THE HACKER MENTALITY:

EXPLORING THE RELATIONSHIP BETWEEN PSYCHOLOGICAL VARIABLES AND HACKING ACTIVITIES

by

HYUNG-JIN WOO

(Under the Direction of Joseph R. Dominick)

ABSTRACT

This study investigated hackers' psychological variables and how these variables affect their hacking activities in cyberspace. 1,385 hackers from 30 different countries participated in an on-line survey. Specifically, this research examined 1) how hackers' personality affects their angry temperament, reaction, and behavior, 2) what motivations prompt hackers to be involved in hacking activities, 3) why they keep breaking into others' computer systems, and 4) how they respond when they face a threat to their own cultural worldviews. The results indicated that hackers with high narcissism reported more aggressiveness scores than hackers with low level of narcissism. Intrinsic motivation as well as extrinsic motivation in a hacker was partially associated with hackers' aggressiveness. Hackers with high level of flow tended to get more involved into hacking activities than hackers with low level of flow. Hackers who strongly endorsed nationalism showed higher aggressiveness scores than hackers with lower levels of nationalism when they felt threatened.

INDEX WORDS: Hackers, Cyberterrorism, Narcissism, Flow, Terror Management Theory, Intrinsic and Extrinsic motivation, Aggressiveness

THE HACKER MENTALITY:

EXPLORING THE RELATIONSHIP BETWEEN PSYCHOLOGICAL VARIABLES AND HACKING ACTIVITIES

by

HYUNG-JIN WOO

B.A., Chung-Ang University, Korea, 1995

M.P.S., Chung-Ang University, Korea, 1997

M.A., The University of Georgia, 1999

A Dissertation Submitted to the Graduate Faculty of The University of Georgia in Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA

2003

THE HACKER MENTALITY:

EXPLORING THE RELATIONSHIP BETWEEN PSYCHOLOGICAL VARIABLES AND HACKING ACTIVITIES

by

HYUNG-JIN WOO

Major Professor:	Joseph R. Dominick
Committee:	Spencer F. Tinkham Bruce C. Klopfenstein Andy Kavoori Leonard L. Martin

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
May 2003

To Yeora and Grace (Hyejoon),

whose enduring love and courage make

this possible.

ACKNOWLEDGEMENTS

First of all, I attribute my all honor to my God. Without your help, none of this would be possible. I would like to acknowledge Dr. Joseph R. Dominick, my major professor and academic father in my life. He shows me not only the way to guide this study but also direct me how to deal with the truth. Without his intellectual advice, I would not be able to finish this work.

I appreciate Dr. Spencer F. Tinkham, Dr. Bruce C. Klopfenstein, Dr. Andy Kavoori, and Dr. Leonard L. Martin as members of advisory committee. Their comments and supports make me think alternative ways when I have troubled with hacker study.

Thanks to the *Hackerslab*'s *free hacking zone* team. Specially, I appreciate Mr. Leem, Man-Gi. His supports enable me to get invaluable data in this study.

Finally, I would like to thank my wife Yeora Kim and lovely daughter Grace Woo (Hyejoon!). I love you from the bottom of my heart. Without your support and love, I ‘d be lost. Thanks to my family for their encouragement.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

> "You can play the stock market on-line. You can apply for a job on-line. You can shop for lingerie on-line. You can work on-line. You can learn on-line. You can borrow money on-line. You can engage in sexual activity on-line. You can barter on-line. You can buy and sell real estate on-line. You can purchase plane tickets on-line. You can gamble on-line. You can find long-lost friends on-line. You can be informed, enlightened, and entertained on-line. You can order a pizza on-line. You can do your banking on-line. In some places, you can even vote on-line.
>
> You can perform financial fraud on-line. You can steal trade secrets on-line. You can blackmail and extort on-line. You can trespass on-line. You can stalk on-line. You can vandalize someone's property online. You can commit libel on-line. You can rob a bank on-line. You can frame someone on-line. You can engage in character assassination on-line. You can commit hate crime on-line. You can sexually harass someone on-line. You can molest children on-line. You can ruin someone else's credit on-line. You can disrupt commerce on-line. You can pillage and plunder on-line. You could incite to riot on-line. You could even start a war on-line (Power 2000, pp.3-4)."

Background and Justification

Cyberspace is another extraordinary extension of the human experience. Communication mediated by computer makes it possible to extend the scope of knowledge and to shrink physical distance and time limitations. Particularly, the advent of the Internet has enabled people to express their opinions, causes, and ideologies in more free and convenient ways so that it helps them to turn from a consumer in the process of communication to a producer. As Dominick (1999) mentioned, personal home pages on the World Wide Web make it possible for anyone to be a mass communicator.

With this unprecedented phenomenon, we face new challenges in cyberspace because of malicious computer-mediated-communication producers. Frequent web defacements, computer viruses, or e-mail bombings produced by hackers have been hot issues at both the domestic and international levels. In some areas the interactive cyber-net and the new communication technologies are seen as a means for facilitating anti-social activities which undermine national security and law enforcement and thereby threaten the social formation (Thomas and Loader, 2000).

Dunn (1993) noted 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 (Los Angeles Times, April 3)." Intensive conflicts in the off-line world immediately trigger on-line space battles. This trend is seen in the conflict between Israelis and Palestinians (iDefense, n.d.), between Koreans and Japanese (CNN.com, n.d.), between Taiwan and China (Itsecurity, 2001), between Armenia and Azerbaijan (Rogers, 2000a), and between Chinese and Americans (UPI, October 29, 2002) in cyberspace. Many researchers have reported on this kind of confrontation on the net (Denning, 2001; Taggart, 2001; Paul, n.d.; Gentile, n.d.; Luening, n.d.). Taggart (2001) said, "various transnational groups of hackers and defacers split along nationalistic, religious, and ethnic lines have joined the conflict (p.1)."

In contrast, a great number of hackers do not pay attention to the political possibilities of the net. Rather, they focus on very personal issues, making a game of taunting other web sites and breaking into other computer systems in order to destroy and download individual files and information for enjoyment. Many hacker groups and individual hackers have continued to produce e-mail bombs and computer viruses to disrupt web sites and servers, regardless of the sites' national, religious, or ethnic identity. They are more likely to have "anarchistic interests"(see Jordan & Taylor, 1998).

Although cyberspace gives people tremendous benefits, its shadowy side may deteriorate our social and cultural systems and daily activities. Computer-mediated-communication no longer just entails watching and listening to media content on the Internet. It also extends to stealing information, destroying personal files, and annihilating computer systems. What is worse, hacking, hate crime, and cyber-terror on the Internet can be joined with nationalism, ethnicity, religion, and ideology. This combination can increase the danger and deteriorate existing communication infrastructure.

How can we define, explain, and predict these phenomena? People know that computer hacking is a serious problem in our society, but no one clearly know any reasons why people hack, what makes them attack other countries' government sites, and how they react when they feel threatened by an opponent. Furthermore, there is no concrete theoretic rational to explain hackers activities. Little research has been conducted to deal with this problem. Only a few studies have tried to understand hackers and cyberterrorism in an empirical way because of the difficulty of acquiring data from malicious cyberspace users.

> Most existing studies about hackers and cyberterrorism are based on interviews with a few former computer hackers, newspaper articles that report cyber crimes and warn about possible cyber-terrors, and surveys from the computer security business. There are only a few empirically-based research studies administered by government, congress, and business. Consequently, it is hard to generalize computer hacking impact on society and to explain why hackers are involved in hacking activities without direct data from hackers. This point emphasizes the lack of

> generalizability in describing, explaining, and predicting the hacking phenomenon and its impact on people, society, and culture. In order to solve this problem, this study will obtain data directly from hackers, and use more appropriate theoretical concepts to examine the reasons why they are involved in these antisocial behaviors in cyberspace. Because hackers have collective identities that are complicated psychological mindsets (e.g., some hackers are involved in this activity for some ethical reasons but others do it for unethical purposes), several theoretic rationales that help to understand hackers and hacking are needed. Accordingly, this study will draw upon several theories from social psychology.

Purpose of the Study

This study will use an online-survey in order to investigate hackers' psychological structures and then how these have an influence on hackers' aggressiveness and hacking intention against those in other nations. Specifically, this study tries to 1) assess the relationship between hackers' levels of narcissism and their aggressiveness (e.g., angry temperament, angry reaction, and angry behavior), 2) explain what makes hackers get involved in hacking activities by investigating their motivations, 3) investigate what makes hackers keep breaking into other computer systems and what factors in hackers psychological structures affect hacking using the concept of flow, and 4) explore, using terror management theory, how hackers react when they feel a threat to their own cultural worldviews.

Because hacking is a crime and little research exists, the first part of research by necessity will be descriptive and exploratory. The next stage will be explanatory and will investigate the relationships among self-esteem, motivations, aggressiveness and hacking behaviors. As a result, this study mainly focuses on hackers' psychological mindsets as producers of computer-mediated-communication. Through this study, we may gain insightful clues why hackers try to deface web pages, break into computer systems, and contaminate cyber properties with computer viruses. In addition, this study will examine how other factors (i.e., nationalism, religion, or other variables) are mixed with hacking activities.

Chapter Organization

1) Chapter I introduces the justification and provides the purposes of this study.
2) Chapter II reviews the literature about previous studies, journals, and articles related to hacking issues and its impacts on people, society, and culture in both the domestic and international levels.
3) Chapter III provides a various theoretic rationales (specially from social psychology) to delineate hackers' psychological mindsets and their activities.
4) Chapter IV describes methodology: data collection, sampling, instrument and operationalization of independent and dependent variables in this study.
5) Chapter V summarizes the research findings.
6) Chapter VI provides a discussion of the implications of this study, limitations, and suggestions for future research.

CHAPTER 2

REVIEW OF LITERATURE

Media industries, particularly, film and television have portrayed hackers and cyberterrorism in a stereotyped way. Hackers in television programs, books, movies and newspaper/magazine articles are generally depicted as the technical wizards and as subversive technological whiz-kids. Hollywood provided people with the fearful image of cyberterrorism through *Die Hard II, Sneakers, War Games,* and *The Net* (Taylor, 1999). According to previous studies, journals, and speculations about hackers and cyberterrorism from academy, government, and business, unlike media portrayals of hackers and cyberterrorism, many differences were found in hackers. Although the findings were not consistent among studies related to hackers' psychological mindsets, misrepresentation and exaggeration by the media does not help understand the hacker community.

Some studies using self-report surveys have observed that hackers perceive themselves as loners, psycho-sexual perverts, under-achivers, socially inept, and the products of dysfunctional families (Chantler, 1996; Post, 1996; Taylor, 1999). On the other hand, other researches noted that a demographic description of the hacker is not sufficient to explain hackers' motivation engaging in criminal activities (Goodel, 1996; Hafner & Markoff, 1995; Littman, 1997). Rather, Woo, Kim and Dominick (2002) reported that hackers were actively communicating with their co-workers in cyberspace and shared valuable resources, information, and techniques with other members.

Furthermore, they tend to avoid sexually explicit content, and a large number of hacker groups positively participate in political activities. In addition, Rogers (2000b) noted that hackers even hold conventions in Las Vegas[1] in order to exchange ideas, techniques, and intelligence. Hacker specific newsgroups, chat channels, and periodicals (i.e., *2600 Magazine*) have been established.

