most comprehensive one available is the defacement archive at http://attrition.org.[3] This Web site has collected Web pages defaced by hackers since 1995 and has made a list in chronological order. Unfortunately, they stopped the service as of May 2001 due to immense defacement activities beyond their capacity. However, they still hold the collections on their server. The defaced Web page collection at attrition.org provides (a) defacement date; (b) the identity (usually some screen name or handle such as ttyo or Nitrogear) of the person or group who defaced it; (c) the defaced Web pages as well as the original page; and (d) the defaced server system such as NT, UNIX, or Windows® 2000.

To obtain a random sample in this study, we selected defaced Web pages from January 1, 2001 to April 30, 2001 in every fifth site after a random start. A total of 770 defaced Web sites from the defacement archive at attrition.org was chosen as a sample. Each selected defaced page and the original were printed out to protect them from a second defacement and to avoid their being removed by attrition.org. Defaced Web pages that contained audio, active animation, and streaming activities were recorded by checking whether an attribute had a multimedia file. Coders checked the all files on HTML sources whenever they looked at those effects on the defaced page.

Unit of Analysis and Content Categories

McMillan (2000) claimed that "defining the unit of analysis is a unique challenge on the World Wide Web" (p. 82). Ha and James (1998) concluded that the home page can be the most appropriate unit of analysis because many visitors to a Web site decide whether they will continue to browse the site on the basis of their first impression of the home page. Ha and James also suggested that coding an entire site could be extremely time consuming and introduce biases based on Web site size. Because hackers/defacers usually erase original content and put new texts and images of their choice on the index page of a site, this study selected the index page of a defaced site as its unit of analysis rather than coding all of the Web pages of a defaced site.

The first purpose of this study was to describe how hackers defaced Web pages. The following variables (all measured at the nominal level) were examined:

On the defaced page:

1. Presumed motivation for hacking.
   Based on a review of previous literature, the purpose behind the defacement could include promoting nationalism, religion, ethnicity, freedom of information against transnational corporations, stopping porn sites or other sites encouraging unacceptable behaviors, gaining peer recognition by marking territory, impressing a romantic partner, beating the system (successfully invading the target site and chastising the system administrator), showing off and bragging about hacking skills, multipurpose, and other.

2. Identity of hacker.
   Were hackers' names or other identification on the defaced Web pages? If the hacker who defaced a site left a handle (a screen name), the name was recorded by attrition.org

3. Calling cards and greetings.
   Do hackers align themselves with their cyber friends (in-groups) and derogate their enemies (out-groups)? Each site was checked to see if "Fuckz," "Greetz," "Prop," or "Shout out" (common words of greeting and scorn among hackers) appeared to identify recognition of specific hackers' communities.

4. Length of message and channels used to express their message.
   Each site was checked to see if hackers put texts, pictures, audio files, active animation files, streaming media files, or drawings and whether they put interactive functions such as hyperlinks, e-mail addresses, or hackers' homepage URLs. The length of the message was measured by counting the number of sentences left at the defaced site.

Last, information about the domain and the country that hosted the defaced Web sites was recorded.

The second purpose of this study was to test two hypotheses suggested by social identity theory. The defaced Web pages were divided into two groups: Those defaced Web pages whose alteration was apparently motivated by politics, nationalism, religion, ethnicity, responses against transnational corporations and efforts to stop porn sites were placed in the "reaction against an out-group" category and the hackers involved were named *militants.*[4] The hacking on the rest of the pages did not seem to be provoked by a confrontational motive (impressing a romantic partner, bragging, peer recognition, beating the system), and these pages were placed in the *prankster* category. "Multipurpose" and "other" categories were dropped from this analysis.

H1 suggested that the militant group would behave more aggressively than the pranksters. What constitutes an aggressive act when defacing a Web page? *Aggression* is commonly defined by social psychologists as behavior with intent to harm the individual who is its object (e.g., Baron & Richardson, 1994; Berkowitz, 1993). According to Baumeister, Bushman, and Campbell (2000), aggression ensues when favorable opinions are disputed or questioned by other people. Some researchers have suggested that verbal violence that intimidates or embarrasses people may inflict psychological or emotional harm (Kunkel et al., 1995; Stein & Freidrich, 1975; Williams, Zabrack, & Lesley, 1982). Other scholars have believed noxious words to be violent behavior (Mustonen & Pulkkinen, 1997; Van der Voort, 1986). Potter and Warren (1998) included verbal threats and hostile remarks as aggressive behaviors. Accordingly, verbal attacks (aggressive expressions against target Web sites) were the units of analysis used to test the hypothesis.