Regarding the motivation for hacking, Post (1996) claimed that hackers were motivated by the challenge, the excitement to succeed, and a desire to learn for the pure intellectual satisfaction whereas some hackers were propelled by vengeance, sabotage, and fraud. Rogers (2001) suggested that individuals who had engaged in criminal computer activities would have higher rates of moral disengagement than individuals who had no criminal activity. In contrast, Denning (1990) maintained that most hackers are not intentionally malicious. Voiskounsky, Babaeva, and Smyslova (2000) argued that "hackers are intellectually curious, smart, good learners, aggressive, self-assertive, risky, disdainful towards lamers, possibly perverted in moral norms, have a peculiar mixture of cosmopolitan and patriotic views, poor communicators and polemicists, and devoted to cyberspace problems while having strong interests in real life (p. 82)."

Therefore, one-dimensional explanation concerning hackers and their activities as the media depict might provide us with the wrong impression and distorted understanding. According to Rogers (2000), "the current method of categorizing all persons involved in various computer specific criminal activities into the one generic category of hackers holds little utility (p.23)." More sophisticated and in-depth

[1] Defcon is a yearly hacker convention held an each summer in Las Vegas, Nevada. Hackers from all over the world participate in this convention. In addition, there are several mini-conventions such as ToorCon 2k++ (held at the San Diego Concourse), Cuervocon (held at Laredo, Texas), @LANtaCON (held in Atlanta, Georgia), and Rubi Con (held in downtown, Detroit) (www.DEFCON.com, 2001, September 12).

descriptions, explanations, and predictions will be needed to cover the diverse characteristics of hackers.

Diverse Profiles of Hackers

According to Rogers (2000d), "hackers are not a homogeneous group (p.1)" In addition, "there is no generic profile of a hacker (p.14)." Voiskounsky et al. (2000) claimed that hackers derive from the heterogeneity of the population of the hacker community in Russia. Many researchers tried to categorize hackers into several sub-groups depending on diverse characteristics (see Rogers, 2000b). This section introduces several subcategories of hackers made by some researchers from Rogers's (2000b) taxonomy of hackers.

Landreth (1985) defined the hacker community as novice, students, tourists, crasher, and thief based on the activities hackers were involved in. The novice is thought to be the least experienced and the person who makes petty mischief. The student group is considered those who easily get bored and are unchallenged at school and who try to explore others' computer systems at home. The tourist group wants to test their skills and experience the thrill of breaking into other computer system. This activity is out of a sense of adventure. The crasher's main purpose to commit hacking is to damage information and system intentionally whenever they are involved in hacking. The thief group makes monetary reward from their activity.

Hollinger (1988) claimed that people involved in hacking activities should fit into three categories: pirates, browsers, and crackers. The pirates have a low level of hacking techniques. They are limited to pirate computer software. The browsers have middle level of technical ability and are able to access to individuals' personal files. They usually don’t destroy files. The crackers have the best hacking techniques and are considered the most serious abusers.

Goodell (1996) maintained that hackers can be divided into three groups: hackers, crackers, and phreakers. Hackers are involved in hacking to obtain knowledge and satisfy intellectual curiosity. Crackers usually commit destruction, vandalism, and defacement on web pages. Phreakers are mainly interested in manipulating and attacking the telephone system.

Chandler (1996) categorized hackers into four different generations. The first generation of hackers was smart and techno-oriented students, programmers, and computer scientists from MIT. They were interested in hacking for academic and professional curiosities. The second generation of hackers was more likely to be technological radicals. They made “blue boxes” that allowed a person to get long distance telephone service without charge. The third generation was young people who were really crazy about personal computer and computer games. To get game software protected by secret codes freely, these hackers tried to find ways of breaking the copyright codes. The fourth generation of hackers has some criminal activities triggered by greed, power, revenge, or some other malicious intent.

Chantler (1996) categorized hacker groups into three sub-groups: elite, neophytes, and losers (lamers) based on hackers’ attributes such as hackers’ activities, their prowess at hacking, their knowledge, motivation, and how long they had been hacking. The elite group has a high level of hacking techniques and desires to achieve self-discovery and enjoys the excitement and challenge. The neophytes have moderate level of hacking skill and still learn more knowledge about hacking. The losers (lamers) don’t have intellectual knowledge and mainly use hacking skill for a desire for profit, revenge, theft, and espionage.

Power (1998) indicated that hackers can be categorized into sport intruders, competitive intelligence, and foreign intelligence. The sport intruders break into computer servers, deface web pages, and damage files. The competitive intelligence try to avoid illegal hacking and unethical activities and mainly fall into the realm of competitive espionage (Rogers, 2000b). The foreign intelligence are involved in hacking activities for the purpose of a nation's security or economic interests.

Parker (1998) subdivided hackers into seven profiles of cybercriminals: pranksters, hackersters, malicious hackers, personal problem solvers, career criminals, extreme advocates, and malcontents, addicts, and irrational and incompetent people. Pranksters are referred to people who perpetrate tricks on others. They seldom inflict harm on others. Hacksters explore others' computer systems because of curiosity, competition, or social justice. Malicious hackers are similar to crackers. Personal problem solvers intend to solve personal issues through hacking when they fail to solve their problems. Career criminals use hacking skill in order to obtain some income. Extreme advocates are considered cyberterrorists. They have strong social, political, and religious views. Malcontents, addicts, and irrational and incompetent people are mentally ill.

Adamiski (1999) noted that hacker community has a loose hierarchy, and this is composed of the elite, ordinary, and darksiders. The elite has a high level technique so that they can make software and attack tools. The ordinary hacker group is similar to crackers. They are involved in breaking into computer systems and attacking telephone company computer switches. The darksiders are engaging in financial gain through hacking.

Rogers (2000b) classified the hacking community in seven distinct categories: newbie/tool kit (NT), cyber-punks (CP), internals (IT), coders (CD), old guard hackers (OG), professional criminals (PC), and cyber-terrorists (CT) depending upon level of technical ability. The NT has limited computer skills and use tool kits[2]to conduct attack. The CP category is made up of hackers who usually have better computer skills. They can make basic levels of their own software; they also intentionally engage in defacing web pages or send “Spam” mails. The IT category consists of persons who have worked in the computer industry. Because they have relatively high computer skills, they are able to carry out hacking easily. The OG category is similar to the first generation of hackers. They are interested in intellectual curiosity and have no criminal intent. The PC and CT groups are well trained and are the most dangerous group in hacking community. They specialize in corporate espionage to have access to state.

The diverse descriptions of hackers were based upon data from the content of the popular media, self report surveys, or personal observations (Rogers, 2000d). Rogers (2000d) noted that previous studies “relied on the subject’s own classification as a hacker with no corroborating evidence (i.e., arrest record) (p.1).” Actually, most studies divided hacker communities into sub-categories depending on their subsequent consequences after they engaged in hacking activities whereas a few research categorized them into subgroups by motivations, levels of technique, and generations. Rogers (2001) reported that “the researchers have been criticized for relying heavily on interviews and the

[2] The tool kits are readily available on the Internet. With this software, less experienced hackers can have unauthorized access.

subjects' own self-classification as a computer criminal or hacker (p.60)." Some theoretical models are needed to explain hackers' psychological mindsets. This study seeks to provide the theoretic rationales to understand hackers and their impact on people, society, and culture. In Table 2.1, the hacker communities can be broadly differentiated into non-malicious and malicious (shaded cells on table 2.1). If this study successfully supports some theoretic models to explain why hackers break into computer systems, what makes them involved in hacking, and what factors affect hacking against others, we may predict who is going to participate in hacking and what hacking activities they might engage in.

Table 2.1. Summary of Hacker's profile suggested by previous studies

Landreth (1985)	Holliger (1988)	Goodell (1996)	Chandler (1996)	Chantler (1996)	Power (1998)	Parker (1998)	Adamski (1999)	Rogers (2000)
Novice	Pirates	Hackers	First generation	Elite group	Sport intruders	Pranksters	The elite	Newbie/tool kit (NT)
Student	Browsers	Crackers	Second generation	Neophytes	Competitive intelligence	Hacksters	Ordinary	Cyber-punks (CP)
Tourist	Crackers	Phreakers	Third generation	Losers & lamers	Foreign intelligence	Malicious hackers	Darksiders	Internals (IT)
Crasher			Fourth generation			Personal problem solvers		Coders (CD)
Thief						Career criminals		Old guard hackers (OG)
						Extreme advocates		Professional criminals (PC)
						Malcontents, addicts, and irrational & incompetent people		Cyber-terrorists (CT)

Note. The shaded profiles are hackers who have malicious purposes.

The Motivation of Hackers

What makes individuals hack, crack, and deface other web properties? One hacker claimed that his reason was "to seek knowledge, discover something new, be the first reason to find a particular weakness in a computer system or the first to be able to get a certain result from a program" (e.g., Emmunual Goldstein, interviewed by CNN.com, n.d.a). Denning (1999) reported that the thrill of illicit behaviors, excitement, and challenge is the main reason for hacking. Meanwhile, like the case of E.H.A.P (e.g., *Ethical Hackers against Pedophilia*-http://www.ehap.org), some hackers seek out and stop the exploitation of children on the Internet. A number of hacker groups want to maintain cyberspace as a free playground and argue that information should be free (Levy, 1984). Because they object to the control and monopolistic power from transnational corporations and governments in cyberspace, they try to sustain cyberspace as an unlimited, anti-commercial, and deregulated realm where information should be shared without any monetary compensation. Therefore, they frequently break into transnational companies' computer systems and disclose passwords for all computer users to freely access important software sources or new computer programs in the main computer systems of these companies (i.e., Microsoft, Sony, Nokia, etc.). On the other hand, although some hackers tend to show negative attitudes toward transnational companies, others try to make good money by stealing information from those companies (Shaw, 2001).

Further, patriotism catalyzes hacking in behalf of the hackers' country (Denning, 2001). Some scholars have noted that hacking activities are propelled by nationalism (Dunn, 1999; Gentile, 2001; Luening, 2001; Taggart, 2001). Hackers who have certain cultural worldviews concerning religion, ethnicity, and nationalism are enthusiastically involved in attacking web sites and computer systems of opposing sides. According to Woo and his colleagues (2002), their research findings indicated that about 20% of the sample in their content analysis of defaced web pages belonged to politically motivated web defacement (e.g., defaced web pages on account of nationalism, ethnicity, and religion). Taylor (1999) claimed that political acts could be one of possible motivations why engaging in hacking.

Another reason for hacking is that hackers try to inform other hacker communities in order to provide valuable information, techniques, and as a source for sustaining friendships in hackerdom. Furthermore, hackers often hack in groups. Unlike popular mythology, hackers are not "solitary individuals" who are more comfortable relating to machines than to other humans (Jordan & Taylor, 1998). 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 (p.2)." These greetings for peer hackers or hate statements against rival hacker groups on defaced web pages are evidence that hackers try to align themselves with or against other hackers depending on their ideology, agenda, or issues.

Raymond (2001) maintained that to be a hacker, a person must get a thrill from solving problem, sharpening skills, and exercising intelligence. Some hackers try to put some words and images on others' web pages to impress their boy/girl friends (Itworld.com, n.d.).

According to Rist (1998), a prime motivational factor for hacking is "a mixture of ego and political commentary (p.1)." He 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." Not surprisingly, hackers often brag and show loopholes in the site to webmasters thus proving that they are better technocrats than are those who manage the web site. Woo and his colleagues (2002) noted that hackers tend to leave their purpose why they deface, who did it, greetings for peer hackers or hate statement, and bragging remarks on the defaced web pages. Dominick (1999) noted that people use personal homepage as a way of self-presentation by including some features such as a feedback mechanism, links to other sites, likes/dislikes, and opinions, etc. on their web pages. In turn, hackers use web sites which others possess in a way of adverse-presentation against others by defacing original web pages and then replacing them by images and texts of the hacker's choice.

Cyber-Wars and Cyber-Protests

> "America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb (Pollitt, 2000)."

Modern societies are definitely dependent upon the development of computers, the Internet, and new communication technologies such as fiber-optics, satellites, and cell phones. These new vehicles provide us with a chance to access and participate in the affairs of government, business, education, religion, international relations and culture. Through technology, people are able to share, exchange, or send their opinions, data, and graphics to one another. People can communicate with others on any agenda by way of one-on-one or one-on-multiple arrangements regardless of time and distance. In spite of the new benefits, the more society relies on a computer system, the more it faces the danger of hacking. Hacking techniques are no longer limited to the person who has high tech-oriented skill. It is true that anyone can possess hacking tools that are freely available through the Internet (Rogers, 2000c). Because of the new communication environment, we face a new type of conflict in cyberspace between people, organizations, and nations as we saw historically on the earth, ocean, sky and space.

In describing this phenomenon, futurists, researchers, policy makers, and writers have coined new terms such as information warefare, infowar, information operations, strategic information warfare, Internet war, cyberwar, cybotage, netwar, cyber-attack, Cyber-Conflict, Digital Revolt, etc (Denning, 1999; Libicki, 1995; Arquilla & Ronfeldt, 1997; Arquilla & Ronfeldt, 2001; Belcher &Yoran, 2002; Taggart, 2001; Waltz, 1998). Although there are some variations in jargon, in general, these terms indicate that political conflicts in cyberspace can occur between people, organizations, and states. Denning (2001) characterized this phenomenon as three different levels: activism, hactivism, and cyberterrorism. She explained that

> "Activism refers to non-disruptive use of the Internet in support of an agenda or cause. Operations in this includes browsing the web for information, constructing web sites and posting materials on them, transmitting electronic publications and letters through e-mail, and using the Net to discuss issues, form coalitions, and plan and coordinate activities. Hacktivism refers to the marriage of hacking and activism. It covers operations that use hacking techniques against a target or multi-targets Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are Web sit-ins and virtual blockades, automated e-mail bombs, Web hacks, computer break-ins, and computer viruses and worms. Cyberterrorism refers to the convergence of cyberspace and terrorism. It covers politically motivated hacking operations intended to cause grave harm such as loss of life or severe economic damage. An example would be penetrating an air traffic control system and causing two planes to collide (p. 2)."

According to Denning (2001), even if these three categories are different, their boundaries are blurry. Nonetheless, the three terms cover all kinds of political conflicts in cyberspace.

1) Activism

By means of the Internet's ubiquity, people can reach each other and use the Internet to promote an agenda. The members and supporters, from any geographical region on the Internet, who pursue the same opinion are able to put together and wield their power in order to support their cause and to have an influence on foreign policy that they don't like. They are able to publicize their issues through the Internet using such techniques as collection, publication, dialogue, coordination of action, and direct lobbying of decision makers (See Denning 2001). For instance, e-mail demonstration from the South Koreans on the short-track speed skating in 2002 Salt Lake Winter Olympic game[3], NGO's battle in Seattle[4], the Internet promoting democracy in Burma[5] and the Kosovo conflict[6] belong to the activism category. Through the Internet, people who support or object to an agenda group together and propagandize their issues just like demonstrators with picket signs on a square.

[3] South Koreans, angry after Kim Dong Sung was disqualified in the men's 1,500 short-track speedskating, and the gold medal awarded to American Apolo Anton Ohno sent e-mails to the United State Olympic Committee with 16,000 messages and threats to Ohno. Consequently, this activity forced the USOC to take down its Internet server. This was turned over to the FBI for investigation (Jenkins, 2002; News Services, 2002).

[4] To demonstrate against the WTO, a confluence of loosely organized social activists converged on the sessions in both physical and cyber space. As a result, the WTO sessions and ceremonies were disrupted, and police credibility was challenged, particularly as the demonstrations were seen on global television and simultaneous demonstrations spilled over in cities across the globe (Sullivan, 2001). The Battle in Seattle provides us with the point that anti-government groups are establishing alliances and coalitions in terms of providing a central place where the times and locations of protests and meetings can be posted, moreover, demonstrations can be coordinated through the Internet in real time-based (Denning, 2001).

[5] Burmese and non-Burmese activists form the United States as well as from Europe and Australia joined a long-standing effort to bring democracy to Burma. Their global campaign raised constitutional and national policy questions in the United States. Finally, in April 1997, President Clinton signed federal legislation banning any new investment by U.S. companies in Burma (Danitz and Stroble, 2001).

[6] During the Kosovo conflict, organizations and individuals throughout the world used their web sites to publish information related to the conflict and, in some cases, to solicit support. Non-government organizations with Kosovo-related web pages included the press, human right groups, humanitarian relief

2) Hacktivism

With the help of hacking tools (i.g., BackOrifice2K, Rootkit, COPS, SATAN, and PRIES), hackers can block computer servers and overload their traffic. Rogers (2000c) noted that intrusive hacking tools are freely available through the Internet, and the level of technique has become sophisticated and is getting easier to understand. According to Denning (2001), hackers visit their target sites and generate so much traffic with hacking tools against the site that other Internet users cannot reach it (i.e., Strano Network,[7] EDT,[8] NATO's Accidental bombing of China embassy,[9] cyberwar between China and Taiwan[10]).

3) Cyberterrorism

Pollit (2000) defined cyberterrorism as a politically motivated attack against an information infrastructure such as computer systems, computer programs, and data which result in violence against noncombatant targets by subnational groups or clandestine agents. Collin (1997) noted that cyberterrorism is the union of cyberspace and terrorism, and expected that politically motivated hacking attacks in cyberspace could cause serious

organizations, churches, and women groups. Their stories told of fear and devastation, the latter caused no only by the Serb military, but also by NATO bombs (Denning, 2001; Arquilla & Ronfeldt, 2001).

[7] On December 21, 1995, A group go by itself Strano Network launched a one-hour Net-Strike attack against the Web sites operated by various government agencies. At the appointed hour, participants from all over the world were instructed to point their browsers to the government web sites. Some of the site were effectively down for the period (Denning, 2001).

[8] In 1998, The Electronic Disturbance Theater (EDT) organized a series of Web sit-ins against Mexican President Zedillo's web site and later against President Clinton's White House web site, the Pentagon, the School of the Americas, the Frankfurt Stock Exchange, and the Mexican Stock Exchange (Denning, 2001).

[9] In May 1999, NATO accidentally bombed China's embassy in Belgrade. Angry Chinese hackers cracked several U.S. government web sites (Denning, 2001).

[10] In August 1999, Chinese hackers defaced several Taiwanese and government web sites with pro-China messages saying Taiwan was and would always be an inseparable part of China. Taiwanese hackers retaliated and planted a red and blue Taiwanese national flag and anti-Communist slogan on a Chinese high-tech Interent site (Denning, 2001).

harm, such as severe economic chaos, loss of power or water, and damage to life. For example, cyberterrorists can break into air traffic control systems, nuclear plants, dam control computer systems, 911 emergency system,[11] etc. They may turn the computer control devices off or put computer viruses into the main servers in order to contaminate all systems. President Clinton's Commission on Critical Infrastructure Protection (1997) warned that infrastructures such as telecommunications, banking and finance, electrical power, oil and gas distribution and storage, water supply, transportation, emergency services and government services were potentially vulnerable. However, there has been no evidence of a true cyberterrorist attack (Denning, 2001).

A Mixture of Activism, Hacktivism, and Cyberterrorism

Although Denning subdivided all types of cyber-conflicts into his three categories, in fact, politically motivated hacking cases convey all three characteristics. Combined and convergent strategies (e.g., hacking + demonstrating + propagandizing + writing computer viruses) were frequently used in cyber-conflicts such as NGO's net-war in Seattle, Zapatista's social activities against Mexico government, and Kosovo conflicts. Until now, however, chaos under cyberterrorism has not been appeared.

Notwithstanding, the potential symptom is apparent, particularly regarding conflicts in the Middle East, Asia, and East Europe. Woo *et al.* (2002) maintained that political and military battles between nations may affect cyber conflicts between two or more sides. This phenomenon tends to be intertwined with nationalism, patriotism, Nazism, extreme-foundationalism or anarchism. Taggart (2001) noted that transnational

[11] A Swedish hacker jammed the 911 emergency telephone system throughout west central Florida. FBI Director Louis Freeh called the incident " a dress rehearsal for a national disaster (Computer Law Tip of the week, 1999)."

hacker and defacer groups[12] divided by nationalistic, religious, and ethnic identity have joined the conflict to fight one another on behalf of supporting sides. According to Woo (2003), nationalism-oriented hackers use their web defacement skills to disrupt opponents' servers and propagandize their causes with hate statements against the enemy. Many examples demonstrate this phenomenon: the controversies between Korean and Japanese governments about distorted history textbooks in Japan compelled many Korean hackers to attack Japanese government official web sites and to take down several newspapers' computer severs that supported Japanese government policy (CNN.com, n.d.); After the conflict between America and China[13] about a U.S. spy plane crash in a Chinese area, there was intensive hacking between two sides (Cha, 2001).

Because of the magnitude of cyber war, nations are increasingly aware that the use of cyber strategies can act as military power. Shimeall, Williams, & Dunlevy (2001) claimed that "smaller countries that could never compete in a conventional military sense with their larger neighbors can develop a capability that gives them a strategic advantage (p.16)." Cyber attacks under a war situation are a very attractive and effective strategy to many foreign entities because it is a low-cost alternative and can damage the opposite side with real violence and chaos (The Center for the Study of Technology and Society, 2001). Since powerful countries recognize the possibility of cyberwar, they have prepared for new types of military strategy. For example, in the U.S., the federal government has already created special offices to protect critical systems against cyber attack (The Computer Law Tip of the Week, 1999), In Japan, the Defense Agency

[12] Pro-Arab hacker groups: the World's Fantablous Defacers (the WFD), the Silver Lords, Gforce Pakistan; Pro-Israeli hacker groups: the m0sad team, InfernoZ; Pro-Korean Hacker groups: 815hackers.

developed computer systems to combat attempt by hackers to disrupt the country's defense operation, and the Japanese government organized a squad to handle anti-hacker and anti-virus schemes (The Japan Times, Oct 24, 2000). China also has accelerated its capability to carry out Information Warfare (U.S. Defense.com, May 10, 2000).

Woo and his colleagues (2002) reported that politically motivated-defaced web pages (e.g., web defacement activities triggered by a certain ideology) contained more propagandistic information and content than the apolitical type of defacement due to the fact that hackers who have a specific cultural worldview, when they feel threats from others, or when they are pressured by those who don't share the viewpoint, tended to erase the offending content and insert their own views in order to recover their self-respect and feel safe.

According to Collin (1997), there are many hundreds of significant extremist sites, from anarchists on the left to militias on the right, to religious, political, and ideological extremists in every direction imaginable. These groups can effectively distribute propaganda in multimedia ways. Therefore, we infer that conflicts between nations, religions, and ethnicities in real world will happen in the on-line world. Furthermore, because diverse political groups such as Hitlerites, Pakistani nationalists, pro-Israel groups, radical environmentalist, anti-capitalist, and anti-porn activists, etc. continue to build their own web sites as a public sphere for their causes, these phenomenon may also promote the cyberwar between opposing sides.

[13] A Chinese group known as "hong ke red" guests is spearheading a cyber-war campaign to avenge the death of fighter pilot Wang Wei, who died in the US spy plane crash (Itsecurity, 2001).