Verbal attacks were made up of (a) profane or obscene language (e.g., “Fuck,” “Son of a Bitch,” or genital-oriented curses), (b) verbal insults (humiliating opponents without curses, e.g., “stupid,” “dumb,” or “bird brain,” etc.), and (c) serious threats (e.g., “I’ll kill you,” “I will annihilate your nation”) on defaced Web pages.

Another measurement for aggression was visual attack. According to Phillips (1999), hatred against others is explicitly reflected in hip-hop graffiti. By using signs, marks, or gang-oriented slang, gang members try to identify alliances and enemies. Likewise, hackers also use signs, drawings, or sexually explicit materials to express their anger toward their enemies. Thus, in this study we measured visual attacks composed of (a) insulting active animation (e.g., parody pictures produced by a flash Web tool), (b) insulting drawings, (c) insulting pictures, (d) sexually explicit materials, and (e) bizarre materials (e.g., dead body, human excrement, devil face, skeleton, etc.).

H2 suggested that militants would leave longer messages and use more communication channels. Message length was measured by counting the number of text messages left on the site. Communication channels were measured by noting if the hackers added the following to the defaced site: pictures, audio files, active animation files, streaming media files, drawings, and interactive functions such as hyperlinks, an e-mail address, or the hackers’ homepage.

Intercoder Reliability

Two graduate students coded the content on defaced Web pages. Coders spent 12 hr in training sessions, and all coded 30 defaced Web pages as practice. Both coders had knowledge of HTML and a variety of Web editors, including Dreamweaver,® Flash,® and Photoshop.® Coding was completed over 2-week period during fall 2001. Reliability was calculated by having two coders examine a random subsample of 20% of the defaced Web pages from the sampled English sites provided by attrition.org. Because most of coding decisions involved a simple judgment about whether some feature on a defaced Web page was present or absent, the reliability coefficients in this study were calculated in terms of Scott’s *pi*. Intercoder reliabilities across each variable were acceptable: frequency of features on defaced Web pages (the purpose of defacement = .83; who did it = .82; calling cards = .79; bragging remarks = .80; technical tools[5] = .79 to 1.00); nationality (.88), and type of domain (.81). For aggressive expression, intercoder reliabilities for verbal attacks (profane language = .92; verbal insults = .86; and serious threats = .89) and visual attacks (insulting animation = .84; insulting drawing = .78; insulting picture = .85; sexually explicit picture = .83; and bizarre picture = .83) were slightly lower but still acceptable.

RESULTS

From the initial sample (770 sites), non-English defacement, directory denied sites, and defaced Web pages full of uninterpretable symbols were excluded. This left 462 defaced Web pages for analysis.

Descriptive Analysis

The first purpose of this study was to describe the typical features of defaced Web pages. As far as inferring psychological motivations for hacking, the hackers themselves were helpful. When they defaced others' Web pages, hackers generally explained why they erased old content and put up new content. Table 1 summarizes the frequency of each feature on defaced Web pages.

Specifically, the most frequent reason why hackers break in and change others' Web pages was a broad category that would fall under the general prankster label. About 71% of the defaced pages fell into this category. There were several subsections in this category. The most frequent prankster subcategory (37% of all defacements) was "beating the system," in which the hacker taunted the site's system ad-

TABLE 1
Inferred Motivations for Web Page Defacement

Motivation	Percentage
Pranksters (71%)	
Beating the system	37
Tagging/peer recognition	24
Bragging	8
Romantic	2
Militants (23%)	
Nationalism	10
Ethnicity	7
Freedom of information	3
Stopping pornography	2
Religion	1
Multipurpose	2
Others and no apparent purpose	3
Total	99

Note. $N = 462$. Total percentage does not add up to 100% because of rounding.

ministrator and/or left messages about repairing the site ("I hacked your site. Heh. Heh. Heh"; "Yippie Yai Yah!! an0ther b0x gets 0wned. This is proof on how lazy admins can be"; "Admin: your system is vulnerable. We don't want to prejudicate your system. Hackers are not menace. If you want to know how to fix your system send an e-mail to … ").