Relevant Researches on Hackers

Very little study has been conducted to describe, explain, and analyze hackers and their activities. Recently, with the increasing alarm about hacking issues, a few descriptive empirical research studies on cyber attack, hacking, and computer crime have appeared. One report indicated that the rate of attack activity increased substantially between July and December 2001 (Riptech,[14] 2002). Average attacks toward a business company increased by 79% in this period. A substantial percentage of attacks appeared to be deliberately targeted at a specific organization (39% of attacks appeared to be a deliberate attempt to compromise a specific target system or company; 61% of attacks appeared to be opportunistic in nature). The vast majority of attacks were launched from a small number of countries. Ten countries were the source of approximately 70% of all attacks against the sample.[15] Different industries suffer significantly different rates of attack intensity and severity. High Tech, Financial Services, Media/Entertainment, and Power and Energy companies showed the highest intensity of attacks per company.[16] Power and Energy companies suffered attacks from the Middle East at a rate that was more than three times greater than the mean for all companies in the sample set. High Tech and Financial Services companies suffered attacks from Asia at a rate that was 55-

[14] Riptech, Inc is the one of premier provider of scalable, real-time managed security service. Riptech's Internet Security Threat Report offers a broad quantitative analysis of Internet-based attacks targeted at hundreds of organizations during the last half of 2001. Because of the large sample size of the organizations studied (selected from Riptech's client base), the trends presented in this report provide an overall indicator of threats faced by the entire Internet community.

[15] The United States (29.6%), South Korea (8.8%), China (7.8%), Germany (5.9%), France (4.5%), Canada (3.9%), Taiwan (2.6%), Italy (2.5%), Great Britain (2.5%), Japan (2.0%). About 50% of attacks come from U.S., South Korea, and China. In terms of the number of attacks launched per Internet user, Israel was by a wide margin the largest source of attack activity. Five of the top ten attacking countries are located in the Pacific Rim.

[16] Power and Energy companies suffered severe attacks at a rate that was more than twice the man of all companies in the sample set.

70% greater than the mean for all companies in the sample set. Attack intensity and intent varied depending on company size and based on ownership type.[17]

Woo et al.'s a content analysis on defaced web pages (2002) indicated that about 24% of the defaced web page in sample were owned by the U.S., and 49% of samples belonged to "dot com" domain. All targeted web pages were totally defaced by hackers (only 4% of the sample was changed in a partial way). According to their research findings, hackers tend to put the reason why they deface and write new contents on the web page (about 72% of the sample). The most frequent reason why hackers break into and change web pages was "just for fun" (27% of the sample which deliberately put the purpose).[18] Hackers are also likely to publicize their pseudo-identification (i.e., krAzy, IdIot, gO_rOOr, WFD, ConClaveCrew, Hi-Tech Hate, and cDc) on the defaced web pages in order to let others know who did it. About 92% of the sample contains attackers' name. Half of hackers in the study put "fuckz," "greetz," "props," or "shout out" to their rivals or cyber-friends who align with them. In addition, politically motivated hackers defaced a target web page in more aggressive ways than hackers who didn't have any cultural viewpoint (driven by nationalism, religion, or ethnicity).

Parker (1998) noted that people involved in computer crime may have different levels of skill in formal education, social interactions and use of computer systems. Their

[17] Companies with greater than 500 employees suffered at least 50% more attacks per company than companies with fewer than 500 employees. Attackers are slightly more likely to launch targeted attacks against companies with more than 1,000 employees than companies with less than 1,000 employees. Public companies suffered approximately twice the number of attacks per company as private and nonprofit companies.

[18] On these defaced web pages (defaced as just for fun), this study frequently found that "your site is defaced, owned, or hacked by me (mainly hackers' group name) because I like it," followed by no-purpose (24%), nationalism (10%), checking security (9.6%), bragging skills (7.7%), ethnicity (7.4%), the freedom

motivations include greed, need, desensitization of the harm done to others, personification of computers, the Robin Hood syndrome (stealing from the rich is morally justified). Many hackers believe that breaking into computer systems without theft, vandalism or obvious breach of confidentiality is a harmless and an ethically acceptable hobby. Most active hackers are young males aged 12 to 24 years old.

A CSI's report[19] (Computer Security Institute, 2001) highlighted that 64% of the sample acknowledged financial losses due to computer breaches and 35% (186 respondents) reported $377,828,700 in financial losses.

Kabay (2000) summarized that a variety of studies survey findings of computer crime. However, most studies are based on security companies' reports and government investigations.

Very little survey research has been directly conducted on hackers and the persons who are willing to be hackers. In fact, hacking operations: cyberwar, cyberterrorism, cyberconflicts, etc. are frequently carried out at personal, business, national levels. However, we are not quite sure what factors in each level are related to hacking activities. In this sense, a logical and consistent theoretic rationale to describe, explain, and predict hacking activities and hackers' psychological mindsets is needed.

of information (3.4%), multi-purpose (1.9%), stopping porn site (1.7%), lover (1.5%), and religion (1.3%), and others (2.6%).

[19] The Computer Crime and Security Survey is conducted by CSI with the participation of the San Francisco Federal Bureau of Investigation's (FBI) Computer Intrusion Squad. The purpose of this survey is to raise the level of security awareness, as well as help determine the scope of computer crime in the United States. Based on responses from 538 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities, the findings of the "2001 Computer Crime and Security Survey confirm that the threat from computer crime and other information security breaches continues unabated and that the financial toll is mounting (CSI, 2001).

CHAPTER 3

THEORETIC RATIONALE

Although many researchers, journalists, and government officials tried to explain hackers and their antisocial activities, most findings seemed to be based on non-theoretic and intuitive approaches. Rogers (2000; 2000b; 2001) has criticized the lack of theoretical explanation concerning hackers and their impact on society. Accordingly, this research uses several theoretic rationales to explain how hackers' personalities affect their aggressiveness, what motivations prompt hackers to be involved in hacking activities, why they keep breaking into computer systems, what makes them fall in love with hacking, and how they respond when they face any threat about their cultural worldviews. This chapter examines the concepts of self-esteem, motivation, flow, and terror management theory. Although these theoretic models are referred to in different terms, they are somewhat intertwined.

Self- Esteem

The concept of "self" is rooted in universal human experience of reflexive consciousness,[20] interpersonal being,[21] and executive function[22] (Baumeister, 1999).

[20] "The conscious human mind can turn its inquiring attention back toward its own source and seek the self. The self is not known directly but either observed in action or interred from social events (p. 2)." In other word, this implication can be considered as self-awareness: people are able to become aware of themselves.

[21] The self is a member of groups and relationships, and indeed one of the crucial functions of the self is to enable people to relate to others (p. 2)." People realize their self in terms of connections from social communities such as family, culture, gender, etc.

[22] "This enables the self to make choices, initiate action, and exert control over self and world (p. 2)" This aspect of self encompasses on autonomy, self-regulation, and decision-making, and the quest for control.

Because “self” is such a complicated and multidimensional concept, applying the concept of self to this study is too broad and complicated to explain hackers’ activities, and it is difficult to assess its structure (Mruk, 1995). To narrow down the research scope, this study adapts “self-esteem” as a reflective consciousness aspect of the self.

Social psychologists have noted that antisocial behaviors can be explained by the structure of a person’s self-esteem (Baumeister, Smart, & Boden, 1996; Kernis, 1993). Traditional self-esteem assumptions indicated that people with low self-esteem tend to be involved in more antisocial behaviors than ones with high self-esteem.

Previous studies concerning self-esteem claimed that people with low self-esteem are less likely to have a strong, consistent, confident, and stable personality of self-knowledge than people with high self-esteem, and they suffer from a chronic condition of negative affect, feelings of inferiority, unworthiness, loneliness, and insecurity (Mruk, 1995). Furthermore, people with low self-esteem act violently and cause all manner of violence (Staub, 1989; Gondolf, 1985; Long, 1990; Oates & Forrest, 1985; Schoenfeld, 1988; Anderson, 1994; Renzetti, 1992; Jankowski, 1991).

On the other hand, people with high self-esteem are less vulnerable against internal and external impacts such as criticism, negative feedback, anxiety, deviant behaviors and persuasions (Campbell, 1990; Plummer, 1985; Mruk, 1995; Campbell & Lavallee, 1993; Shrauger & Rosenberg, 1970; Brown, 1993; Wells & Marwell, 1976; Blaine & Crocker, 1993).

However, this rationale has been controversial. The traditional assumption that social psychologists had believed for a long time has been modified by a series of research findings. Baumeister (1999) pointed out “researchers have not found that most people with high self-esteem are so cheerfully indifferent to insults, criticism, or disrespect (p. 243)." Also, he provided abundant research findings that people with high self-esteem behave in an irrational manner (Baumeister & Tice, 1985; McFarlin & Blascovich, 1981). There were many contradictions, inconsistencies, and ambiguities in the traditional relationships between low self-esteem and antisocial behaviors (e.g., see California Task Force,[23] 1990).

Subsequently, a large volume of studies has shown that people who have high self-esteem are more likely to behave violently than a low self-esteem group. Rather, people with low self-esteem tend not to participate in risk situations; they try to avoid the situation because they are passive to it. A revised rationale suggests that a person who has high self-esteem but an unstable status acts more aggressively against others than a person who has high self-esteem and stable status. People with high self-esteem and stable status are not vulnerable to negative feedback from others.

1) A turning point in a traditional assumption of self-esteem

An opposite point of view has been offered as an appropriate explanation to the relationship between self-esteem and violence. Baumeister, Smart, and Boden (1996) noted that aggressive people are more likely to have favorable opinions of themselves and, in fact, violence often is triggered when these favorable views to self are attacked. Unlike the traditional assumptions of self-esteem, many researchers found different results: people with high self-esteem tend to have a more hostile attitude when they face negative feedback than do people with low self-esteem; low self-esteem is a poor

[23] In terms of raising children's self-esteem, the program tried to reduce in the rate of crime, delinquency, drug abuse, unwanted pregnancy, underachievement in school, etc. However, the evidence has been doubted (Baumeister, 1999).

predictor of aggression (Bushman & Baumeister, 1998; Baumeister *et al*, 1996; Colvin, Block, & Funder, 1995; Kernis, Granneman, & Barclay, 1989).

To account for these inconsistent results, researchers assumed that people with high self-esteem and self-worth have immunity to ego threats so that they are able to ignore them. However, people with high self-esteem based on egotism (e.g., self-appraisal) can lead directly to violence because self-appraisal is so sensitive to ego-threats. Baumeister, *et al*. (2000) explained that high self-esteem might be a continuum where one side is very non-aggressive, and the other is quite aggressive. These previous research findings do not indicate that all people with high self-esteem act violently but, some people with high self-esteem and with an unstable status (e.g., ego-centric, narcissistic, and inflated sense of self-worth) tend to behave aggressively when they feel external negative feedback. Baumeister (1999) noted that "violent and criminal individuals have been repeatedly characterized as arrogant, confident, narcissistic, egotistical, assertive, proud and the like (p.271)."

Baumeister *et al*. (2000) maintained that narcissism seemed not so much as a direct cause of aggression but a risk factor that can contribute to increasing a violent response to provocation. Therefore, when people who have narcissistic views about themselves are questioned, contradicted, or disputed, they may aggress against the source of the threat in order to protect their ego (Baumeister, 1999).

According to Woo et al. (2002), hackers are more likely to have narcissist-oriented attributes. A content analysis on defaced web pages indicated that hackers tend to leave bragging remarks and their nicknames on target web pages in an attempt to be admired among other hacker communities and for informing the media who did the hacking.

Often they use pseudo-identifications, such as hacker group's names, that show their superiority over others. Post, Shaw, and Ruby (1998) noted that they found a lack of empathy from computer intruders, and concluded that this factor was an indicator of narcissistic and antisocial personalities. Other researchers reported that people engaging in hacking have a proclivity to show off their exploits (Rogers, 2001, Chandler, 1996; Denning, 1998; Parker, 1998; Rist, 1998).

"Narcissism is defined by grandiose views of personal superiority, an inflated sense of entitlement, low empathy toward others, fantasies of personal greatness, a belief that ordinary people cannot understand one, and the like. These traits seem quite plausibly linked to aggression and violence, especially when the narcissist encounters someone who questions or disputes his or her highly favorable assessment of self. Narcissism has also been linked empirically to high but unstable self-esteem, so narcissism seems a very promising candidate for aggression researchers to study." (Baumeister, *et al*., 2000, p. 27).

Bushman, Baumeister, Philliips, and Gilligan (1999) reported that the prisoners showed higher narcissism scores than non-incarcerated groups in their narcissism measurements. This measure consisted of the following factors: entitlement, superiority, vanity, exhibitionism, and authority.

In this sense, narcissism might be a useful concept examining hackers' aggressiveness. Because a narcissistic personality is a sign of unstable high self-esteem (Baumeister, Bushman, & Campbell, 2000; Baumeister, 1999; Kernis, 1993; Rhodewalt, Madrian, & Cheney, 1998), this study uses narcissism as a theoretic rationale to examine hackers' aggressiveness in the cyberspace.

Based on the previous studies, this study proposes the following hypotheses and one research question.

H1-1: Hackers with high narcissism will report a more angry temperament than hackers with low narcissism.

H1-2: Hackers with high narcissism will report more angry reactions than hackers with low narcissism when they feel negative feedback from others.

H1-3: Hackers with high narcissism will report more possibilities of angry behaviors than hackers with low narcissism when they feel negative feedback from others.

RQ1: What kinds of factors in narcissism affect hackers' aggressiveness?

2) True vs. Contingent Self-Esteem

The modified assumption concerning self-esteem has been explained by different researchers using different terms: Mruk (1995) cited that many researchers described this phenomenon in a different ways such as discrepant self-esteem (Coopersmith, 1967), pseudo self-esteem (Branden, 1969), defensiveness (O'Brien & Epstein, 1983), unstable high self-esteem (Kernis, 1993). Deci and Ryan (1995) also defined modified self-esteem as true vs. contingent self-esteem. This study will follow the concept of "true vs. contingent self-esteem" made by Deci and Ryan.

According to Deci and Ryan (1995), "true self-esteem is more stable, more securely based in a solid sense of self (p. 32)." A person's self-worth will be more securely developed when he/she acts autonomously so that the person will not be engaged in evaluating feedback given (Do I have positive feedback or not?). With a high level of high self-esteem (true self-esteem), the person considers such rewards as reputation, money, high status, power, fame, etc. as less important. The true self-esteem is equal to stable high self-esteem.

> "People with high true self-esteem, of course, would have goals and aspirations, and they would attempt to accomplish those outcomes by devoting their personal resources to them, often wholeheartedly. And their emotions would surely be affected by the outcomes of their efforts. They would probably feel pleased or excited when they succeed and disappointed when they fail. But their feelings of worth as people would not fluctuate as a function of those accomplishments, so they would not feel aggrandized and superior when they succeed or depressed and worthless then they fail (Deci & Ryan, 1995, p. 33)."

On the other side of continuum of high self-esteem, Deci and Ryan (1995) described "contingent self-esteem" as different positive feelings about oneself depending on if he/she is matching some standard of excellence or living up to some interpersonal expectations. This kind of a person always feels positively about him/herself only when the person obtains some successful feedback, rewards, cheer, or high score from others, and if the person has satisfactory results when compared with others. Although the person has a high level of self-esteem, the level of high self-esteem is fragile, and its status can be maintained only when meeting some criterion. Ryan (1982) claimed that this kind of contingent self-esteem is associated with aggrandizement, egoism, or narcissism. The contingent self-esteem is equal to unstable high self-esteem.

To determine true or contingent self-esteem depends upon how one's worth is an integrated aspect of one's self and how it would be reflected in agency, proactivity, and vitality (Ryan & Frederick, 1994; Kernis, 1995; Deci & Ryan, 1991; Ryan, 1993). True self-esteem is maximized when one behaves autonomously with a lot of competence and if others support the person or his/her activities.

In hacker communities, there were some groups who, although they have no reason to hack, still have advanced hacking skills and are not concerned about money, national issues, or reputation.[24] They just hack for fun.[25] This type of hacker may have some proclivities that demonstrate true self-esteem - they just don't care about anything but hacking.

Other hacker groups put their reasons for attacking on the target web pages. Among them, a large portion of hackers (about 90% of the sample from Woo *et al*., 2002) left their names for peer recognition, and bragging remarks (about 51% of the sample). Woo *et al*. (2002) noted that hackers who have a certain purpose tend to use more web tools[26] for displaying their causes on the target web pages than do non-purposive hacker groups. In addition, the former group has a tendency to use more verbal attacks[27] on target web pages than the latter group.

This fact is very significant if we accept the following statements: 1) Contingent self-esteem is associated with ego-involvement (Ryan, 1982), 2) violence can emerge from threatened egotism after hackers experience wounded pride, disrespect, verbal abuse, insults, and status inconsistency (Baumeister, 1999), moreover, because achieving a goal (matching excellent standards) determines self-esteem and gives positive rewards to a person, "the person will use whatever means to match the standards, including rationalization, self-deception, and other such defensive process that have been linked to less positive mental health" (Deci & Ryan, 1995, p.32).

[24] According to Woo et al., about 24% of defaced web page contains "no reason to hack." However, 72% of the sample showed that hackers tend to put their reason why they deface the target web page.

[25] According to Woo et al., about 27% of the sample showed that they hack for fun.

[26] The chauvinist group (purposive hackers) uses more web tools such as text, picture, audio file, active animation file, streaming file, hyperlink, and e-mail than the anarchist group (non-purposive hackers).

[27] The chauvinist groups (purposive hackers) uses more profane language, verbal insults, and serious threats than the anarchists group (non-purposive hackers).

Therefore, this study assumes: when hackers with true self-esteem feel threats, constraints or pressures from other people, culture, and government, they may not respond aggressively because they don't care about this negative feedback because of their integrated self-esteem. Meanwhile, when hackers with contingent self-esteem face the same situation, it is possible that this group will show more aggressiveness than hackers with true self-esteem because their ego-system is damaged and attacked.

3) Intrinsic vs. Extrinsic motivations

In general, when people do something, they have an intentional goal. All activities are spurred by a variety of motivations. Social psychology has noted that motivations for influencing behaviors could be divided into intrinsic motivation and extrinsic motivation, depending on true and contingent self-esteem (Deci and Ryan, 1995). Intrinsically motivated behaviors are experienced when a person acts autonomously in accordance with one's true self-esteem. This motivation propels behaviors that people perform when they feel free from threats, constraints, or rewards. The only reward is the spontaneous experience of interest and enjoyment. According to Kernis (1995), "Intrinsic motivation entails curiosity, exploration, spontaneity, and interest in one's surroundings (p. 37)."

In contrast, extrinsically motivated activity is triggered by contingent self-esteem. This motivation promotes behaviors that people act intentionally to obtain rewards such as high status, money, fame, or positive remarks. Because extrinsically motivated behaviors are tied with contingent self-esteem, these tend to be associated with a kind of narcissism or aggrandizement when of comparing oneself with others.

In this sense, the concept of intrinsic motivation can be an appropriate theoretic tool to explain hacking in more systematic ways. A hacker who possesses integrated self (true self-esteem) may hack autonomously. That is, a hacker triggered by true self-esteem believes that he has competence, knows how to break in and out without accidental destruction to a computer system and also believes that his behaviors are based on his own ethics and are supported by others.

Consequently, this intrinsic motivation may lead to hacking. Since intrinsic motivation in a hacker may not be pressured by exterior demands, threats, or rewards, hacking itself gives him happiness and enjoyment. For intrinsically motivated hackers, hacking means just having a pretty good time. They don’t see any other standard or norm. Instead, they just do it autonomously and enjoy it while exploring others’ computer system.

On the other hand, an extrinsically motivated hacker may consider some standards, rewards, or pressures as his or her major reason to hack, crack, or deface target web pages. That is, in order to obtain peer recognition, financial benefits in terms of stealing individual information, being the top hacker among their communities, or promoting some cultural worldviews (i.e., ideology, nationalism, and religion), they may break into others’ computer systems. For extrinsically motivated hackers, hacking means establishing a good reputation from others, bragging about their skills, living with good money or expressing the superiority of their cultural worldview.

Jordan and Taylor (1998) recapitulate that hackers conduct hacking on computer systems and web sites because of the following personal motivations: 1) addicted hacking habit; 2) curiosity as what can be found on the worldwide network; 3) boredom of off-line life; 4) attraction to gain power over restricted computer systems such as NASA, Citibank or the CIA Web site; 5) peer recognition; 6) service to future computer users. In addition, many previous studies (see, the motivation of hackers in literature review section) about hackers' motivation include no-purpose, nationalism, patriotism, checking security, ethnicity, the freedom of information, and lover.

Therefore, if we assume that addiction to hacking, learning more about the computer system, curiosity, no- purpose and boredom belong to intrinsically motivated hacking, and that peer recognition, service to future computer users, gaining power over highly restricted computer systems, patriotism, nationalism, religion, ethnicity, and lover would be categorized into extrinsically motivated hacking, the relationship between true vs. contingent self-esteem and intrinsic and extrinsic hacking motivations may give insights to understand what makes them engage in hacking.

The second hypotheses attempt to measure the relationship between types of motivations triggered by self-esteem (true vs. contingent) and aggressiveness, and between types of motivations and types of hacking behaviors. Based on the above theoretic rationale, this study suggests the following research hypotheses:

H2-1: Hackers with extrinsic motivations will report more aggressiveness than hackers with intrinsic motivations.

H2-2: Hackers with intrinsic motivations will report more non-reward hacking activities (i.e., for fun, no-purpose, or curiosity) than reward hacking ones (i.e., nationalism, peer recognition, or money).

H2-3: Hackers with extrinsic motivations will report more reward hacking activities (i.e., nationalism, peer recognition, or money) than non-reward hacking ones (i.e., for fun, no-purpose, or curiosity).

Flow

Csikszentmihalyi and Rathunde (1993) noted that in some cases, people perform an activity because they enjoy the behavior itself. Further, if people who are engaging in the activity meet certain criteria (balance of high challenge and high skill), people tend to continue to do it, and they want to do whatever they are doing even if the experience is difficult, dangerous, or time-consuming. For instance, daredevils such as rock climbers, motorcycle riders, hang glider pilots, and tight rope-walkers keep trying these activities again and again in order to feel enjoyment. People who love Yoga, Zen, or looking at beautiful sunset also feel a certain optimal experience while doing these behaviors. If they don't feel anything from these activities, they would not think of it again. However, something propels them to initiate this activity. Social psychologists refer to this as "flow (optimal experience or positive experiential state)." Other researchers claim that this phenomenon is not limited to those adventurous people but includes human beings in everyday life: the experience of TV viewing, the experience of leisure, and the relation between energy and well-being (Csikszentmihalyi & Kubey, 1981; Kubey & Csikszentmihalyi, 1990; Graef, Csikszentmihalyi, & McManama Gianinno, 1983; Graef, McManama Gianinno, & Csikszentmihaly, 1981).

The state of flow emerges when a person has harmony among 1) clear goals, 2) immediate positive feedback, and 3) balance between a given situation and ones' ability to manage. In focusing on goal-directed targets, the person in flow feels a loss of unpleasant concerns and a distortion of the sense of time. Therefore, the person feels that he/she becomes the activity itself so that time seems to pass very quickly, and they are also aware of the worth of doing it for its own sake. In this sense, flow is one of the signs in intrinsic experience (Jackson & Marsh, 1996).