Also placed in the prankster category was marking territory for peer recognition (24%) in which the hacker left a personal signature to let others know who hacked the site, similar to "tagging" in graffiti ("This site is owned by 2d8," "hacked by xst," "This site has been compromised by encrypt0 … I hacked this because I felt like it and was bored"). Self-aggrandizement or bragging was the motivation behind about 8% of the defacements in the prankster category ("Microsoft Win 2K is a piece of cake"). Only a few defacements were done for the apparent reason of impressing a romantic partner ("B4dBOy dedicates this one to Simona: please remember I WILL LOVE YOU FOREVER").

The following inferred motivations were placed under the militant label. Ten percent of the pages were defaced for political or nationalistic reasons ("USA we don't want to be controlled by you"; "USA > *.CN"). About 7% of defacements seemed prompted by ethnicity (" Fuck you to … all bloody Israelian Jews").

Only a few defacements seem prompted by freedom of information (one defacement showed Bill Gates leading a parade of Nazi storm troopers), stopping porn sites (one defacement aimed at stopping the spread of child pornography sites contained a "Pedophile profile of the week"), and religion ("Greetings to our Muslim Brothers … long live Islam"). Less than 2% of the pages were classified as multipurpose. In short, far more of the defacements fell into the prankster category than the militant category. Table 2 summarizes the remaining descriptive variables.

Most defaced sites belonged to groups in the United States (24%) and most shared the .com domain (50%).[6]

Hackers are proud of their work. When they hacked a page, they almost always wanted others who accessed the site to know who controlled, owned, and conquered it. This occurred in 9 out of 10 defaced Web pages. Hacking is not an anonymous activity.[7]

Unlike the media stereotype (the films *War Games, Sneakers, The Matrix;* The Lone Gunmen" TV series), hackers are not solitary, socially isolated individuals. In fact the data suggest that hackers belong to an extensive social network and identify with a larger hacking community. More than half of the hackers in this study put "fuckz," "greetz," "props," or "shout out" to their rivals or cyber friends ("Shouts go out to the following people: WHO, Antifarmer, Sneed, Soldier X …"). Of all defaced Web pages, 12% insulted rivals by "fuckz" or some other derogatory message. (Some insults were general. One hacker replaced the familiar Windows

TABLE 2
Frequency of Items on Defaced Web Pages

Item	Percentage
Identifying signature	92
Greetings/taunts	51
Bragging/sarcastic remarks	51
Technical tools used in defacement	
Text	85
Drawings	39
E-mails	39
Hyperlinks	17
Picture	13
Audio files	3
Active animation files	3
Hacker's home pages URL	2
Streaming files	0.4

Note. $N = 462$.

"This page cannot be displayed" message with a parody look-alike page that read, "If you typed the page address in the address bar, make sure that it is spelled correctly, if it's not then you are a retard and shouldn't be online." Other insults were intensely personal. "KebabKru: Fuck you! You want to insult me on your defacements, go ahead. I can do that to you also.")

These data suggest that social identity theory is an appropriate analysis tool for this group; hackers categorized themselves into in-groups and had a definite conception of out-groups.

In addition, about one out of two hackers left sarcastic statements about Webmasters' Web design, security, and server systems. They usually recommended that the Webmasters who could not protect their server from hacking should change their NT system into Linux. Moreover, many hackers asked Webmasters to e-mail them to show how to recover the vandalized system and Web pages.

Almost all hackers used text to present their agendas. Again, contrary to the common stereotype that hackers admire technology, hackers used traditional word-based expression to deface Web sites rather than more sophisticated Web tools such as audio, active video, and streaming.[8] The mean score of text usage was five sentences per defaced Web page. The use of sophisticated Web tools on defaced Web pages was less than 3%. Most typical defaced Web pages were done using text, drawings, e-mails, hyperlinks, and pictures. One interesting point was that hackers were more likely to let others know their e-mail address rather than inviting them to visit their home page. Perhaps they worried about counter-hacking by other hackers.

Differences Between Pranksters and Militants

The second purpose of this study was to test if social identity theory predicted how hackers defaced Web pages. The first hypothesis predicted that militant or politically oriented Web defacements would use more verbal and visual forms of aggression than defacements done for some other purpose. In the militant group, defacements were done for the following motivations (as summarized in Table 1): politics, nationalism, religion, ethnicity, freedom of information, and stopping porn sites. Total *N* for this group was 112. The other group (the prankster group) included defacements for all other reasons. Total *N* for this group was 329. The multipurpose and other group were not included in this analysis.