Interestingly, flow is not maintained forever. When a certain activity is repeated, the skills of the person improve, much like children who train themselves to pass each level of video games. Once the person passes a level in game, he/she may get bored and return to feel flow again by meeting more complicated and higher levels of challenges. That is, in the situation of high skill but low challenge, flow cannot be produced so that people try to find new challenge to meet their upgraded skill.

Csikszentmihalyi and Rathunde (1993) summarized the sub-dimensions of the flow experience: clear goals,[28] immediate feedback,[29] challenge-skill balance,[30] action and awareness merge,[31] concentration on the task at hand,[32] sense of control,[33] loss of self-consciousness,[34] sense of time altered,[35] and autotelic experience.[36]

Flow concept may explain why hackers keep breaking into computer systems, and why they want to explore tightly restricted computer systems such as top-secret government computer infrastructure, military networks, and nuclear plants. For instance, if a hacker endorses the cause that "information should be free from government;" if the hacker thinks how well he/she is doing; if he/she feels the confidence to break into the CIA computer systems, these situational conditions may propel the hacker to feel optimal

[28] Clear goals define a person really knowing what he or she is going to do.

[29] Immediate feedback is that one knows how well one is doing.

[30] Challenge-skill balance is defined as a state when a person has skills to meet a given challenge.

[31] Action-Awareness merging is that "involvement in the flow activity is so deep that it becomes spontaneous or automatic" (Jackson & Marsh, 1996).

[32] Concentration on task at hand is being focused.

[33] Sense of control indicates that you can control anything in your body and soul. You can do anything you want.

[34] Loss of self-consciousness is that concern for the self disappears when a person really focuses on an activity. The person does not consider what others see to him or her. "This does not mean that the person is unaware of what is happening in mind or body" (Jackson & Marsh, 1996).

[35] Sense of time altered is that time may simply become irrelevant and out of one's awareness so that a person in flow feels that time goes so fast.

experience (flow). In other words, after frequent illegal access to several university web sites, hackers who break into the main computer systems in a university feel that this is very easy to do might want to test their hacking techniques with computer banking systems which are a little bit more difficult to access. Once the hacker successfully attains the goal in a bank, he/she is likely to look for the most difficult computer networks such as intelligence, military, government,[37] emergency systems,[38] or nuclear plants.[39]

If there are the hackers who have no expectation of some future reward or benefit, we may detect flow from them, and generalize that flow is one of motivations to have them fall in love with hacking and to explain why they continue to do this and what makes them to pursue tightly secured computer systems.

This study develops the following research hypothesis based on the concept of the flow.

H3-1: Hackers who feel high level of flow will be more frequently involved in hacking activities than hackers with low level of flow.

RQ 2: What kinds of dimensions of flow make hackers are involved in hacking activities?

Terror Management Theory

This theoretical frame stems from Ernest Becker (1973)'s concept: the terror of death. That is, a person's self-esteem is driven by the denial of death. People want to escape from the anxiety that would arise from recognizing that one will die (Baumeister,

[36] Autotelic is defined as the situation: if a person is in flow, he or she really enjoys the experience. An situation leaves you on a high. An activity is autotelic if it is done for its own sake, with no expectation of some future reward or benefit.

[37] In May 1993, angry Chinese hackers defaced several U.S. government sites (Denning, 2001).

[38] See, footnote #13.

[39] " In June 1998, a group of international hackers calling themselves Milw0rm hacked the Web site of India's Bhabha Atomic Research Center (BARC)" and replace the original site with a mushroom cloud and the text "if a nuclear war des start, you will be the first to scream…" (Denning, 2001, p. 272)

1999). According to this theory, unlike animals, human beings have cognitive abilities so that they can anticipate the end of their life (e.g., death, vulnerability, or mortality); they also have instinctive aspiration that their existence keep continuing (e.g., self-preservation, continued existence or immortality). The conflict between these two perspectives in a person makes him/her feel an enormous potential for anxiety, terror, and negative feelings toward death.

Therefore, to get rid of this potential terror, people tend to use "cultural worldviews that help individuals manage this terror by denying that life is a purposeless biological accident and that death is absolute annihilation for the individual (Greenberg, Pyszcznski, & Solomon, 1995, p. 75)." To buffer anxiety or potential terror, cultural worldviews function as following:

> "Three sets of cultural constructs play an especially important roles in terror management. First, all cultures infuse the universe with meaning by offering explanations for the origin of human beings and the place of humans within the cosmic scheme of things. Second, all cultures provide prescriptions for feeling good and valuable, largely through the provision of valued social roles, behavior, and attributes. Finally, all cultures offer safety and hope of literal or symbolic immortality to those who meet the prescriptions of value. Literal immortality consists of notions of an afterlife (e.g., spirit souls); symbolic immortality consists of extensions of the self, such as prosperous children, permanent marks on reality (e.g., buildings, monuments), enduring achievements (e.g., a great painting or novel), and identification with ideologies and entities that transcend death (e.g., a political ideal, one's country, the cosmos)" (Greenberg, et al., 1995, p. 75).
>
> In addition, "The terror is managed by a cultural anxiety buffer that has two components: a) an individualized version of the cultural worldview that imbues the world with meaning, order, and permanence; provides standards for valued behavior; and promises either literal or symbolic immortality to those who meet or exceed these prescriptions for value b) self-esteem, the belief that one is meeting the standards of value espoused by one's worldview" (Arndt, Greenberg, Solomon, Pyszczynski, & Simon, 1997, p.6).

Many studies using hypotheses from terror management theory have provided us with the conclusion that when people are reminded of their own mortality, their need for faith in their worldviews is increased (Greenberg, Simon, Pyszczynski, Solomon, & Chatel, 1992; Greenberg, Pyszczynski, Solomon, Resenblatt, Veeder, Kirkland, & Lyon, 1990; Rosenblatt, Greenberg, Solomon, Pyszczynski, & Lyon, 1989). According to Kernis (1995), threats to a certain cultural worldview lead to negative judgments of others who challenge cultural norms as well as positive evaluations of ingroup members.

This kind of tendency is well represented in the literature on genocide, political terror, and prejudice (Baumeister, 1999). As a result, people generally respond favorably to those who share their worldview and unfavorably to those who do not. Based on the above explanations and research findings, terror management procedures in self-esteem seem to belong to extrinsically motivated behaviors. That is, self-esteem is dependent upon a certain cultural worldview.

Terror management theory also posits that confidence in a particular worldview can be restored not only by derogating different others, but by actually annihilating them (Greenberg, Solomon, & Pyszczynski, 1997). Other research findings have revealed that mortality salience encourages aggression against a worldview threatener (McGregor, Lieberman, Greenberg, Solomon, Arndt, Simon, & Pyszczynski, 1998; Solomon, Greenberg, & Pyszczynski, 1991).

In other words, when a person is criticized by others concerning his/her cultural worldview, he or she will have more aggressive expressions against the worldview-threatening others than those who do not feel any threat to their own cultural worldview. Historically, many have tried to remove the group who do not share their worldview by attempting to annihilate those who are different (i.e., massive murder of Jews by Nazi, the ethnic cleansing in Rwanda, and the crisis between Bosnians and Serbs, etc.). Greenberg, *et al.* (1990) reported that mortality salience led Christian respondents to give more positive evaluations of a fellow Christian and more negative evaluation of a Jew. Nelson, Moore, Olivetti, and Scott (1997) suggested that there is possibility: mortality-salience-induced biases enable organizations or nations to represent worldviews different from an entity with other cultural worldviews and consistent with one's own cultural worldview. So, when people feel mortality salience with other countries, they may tend to become more patriotic or nationalistic.

Based on this rationale, we may infer that hackers can feel threatened by some others who are different in politics, religion, nation, or ethnicity. In this study, we point out hackers' cultural worldviews espoused by nationalism, religion, ethnicity, and any kind of ideology. As Taggart (2001) mentioned, many hackers and web defacers have participated in a series of cyber-wars on behalf of their nations, religions, or ethnicities. Woo *et al.* (2002) suggested that the cultural worldview-oriented type of web defacement has more aggressive expressions than does non-cultural worldview type of web defacement. Woo (2003) reported that hacker groups involved in high intensive international conflicts showed more aggressive expressions and verbal attacks against the opponent than ones in relatively low intensive conflict.

As human beings, if hackers have a faithful cultural worldview such as nationalism, religion, or any kind of ideology, they may feel some threats from others (e.g., Palestinian hackers may be threatened by Israel web sites; Chinese hackers may feel negative things from U.S. military web sites; Korean hackers may feel offensive against

Japanese government web sites); if the hackers directly or indirectly feel any threat from others, they may try to present their negative judgment or expression to the opposite with their own hacking methods. Woo, *et al.* (2002) noted that off-line conflicts tend to break out in on-line battles and that defaced web pages that are full of profane language, hate statements, or insulting pictures may be attacked by hackers who have totally different cultural worldview and strongly stick to their worldview.

Along with their argument, terror management procedure in a hacker's psychological mindset may compel him/her to attack, hack, crack, or deface the web site or computer systems of challengers who threaten to their cultural worldview.

To investigate this, the following hypotheses will be tested.

H4-1: <u>When a hacker feels any threat to own worldview from other countries, hackers with high nationalism will report more aggressiveness than hackers with low nationalistic ideology</u>.

H4-2: <u>When a hacker feels any threat to own worldview from other religions, hackers with strong religious pride will report more aggressiveness than hackers with weak religious pride.</u>

H4-3: <u>When a hacker feels any threat to own worldview from other ethnic groups, hackers with strong ethnic coercion will report more aggressiveness than hackers with weak ethnic coercion.</u>

<u>Possibility of Cyberterrorism against Other Countries</u>

This study tries to investigate the possibility of cyberterrorism against other nations in terms of analyzing hackers' psychological mindsets and their demographic factors. Hackers' criminal activities could be different depending on what kinds of self-esteem they possess, what flow levels they maintain, what kinds of cultural worldviews they stick to, and what kinds of aggressiveness levels they have, etc. All kinds of factors and their interactions between factors may prompt hackers attack other nations but it still is unknown what makes them to do so.

Online battles between nations are no longer an imaginary war game. This kind of international conflict is possible. So, this study states a research question:

RQ 3: What kinds of psychological factors and other elements of hackers affect their hacking intention against other nations?

CHAPTER 4

METHODOLOGY

Sample

An on-line survey of computer hackers was conducted. Because most hackers do not want to reveal their identities, it was impossible to send invitations to participate in this research directly to the hackers. To solve this problem, the *Hackerslab's*[40] *free hacking zone* was used. The *Hackerslab* holds hacking contests every other year. The first contest was held in August, 1999; the second one was in August, 2001. The *Hackerslab* reported that about 100,000 hackers from all over the world participated in these contests. The *Hackerslab* created 18 different levels in a *free hacking zone* that ranged from level 0 to level 17. If a hacker passes level 0, the hacker automatically goes to level 1. If the hacker passes level 1, the contestant automatically goes to level 2. As long as there is no failure until the 17th level, the hacker's name or nickname automatically goes to the hall of fame, and the winner get some monetary reward. After the contest, the *free hacking zone* is open to the public so that any person who has hacking skills is able to access to the *free hacking zone* and test his/her hacking techniques.

The *free hacking zone* was an appropriate source to advertise this survey because many hackers visit this web site.[41] The FHZ (free hacking zone) team helped this study by creating a database and an online survey. Furthermore, to protect the database and the

[40] The *Hackerslab* is a computer security company located on Seoul, Korea (www. Hackerslab.org).

online survey files from malicious hacking, the team put all database and survey files into their main server where they were protected by a firewall. In addition, this research had been publicized to *Defcon,*[42] *Hacktivismo,*[43] and a variety of hacking communities all over the world.

The survey period was from September 16, 2002 to November 1, 2002. The respondents, presumably computer hackers, were asked to check 68 questions. Two versions (English & Korean) of the questionnaire were used. The content of these questionnaires was exactly same, and the English version of the questionnaire was translated into Korean. To avoid wrong translation, the researcher translated the English version of the questionnaire into Korean, first and then, two Korean Americans who have bilingual ability re-translated it into English version in order to check translator's inter-reliability between different versions of the questionnaire. In order to check the reliability and validity of measurements used in this question, two pilot tests were conducted. 17 hackers and 23 hackers recruited by the *Hackerslab* participated in each test.

Online survey files of the both versions of the questionnaire were loaded on the *Hakcerslab*'s main server. About 1, 390 hackers participated in this survey, and participants were from at least 30 countries. Because of privacy concerns, this survey did not ask participants' nationality. Instead, this survey used an alternative way to infer

[41] According to the *Hackerslab*, about 2,000 hackers visit their web sites per day.

[42] See, footnote 1.

[43] "Hacktivismo is a special operations group sponsored by the CULT OF THE DEAD COW (cDc). We view access to information as a basic human right. We are also interested in keeping the Internet free of state sponsored censorship and corporate chicanery so all opinions can be heard. The cDc is the most influential group of hackers in the world. Grandmaster Ratte' and Franken Gibe spawned the herd in 1984 in Lubbock, Texas. We publish the first and longest running e-zine in the history of the Internet, are thorns in Billion Gates ass, and are the only reasons worth getting out of bed in the morning. We're also very good at card tricks and dancing." (http://hactivismo.com).

respondents' nationality by asking their mother language. The questionnaire asked the respondents to check their first language in order to infer computer hackers' nationality. Thirty different languages were chosen in response to the item (e.g., "What language do you speak most often?"). In addition, 15 respondents checked "other" item. Consequently, this study estimated that hackers who came from at least 30 nations participated in the survey.

To increase the validity of the study, the researcher eliminated disqualified and incomplete surveys. Two strict rules were established to remove disqualified data. The first was that data should be removed if a respondent answered less than 70% of the questionnaire, and if a respondent did not appear to answer sincerely (e.g., such a checking answer as 1, 1, 1, 1, 1, 2, 2, 2, 2, a, a, a, a, a, b, b, b, b, b). About twenty percent (279 respondents) of the 1,385 data were disqualified by this rule.

The second rule was that data should be eliminated if a respondent did not answer the following questions: 1) "In the last month, have you altered or otherwise changed any web sites belonging to others?" 2) "Have you ever participated in the *Hackerslab*'s *free hacking zone*?" 3) "Have you ever participated in other computer hacking contests?" About twenty-seven percent (377 respondents) of the total participants were eliminate according to this rule. After eliminating data which could not pass these criteria, 729 respondents' data were used to analyze the relationships between variables.

Measurements

1) Demographic & General questions.

   A. Demographic questions

Gender, age, religion, race, education, and language items were provided to the respondents to describe the participants' demographic factors. The scale of each item was used as gender ("male" = 1 & "female" = 0), age (ranged from "less than 19 years old" = 1; "20-25 years old" = 2; "26-30 years old" = 3; "31-35 years old" = 4; "36-40 years old" = 5; "41-45 years old" = 6; "46-50 years old" = 7; "more than 51 years old" = 8). Religion ("Buddhism" = 1, "Catholic" = 2, "Christianity" = 3, "Hinduism" = 4, "Judaism" = 5, "Moslem" = 6, "others" = 7, "no-religion" = 8). Race ("Arab" = 1, "Asian" = 2, "Black" = 3, "Caucasian" = 4, "Hispanic" = 5, "Jewish" = 6, "Native American" = 7, "others" = 8). Education ("Elementary school" = 1, "Middle school" = 2, "High school" = 3, "College-2 year" = 4, "College-4 year" = 5, "Graduate school-master degree" = 6, "Graduate school-Ph.D." = 7). Language (35 language items were provided to check the participants' first language).[44]

B. General questions

To measure hackers' frequency of hacking activities per month and hacking contest experience, the respondents were asked to check some general questions: For hacking activities, 1) "In the last month, how often did you break into somebody else's computer systems?" ("Never" = 0, "1-2" = 1, "3-5" = 2, "6-10" = 3, "11-20" = 4, "21-30" = 5, "more than 31" = 6). "In the last month, how often did you alter or change others' web sites?" ("Never" = 0, "1-2" = 1, "3-5" = 2, "6-10" = 3, "11-20" = 4, "21-30" = 5, "more than 31" = 6). For hackers' experience in hacking contests, subjects were asked to check on a yes-no scale on the item "Have you ever participated in the *Hackerslab's free*

[44] This item was used to measure participants' nationality indirectly. The following language were reported in this study: Afghan, Arabic, Bohemian/Czech, Chinese, Danish, Dutch, English, Finnish, French, German, Greek, Hebrew, Hindi, Hungarian, Indonesian, Iranian, Iraqi, Irish, Italian, Japanese, Korean,

hacking zone?" and on a scale of "level 0" = 0, "level 1" = 1, "level 2" = 2 and so on to "level 17" = 17 on the item "What was your final level in the *hackerslab*'s *free hacking zone*?" Respondents also were asked to indicate if they participated in other computer hacking contests ("Yes" = 1, "No" = 0) on the item, "Have you ever participated in other computer hacking contests? (choose one contest that you recently participated in)," and select the final level of the hacking contest ("Top-10%" = 1, "11-30%" = 2, "31-50%" = 3, "51-70%" = 4, "71-100%" = 5) on the item, "What was your final level?"

2) Independent variables

A. Narcissism

Social psychologists maintain that a narcissistic personality is a sign of unstable high self-esteem and that this may lead to a person's aggressiveness (Baumeister, Bushman, & Campbell, 2000; Kernis, 1993; Rhodewalt, Madrian, & Cheney, 1998). In this study, an index of narcissism was used as an independent variable to test the relationship between hackers' level of narcissism and their aggressiveness. Narcissism was measured by asking hackers to read each pair of 16 statements and then indicate which statement comes closest to their feelings and beliefs about themselves. Rose (2001) developed a short narcissistic personality index (SNPI) used by this study. Each narcissistic response is worth one point. The total narcissistic personality score is the sum of narcissistic responses.

In order to reduce the items and evaluate the initial dimensionality, all sixteen items were subjected to a promax with Kaiser Normalization (oblique) rotated principal

Kurdish, Latin, Lebanese, Malay, Norweigan, Polish, Portuguese, Russian, Spanish/Espana, Swahili, Swedish, Thai, Turkish, Vietnamese, and others.

component factor analysis.[45] Four factors were extracted from 13 items (3 items were reduced by factor analysis because factor loadings in three items were below .40[46]). Factor one was referred to as "center of attention" (e.g., "I like to be the center of attention"). This factor explained 19.8 % of total variance with an eigenvalue of 3.17. The Chronbach's alpha reliability coefficient of 3 items was .64. Factor two was known as "inflated confidence" (e.g., "I can make every body believe anything I want them to"). This factor explained 11.3% of total variance with an eigenvalue of 1.80. The Chronbach's alpha reliability coefficient of 4 items was. 54. The third factor was called "control of others" (e.g., "I find it easy to manipulate people"). This factor explained 8.1% of total variance with an eigenvalue of 1.29. The correlation coefficients between these two items was r = .28. The fourth factor was "fantasies of personal greatness" (e.g., "I am an extraordinary person"). This factor explained 6.7% of total variance with an eigenvalue of 1.08. The Chronbach's alpha reliability coefficient of 4 items was .53.

To check the relationship between hackers' narcissistic levels and their aggressiveness, respondents' narcissism scores were summed. If a hacker selected all thirteen narcissistic statements, his/her total narcissistic score was 13. Consequently, the

[45] "An orthogonal rotation method (e.g., varimax, equimax, quartimax, etc.) constrains factors to be independent of each other, while an oblique rotation method allows factors to be correlated. It is often believed that an orthogonal rotation produces a simpler and more easily interpretable structure of factors. However, this common belief (or convention of preferring varimax rotation) is unwarranted and unrealistic. Furthermore, many constructs in communication research cannot be expected to be independent of each other and, even if the factors are indeed unrelated, an oblique rotation will show correlations close to zero" (Park, Dailey, & Lemus, 2002, p. 566).

[46] A common strategy is to retain only those factors with the correlation matrix and eigenvalue greater than 1.0. For item inclusion on a given factor, items were used in the final scales if the item loading factor coefficients were greater than .40.

highest narcissistic score was 13 and the lowest one was 0. The resulting distribution was trichotomized to form three groups: low, medium, and high narcissistic personality.[47]

B. Intrinsic vs. Extrinsic motivations

Deci and Ryan (1995) claim that motivations for influencing behaviors can be divided into intrinsic and extrinsic motivation, depending on true and contingent self-esteem. That is, intrinsic and extrinsic motivations triggered by true and contingent self-esteems, respectively may be related to different motivation for hacking activities (non-reward oriented hacking vs. reward-oriented hacking). Kernis, Paradise, Whitaker, Wheatman, and Goldman (2000)'s motivation items were used to test this hypothesis. Some words in the original statements were adapted for this study. The adapted hacking motivations index was measured by asking hackers to indicate how important they rate eight items: (e.g., "I do hacking because I feel that hacking will help me grow or develop in a way that is personally important to me"; "I do hacking because somebody else wants me to or because I will get something from somebody if I do"). The response option was a 7-point scale ("Is not at all a reason" = 0 to "is an extremely important reason" = 6).

In order to reduce the items and evaluate the initial dimensionality, all eight items were subjected to a promax with Kaiser Normalization (oblique) rotated principal component factor analysis. There were no reduced items. The two factors were extracted: 1) the "intrinsic motivation" factor explained 39.4% of total variance with an eigenvalue 3.15. The Chronbach's alpha reliability coefficient of 4 items (e.g., I do hacking because of the interest and enjoyment of doing it") was .77. 2) the "extrinsic motivation" factor

[47] The choice of cut point is an important decision because the three cut points used in this analysis may create artificial results. Therefore, narcissism scores against the dependent measures (angry temperament, reaction, and behavior) were conducted to check linearity test by SPSS 10.0. The distributions on the three measurements were linear (*p* < .001).

explained 17.3% of total variance with an eigenvalue 1.38. The Chronbach's alpha reliability coefficient of 4 items (e.g., "I do hacking because something about my external situation forces me to do it") was .71.

To check the relationship between hackers' motivation levels and their aggressiveness, respondents' intrinsic and extrinsic motivation scores were summed. The total intrinsic motivation score was calculated with adding 4 items' responses that range 0 to 6. Therefore, the highest score was 24 and the lowest one was 0. The total extrinsic motivation score was calculated with adding 4 items' responses that ranged from 0 to 6. Therefore, the highest score was 24 and the lowest one was 0. The resulting distribution in each motivation was divided into two groups: low and high.[48]

C. Flow

Flow may explain why hackers keep breaking into computer systems, and why they want to explore tightly restricted computer servers because its mechanism provides hackers with the reason why they should hack to computer systems. To investigate the relationship between hackers' flow and hacking activities, a flow state scale (Jackson & Marsh, 1996) was used. Because this instrument was developed from athletes' flow descriptions, the items were adapted for the hackers' situation.

The original index consists of nine constructs (36 items).[49] In this study, only five constructs (challenge-skills balance, concentration on task at hand, loss of self-

[48] The choice of cut point is an important decision because the cut points made by mean used in this analysis may create artificial results. Therefore, each motivation score against the dependent measures (angry temperament, reaction, and behavior) was conducted to check linearity test by SPSS 10.0. The distributions on the three measurements were linear ($p < .01$).