The hypothesis suggested that militant defacements would contain more aggressive expressions than prankster ones. Table 3 demonstrates the frequency of verbal attacks and visual attacks on defaced Web pages for both groups.

The most frequently used verbal attack for both groups was profane/obscene language followed by verbal insults and serious threats. All verbal attacks showed statistical significance between the groups. Militant defacement pages contained more profane/obscene language (“Beat down the Imperialism of America. Fuck USA.”), $\chi^2(1, N = 441) = 41.38, p < .001$; verbal insults (“You lame ass geeks and morons.”), $\chi^2(1, N = 441) = 15.19, p < .001$; and serious threats (“Israel, more will die until you learn what’s not yours.”), $\chi^2(1, N = 441) = 27.17, p < .001$ than the prankster group.

There were relatively few instances of visually aggressive images, making it difficult to find group differences. The only meaningful difference was in the bizarre materials category in which those pages defaced for militant reasons contained a far greater percentage of this content, $\chi^2(1, N = 441) = 15.51, p < .001$. Militant hackers tended to show dead bodies, injured children, or scenes of killing on the defaced pages. On the other hand, pranksters were more likely to include a devil’s face, skeleton, or eerie pictures. In the sexually explicit category, prankster defaced pages were more likely to contain indecent materials than militant ones, but there was no statistical significance. In sum, H1 was supported as far as verbal aggression was concerned. There were too few examples to provide a valid test of the hypothesis with regard to visually aggressive materials.

TABLE 3
Frequency of Verbal and Visual Attacks Against Web Pages

Aggressive Expression	Militants (%)[a]	Pranksters (%)[b]
Verbal attack		
Profane language**	50	19
Verbal insults**	19	6
Serious threats**	13	1
Visual attack		
Insulting active animation and video effects*	2	0
Insulting drawings	6	4
Insulting pictures	3	2
Sexually explicit materials	3	5
Bizarre materials**	12	2

[a]$N = 112$. [b]$N = 329$.
*$p < .05$.** $p < .001$.

The data in Table 4 suggest support for the H2. Those pages defaced for apparently militant reasons were more likely to contain a text message and had longer text messages (10.2 sentences vs. 2.0 sentences), $t(439) = 9.51, p < .001$. The pages altered by the militant group were also more likely to contain pictures, audio, animation, streaming, hyperlinks, and e-mail. The only two channels that did not show a significant difference were the inclusion of the hacker's homepage URL and the presence of a drawing. It would appear that those hackers who are motivated by the threat posed by an out-group used more communication channels to bolster their own position and denigrate the out-group's position than did those who were motivated by other reasons.

DISCUSSION

Web-page defacement has been a hot topic among various Internet communities. However, little empirical study has been conducted on this issue because it is difficult to obtain data from hackers and wrongdoers on the Internet. This study offers some preliminary information about hacking inferred from the content of deface Web sites.

TABLE 4
Different Web Tools Used in Defacements

Web Tools	Militants (%)[a]	Pranksters (%)[b]
Text***	97	81
E-mail**	53	34
Drawing	45	37
Picture***	27	9
Hyperlink**	25	13
Active animation file**	8	2
Audio file**	7	2
Hacker's home page URL	3	2
Streaming file*	2	0

[a]$N = 112$. [b]$N = 329$.
*$p < .05$. **$p < .01$. ***$p < .001$.

Unlike the common stereotype that hackers are computer experts on the cutting edge of cyber technology (Rogers, 1999), this study found that most used basic text messages and basic interactive tools such as e-mails and hyperlinks to express their views. More sophisticated technology such as active animation, streaming media, and audio tools occurred infrequently on defaced Web pages. Another common belief (Chandler, 1996; Goodell, 1996; Littman, 1997) that hackers are socially inept, intrapersonally retrospective, and sexually distorted persons also needs to be reconsidered. In this study, we found that hackers were actively identified with other members and were part of an extensive cyber network of fellow hackers. In addition, they used few obscene materials to express their views.

These data illustrate that social identity theory is an appropriate theory for analyzing hackers' activities. Hackers do not hack in a vacuum. The numerous greetings to other hackers demonstrate that they clearly associate themselves into groups. There is a distinct "us" vs. "them" philosophy and an attempt to differentiate the in-group from the out-group. A concrete illustration of this comes from a message left by a hackers' group called "Hi-tech Hate" on a Web site maintained by the U.S. district court system:

> We will fight under each flag besides people we don't even know but whose idea of freedom is the same as our one. We're against each kind of war, each kind of oppression, against each form of abuse of power. … We don't want that the world will be guided by multinational companies.

Moreover, social identity theory was useful in predicting the characteristics of defaced Web pages. As suggested by H1, Web pages that were apparently defaced for militant reasons were more apt to contain various forms of visual aggression. Also, as predicted by H2, these same sites contained longer messages and used more communication channels.

Given the exploratory nature of this study, however, it would be presumptuous to suggest that the results represent a test of social identity theory. The findings are consistent with this theory, but it does not provide a full explanation. For example, although social identity theory can account for in-group and out-group effects for militants, it is less helpful in explaining the motivations of some of the hackers who fall in the prankster category. It is difficult, for example, to identify an in-group and an out-group for hackers who deface Web sites to impress girlfriends. Moreover, although pranksters who hack to gain peer recognition or to feel superior when they beat the system have a fairly definable in-group (the hackers' community), the out-group for these individuals is less clear.

In these instances, a relevant theoretic framework might be Breckler and Greenwald's (1986) three facets of the self: the private self, public self, and collective self. In brief, the private self earns self-regard from meeting or exceeding internal standards of success, whereas the public self is sensitive to the evaluations of significant others and seeks to gain their approval. Last, the collective self establishes self-worth by helping to achieve goals of important reference groups such as family, teachers, coworkers, political factions, ethnic groups, and so forth.

This rationale suggests that hackers who deface Web pages to impress peers or girlfriends or boyfriends may be motivated by their public self, and hackers who hack to achieve a measure of personal satisfaction would be motivated by their private self. Hacking for a political cause may be a manifestation of the collective self. The strength of an individual's identification with one of these orientations should influence his or her response. The findings on H1 would be consistent with this model if hackers (a) identified themselves with the reference groups relevant to the collective self and (b) if these groups endorsed hostile and aggressive responses as a means of achieving a goal.

Realistic group conflict theory (Campbell, 1965) is also relevant. It suggests that incompatible goals and competition for scarce resources cause conflicts between groups. In addition, a perceived realistic threat will cause hostility toward the source of the threat and increase in-group solidarity and cohesion. Consequently, in this context, hackers who perceive Web sites of opposing groups to constitute a threat to their own group should respond with more aggressive responses toward the threatening Web sites, as predicted by H1.

Finally, terror management theory offers another possibility. This theory suggests that when people are reminded of their own mortality, their need for faith in their own worldview is increased (Greenberg, Pyszczynski, Solomon, Rosenblatt, Veeder, Kirkland, et al., 1990). According to Kernis (1995), threats to a certain worldview lead to a negative judgment of those who challenge cultural norms and to positive judgments of those who endorse them. As a result, people generally respond favorably to those who share their worldview and unfavorably to those who do not. Such a negative response might be manifested in increased hostility. Israeli hackers, for example, might react aggressively to Arab sites that threaten their ways of thinking, an outcome consistent with H1. In any case, future research should strive to clarify the theoretical mechanisms underlying hackers' motivations.

Furthermore, although the number of defaced Web pages done by pranksters outnumbered those done by militants by more than a three to one ratio, this result should not be taken to suggest that Web page defacement is a harmless pastime. Social identity theory suggests that conflicts between in-groups and out-groups can escalate to more intensive levels. Conflicts between nations, religions, and ethnic and political groups can carry over into the online world. If the conflict becomes severe enough, what starts out as a prank could easily accelerate into more serious cyber warfare. In fact, a recent item in *Newsweek* (Hosenball, 2002), suggests that such a pattern is actually taking shape. A group calling itself the "Muslim Hackers Club" surfaced about 5 years ago. Their activities were generally confined to defacements and postings of hacking strategies, but in 2002, government officials warned that the group now included experts who taught courses in cyber terrorism.

This study has some limitations. First, this study selected only the defaced Web pages posted in English. Hence, the findings of hacking/defacing issues may reflect characteristics of just a part of the hacking communities. Second, this study divided the sample into the two general groups (militants vs. pranksters) based on the inferred motivation for hacking a site. This was an admittedly rough categorization and probably lumped together several different motivations that might be useful to study individually. Third, the best sampling frame available was that provided by attrition.com. It is unclear if this listing is an accurate representation of the entire world of hacking. Finally, this study considered only defaced Web pages, arguably the mildest form of hacking. These data shed no light on the activities and motives of those who perform the more serious kinds of hacking: denial of service, destruction of files, and spreading viruses.

Of course, the best way to investigate the social world and motivations of hackers would be to collect data from the hackers themselves. Future research might focus on hackers' personal characteristics such as narcissism, intrinsic and extrinsic motivations, and self-esteem. A survey might provide more detailed demographic information about hackers and examine the relations between the purpose of hacking and aggressiveness in more systematic ways. Last, comparing hackers of different nationalities would be revealing to see how different political issues are involved in cyber war.

ACKNOWLEDGMENT

An earlier version of this article was presented to the Communication and Technology Division of the International Communication Association, Seoul, Korea, November 2002.

NOTES

[1] The widespread availability of these tools has led to a new generation of hackers called "script kiddies." These are hackers who do mischief with programs written by others often without understanding how they did it. Although there is no way to determine an actual number, it is likely that script kiddies altered many of the defaced pages examined in this study. Veteran hackers view script kiddies with derision.

[2] Although some hackers show hostility toward capitalistic transnational companies, others try to make money by stealing information from those same companies (Shaw, 2001).

[3] Another such site is alldas.de

[4] *Hacktivist* or *Confrontational* might be other apt names for this category.

[5] Intercoder reliability for variables measured using percentage of perfect agreement were the following: text, .79; picture, .85; audio file, .85; active animation file, 1.00; streaming media file, .91; hyperlink, .81; e-mail, .93; hacker's homepage URL, .89; and drawing, .82.

[6] In second place was China (8%), followed by Korea (4%), Taiwan (4%) and Japan (3%). No other country accounted for more than 3% of the defaced pages. Many defacements appeared to be cross-border, as hackers in one country chose to deface pages in some other country, perhaps assuming that there was less chance they would be prosecuted by authorities in the target country.

[7] Using a pseudonym lets hackers maintain privacy and secrecy while at the same time letting them ally with and rally against various groups.

[8] This lack of technical sophistication is another indication that many defacements were done by script kiddies.

REFERENCES

Baron, R. A., & Richardson, D. R. (1994). *Human aggression* (2nd ed.). New York: Plenum.

Baumeister, R. F., Bushman, B. J., & Campbell, W. K. (2000). Self-Esteem, narcissism, and aggression: Does violence result from low self-esteem or from threatened egotism? *Current Directions in Psychological Science, 9,* 26–29.

Berkowitz, L. (1993). *Aggression: Its causes, consequences, and control.* Philadelphia: Temple University Press.

Branscombe, N. R., & Wann, D. (1994). Collective self-esteem when a valued social identity is on trial. *European Journal of Social Psychology, 24,* 641–657.

Breckler, S. J., & Greenwald, A. G. (1986). Motivational facets of the self. In R. M. Sorrentino & E. T. Higgins (Eds.), *Handbook of motivation and cognition* (Vol. 1, pp.145–164). New York: Guilford.

Campbell, D. T. (1965). Ethnocentric and other altruistic motives. In D. Levine (Ed.), *Nebraska symposium on motivation* (pp. 283–311). Lincoln: University of Nebraska Press.

Cha, A. (2001, April 12). *Chinese suspected of hacking U.S. sites.* Retrieved June 11, 2002, from http://www.washingtonpost.com/wp-dyn/articles/ 13431-200 April12.html

Chandler, A. (1996). The changing definition and image of hackers in popular discourse. *International Journal of the Sociology of Law, 24,* 229–251.

Denning, D. (2001, February 14). *Activism, hacktivism, and cyber terrorism: the internet as a tool for influencing foreign policy.* Retrieved from http://www.terrorism.com/documents/denning-infoterrorism.htm

Dickey, C. E. (1999, September 1). Web page hacker arrested, government sites becoming more secure. *ArmyLINK News.* Retrieved from http://www.dtic.mil/armylinknews/Sep.1999

Dominick, J. R. (1999). Who do you think you are? Personal home pages and self-presentation on the World Wide Web. *Journalism & Mass Communication Quarterly, 76,* 646–658.

Dunn, A. (1999, April 3) Crisis in Yugoslavia: Battle spilling over onto the Internet. *Los Angeles Times,* p. 12.

Elsbach, K., & Kramer, R. (1996). Members response to organizational identity threats. *Administrative Science Quarterly, 41,* 442–476.

Goodell, J. (1996). *The cyber thief and the samurai.* New York: Dell.

Greenberg, J., Pyszczynski, J., Solomon, S., Rosenblatt, A., Veeder, M., Kirkland, S., et al. (1990). Evidence for terror management theory II. The effects of mortality salience reactions to those who threaten or bolster the cultural worldview. *Journal of Personality and Social Psychology, 58,* 308–318.

Ha, L., & James, E. L. (1998). Interactivity re-examined: A baseline analysis of early business Web sites. *Journal of Broadcasting & Electronic Media 42,* 457–474.

Hartman, B., & Gerstein, J. (1999). *White house hacked.* Retrieved July 19, 2002, from http://abcnews.go.com/sections/tech/Daily News/whhack 990511.html

Hosenball, M. (2002, May 20). Islamic cyber terror. *Newsweek,* 8.

Japanese textbook dispute sparks cyber attack. (2001). Retrieved July 23, 2003, from the CNN Web site: http://asia.cnn.com/2001/WORLD/asiapcf/ east/03/31/japan.korea.Website/

Kernis, M. H. (Ed.). (1995). *Efficacy, agency, and self-esteem.* New York: Plenum.

Kunkel, D., Wilson, B., Donnerstein, E., Linz, D., Smith, S., Gray, T., et al. (1995). Measuring television violence: The important of context. *Journal of Broadcasting and Electronic Media, 39,* 284–291.

Leyens, J., Yzerbyt, V., & Schadron, G. (1994). *Stereotypes and social cognition.* Thousands Oaks, CA: Sage.

Littman, J. (1997). *The watchman: The twisted life and crimes of serial hacker Kevin Poulsen.* Toronto, Ontario, Canada: Little Brown.

McMillan, S. J. (2000). The microscope and the moving target: The challenge of applying content analysis to the world wide Web. *Journalism & Mass Communication Quarterly, 77,* 80–98.

Mustonen, A., & Pulkkinen, L. (1997). Television violence: A development of a coding scheme. *Journal of Broadcasting and Electronic Media, 41,* 168–189.

A 19-year-old Houston man. (2000, March 29). *Wired News.* Retrieved June 10, 2002, from www.wired.com/news/politics/0,1283,35264.00

Phillips, S. (1999). *Gangs and graffiti in L.A.* Chicago: University of Chicago Press.

Potter, W. J., & Warren, R. (1998). Humor as camouflage of televised violence. *Journal of Communication, 48,* 40–57.

Q & A with Emmanuel Goldstein of 2600, *The Hacker's Quarterly.* (2001). Retrieved June 22, 2002, from the CNN Web site: http://www.cnn.com/TECH/specials/hackers/qandas/goldstein.html

Raymond, E. S. (2001). *How to become a hacker.* Retrieved July 23, 2002, from http://www.tuxedo.org/~esr/faqs/hacker-howto.html

Rist, O. (1998). Get to know the hacker's mind-set. *TechWeb.* Retrieved June 12, 2002, from http://content.techweb.com/se/directlink.cgi?lNW 19980921S0055

Rogers, M. (1999). *Psychology of hackers: Steps toward a new taxonomy.* Retrieved July 26, 2002, from the Inforwar.com Web site: http:www.inforwar.com/hacker/99/HackerTaxonomy.shtml.

Sherif, M., Harvey, O., White, B., Hood, W., & Sherif, C. (1961). *Intergroup conflict and cooperation.* Norman, OK: University Book Exchange.

Stein, A. H., & Friedrich, L. K. (1975). Impact of television on children and youth. In E. M. Hetherington, J. W. Hagen, R. Kron, & A. H. Stein (Eds.), *Review of child development research* (Vol. 5, pp. 183–256). Chicago: University of Chicago Press.

Taggart, A. (2001). *The digital revolt: Resistance & agency on the net.* Retrieved June 27, 2002, from http://georgetown.edu/papers/wtaggert.htm

Van der Voort, J. H. A. (1986). *Television violence: A child's eye view.* Amsterdam: Elsevier.

Waging War Online. (2001). Retrieved January 3, 2001, from the NUA Web site: http://www.nua.ie/surveys/analysis/weekly_editorial/archives/issue1no162.html

Williams, T. M., Zabrack, M. L., & Lesley, A. J. (1982). The portrayal of aggression on North American television. *Journal of Applied Social Psychology, 12,* 360–380.