[49] Challenge-skill balance, action-awareness merging, clear goals, unambiguous feedback, concentration on task at hand, sense of control, loss of self-consciousness, transformation of time, and autotelic experience.

consciousness, transformation of time, and autotelic experience[50]) were used. Subjects were asked to check on a scale ("strongly disagree" = 1, "disagree" = 2, "neutral" = 3, "agree" = 4, "strongly agree" = 5) the items (e.g., "I was challenged, but I believed my hacking skills would allow me to meet the challenge" or "I found the hacking experience extremely rewarding"). In order to reduce the items and evaluate the initial dimensionality, all five constructs (20 items) were subjected to a promax with Kaiser Normalization (oblique) rotated principal component factor analysis. Of 20 items, four items supposed to measure "transformation of time" were removed after performing factor analysis because the four items' factor loadings were below .40. Consequently, four constructs (16 items) were used to measure flow state.

"Challenge-skill balance" factor explained 7.1% of total variance with an eigenvalue of 1.42. The Chronbach's alpha reliability coefficient of 4 items (e.g., "I felt I was competent enough to meet the high demands of the situation") was .90. "Concentration on task at hand" factor explained 50.3% of total variance with an eigenvalue of 10.1. The Chronbach's alpha reliability coefficient of 4 items (e.g., "My attention was focused entirely on what I was hacking") was .93. "Loss of self-consciousness" factor explained 5.8% of total variance with an eigenvalue of 1.16. The Chronbach's alpha reliability coefficient of 4 items (e.g., "I was not worried about my performance during hacking") was .89. "Autotelic experience" factor explained 10.4% of total variance with an eigenvalue of 2.07. The Chronbach's alpha reliability coefficient of 4 items (e.g., "The hacking experience left me feeling great") was .93.

[50] "An autotelic experience is an intrinsically rewarding experience. An activity is autotelic if it is done for its own sake, with no expectation of some future reward or benefit" (Jakson & Marsh, 1996, p20).

To check the relationship between hackers' flow levels and their hacking activities, respondents' flow scores were summed. The total flow score was calculated with adding 16 items' responses that ranged from 1 to 5. Therefore, the highest score was 80 and the lowest one was 16. The resulting distribution was trichotomized to form three groups: low, medium, and high level of flow.[51]

D. Cultural worldviews

According to terror management theory, people tend to use "cultural worldviews" to help them manage psychological terror, and when people feel any threat to their nationalistic pride, religious pride, or companionship, they may act aggressively against threatening source. Previous research and newspaper articles indicated that many hackers with political, religious, and ethnic motivations show hostilities toward opponents using their hacking strategies such as web defacement, computer viruses, e-mail bombing, etc.

To measure hackers' cultural worldviews, two different indices were used. The items in the first index contained three subjects (nationalism, religious pride, and ethnic coercion) while the items in the second index focused on only nationalistic pride. The purpose of the second index was to check the first index's validity and reliability.

The first index was from a "smugness"[52] subscale of Kosterman & Feshbach's patriotism-nationalism questionnaire (see, Hurwitz & Peffley, 1999). For the purpose of the current study, the statements of each item were adapted for measuring nationalism, religious pride, and ethnic coercion. In addition, this study added a paragraph (a

[51] Although some studies on flow used categorical measurements (Csikszentmihalyi & LeFevre, 1989), the choice of cut point is an important decision because the three cut points used in this analysis may create artificial results. Therefore, flow scores against the dependent measures (breaking into others' computer systems; changing web sites) were conducted to check linearity test by SPSS 10.0. The distributions on the two measurements were linear (p < .001).

[52] Smugness means the belief that my country, its symbols, and its people are simply the best.

newspaper article containing threats to respondents' cultural worldviews such as nationalism, religious pride, and ethnic coercion) to the index in order to maximize the effect of terror management theory. The below was produced for the purpose of the study.

> "Recently, powerful countries act like an arrogant bully. They wield their power and threaten other countries. Sooner or later, a strong country which has taken all power from the rest of the world will be born. This powerful one will possess all benefits. The majority ethnic group of this country espouses that they should annihilate the small and uncultured ethnics as Nazis did in the 1940s. They plan to convert all different existing religions in order to construct a new world order (Sep 11, 2001: *The Washington Post*)"

Subjects were asked to check on a scale of ("strongly disagree" = 1, "disagree" = 2, "agree" = 3, "strongly agree" = 4) on items such as (e.g., "My country's flag is the best in the world," "My religion is superior to other religions," and "People in my country are the best in the world") after reading the newspaper article. In order to reduce the items, this study performed promax rotated principal component factor analysis to 12 items supposed to measure nationalism, religious pride, and ethnic coercion. There are no reduced items. Three factors were extracted. The "nationalism" factor explained 42.2% of total variance with an eigenvalue of 5.06. The Chronbach's alpha reliability coefficient of 3 items (e.g., "My country is the best country in the world") was .83. The "religious pride" factor explained 16.1% of total variance with an eigenvalue of 1.92. The Chronbach's reliability coefficient of 4 items (e.g., "I would never change my religion") was .88. The "ethnic coercion" explained 8.7% of total variance with an eigenvalue of 1.04. The Chronbach's alpha reliability coefficient of 5 items (e.g., "My people are superior to other ethnic groups in the world") was. 75.

To check the relationship between hackers' cultural worldview levels and their aggressiveness, the respondents' each cultural worldview's scores concerning nationalism, religious pride, and ethnic coercion were summed, respectively. For nationalism, the total score was calculated with adding 3 items' responses that ranged from 1 to 4. Therefore, the highest score was 12 and the lowest one was 3. For religious pride, the total score was calculated with adding 4 items' responses that ranged from 1 to 4. Therefore, the highest score was 16 and the lowest one was 4. For ethnic coercion, the total score was calculated with adding 5 items' responses that ranged from 1 to 4. Therefore, the highest score was 20 and the lowest one was 5. The resulting distribution in three indexes was trichotomized to form three groups: low, medium, and high groups.[53]

The second index mainly contained items to measure national pride as related to the first index's nationalism factor. This index was adapted from ANES' patriotism scale (Hurwitz & Peffley, 1999) in order to check validity and reliability of the first index concerning cultural worldviews since the first index was developed for this study. Respondents were asked to indicate how they feel on a 5 item (e.g., "how proud do you feel when you hear your national anthem?") by checking on a scale of ("not very" = 1, "somewhat" = 2, "very" = 3, "extremely" = 4). Factor analysis was performed to the items. National pride factor has unidimensionality and explained 72.3% of total variance

[53] The choice of cut point is an important decision because the three cut points used in this analysis may create artificial results. Therefore, cultural worldview (nationalism, religious pride, and ethnic coercion) scores against the dependent measures (angry temperament, reaction, and behavior) were conducted to check linearity test by SPSS 10.0. In nationalism, the distributions on the three measurements were linear ($p < .01$). In religious pride, the distributions on the three measurements were linear ($p < .05$). In ethnic coercion, among the distribution on the three measurements, only the distributions of angry reaction and behavior were linear ($p < .01$). The distribution of angry temperament was non-linear. The distribution of it was an exponential curve as resembling a reclining backward "J." Low and medium levels of ethnic coercion index showed much less of angry temperament than did high level of it.

with an eigenvalue of 3.62. The Chronbach's alpha reliability coefficient of 5 items was .90. The Chronbach' alpha coefficients between the first index and the ANES' patriotism scale was .71 and the coefficients between the sub-index of nationalism in the first index and the ANES' patriotism scale was .76. Thus, this result indicated construct validity for the first index scale.

3) Dependent variables

A. Hacking activities

Based on previous studies, journals, and reports concerning cyber crimes and hacking issues, a variety of hacking experiences and activities were enumerated in this survey, and subjects were asked to check on a scale ("Never" =0, "a few" = 1, "sometimes" = 2, "frequently" = 3, "very frequently" = 4) on such as items "I have hacked bank-computer systems," "I have hacked web sites for fun", "I have hacked military web sites," etc. Twenty two hacking activities and experiences[54] were provided to the respondent. All hacking activities were treated individually. All items were subjected to a bivariate correlation analysis. All items were statistically correlated with one another (r = .15 ~ .85, p < .001).

B. Aggressiveness

Although the concept of anger, hostility, violence, and aggression has been studied in a variety of academic areas and for a long time, definitions of these constructs are often used interchangeably and are even more ambiguous and contradictory. As a result,

[54] There are 22 hacking reasons and experiences (i.e., hacking bank, peer recognition, for fun, no-particular reason, checking security, for boy/girl friends, hacking government sites, other religion sites, other ethnic web sites, stopping porn, information should be free in cyberspace, making money, curiosity, boredom, hacking transnational company's web sites, intelligent web sites, military web sites, university web sites, personal homepage, big business sites, making computer virus, small company sites.

the distinctions between the concepts are very difficult. Spielberger, Jacobs, Russell, and Crane (1983) noted, "while anger and hostility refer to feelings and attitudes, the concept of aggression generally implies destructive and punitive behavior directed towards other persons or objects. It should be noted, however, that aggression and hostility are often used interchangeably (p. 162)." They claimed that hostile aggression refers to behavior motivated by anger.

Previous research (Woo, 2003; Woo, *et al.*, 2002) noted that politically motivated hackers showed more aggressive expression and verbal attacks against opponents than personally motivated hackers. In this sense, hackers' aggressiveness can be explained by suggesting that their aggressive behaviors are triggered by their emotional anger. Anger can be a predictor to assess hackers' aggressive expressions, emotions, or behaviors.

To measure hackers' aggressiveness, we might use clinical interviews, behavioral observations, and projective techniques as other aggression studies have done. However, these methods are not appropriate to investigate hackers' aggressive behaviors because hackers do not attack others in physical ways. And methodologically, it is impossible to measure hackers' aggressive behaviors in off-line situations because of legal and ethical problems.

Consequently, this study used the "Angry Temperament and Angry Reaction Subscales (see, Spielberger, et al., 1983, p.180)" in order to measure computer hackers' aggressiveness by examining the structure of anger in a hacker. This instrument assesses hackers' 1) angry temperament,[55] 2) angry reaction,[56] and 3) other trait anger items such as verbal attacks and behavioral attacks.[57]

[55] Angry temperament (e.g., "I have a fiery temperament," "I am quick-tempered," "I am a hot-headed person," and "I fly off the handle").

In order to reduce the items and evaluate the initial dimensionality, the ten items were subjected to a promax with Kaiser Normalization (oblique) rotated principal component factor analysis. There were no reduced items. Subjects were asked to check on a scale (“almost never” = 1, “sometimes” = 2, “often” = 3, and “almost always” = 4) on angry temperament, reaction, and behavior items. Three factors were extracted as in the original scale. “Angry temperament” factor explained 51.5% of total variance with an eigenvalue of 5.15. The Chronbach's reliability coefficient of 4 items was .85. “Angry reaction” factor explained 10.9% of total variance with an eigenvalue of 1.09. The Chronbach’s alpha reliability coefficient of 4 items was .83. “Angry behaviors” factor explained 10.1% of total variance with an eigenvalue of 1.01. The correlation coefficients between these two items was r = .64.

To check the relationship between some independent variables such as hackers’ narcissism, motivation levels, and cultural worldviews and their aggressiveness, respondents’ angry temperament score, angry reaction score, and angry behavior score were summed, respectively. The total score of angry temperament was calculated with adding 4 items’ responses that ranged from 1 to 4. Therefore, the highest score was 16 and the lowest one was 4. The total score of angry reaction was calculated with adding 4 items’ responses that ranged from 1 to 4. Therefore, the highest score was 16 and the lowest one was 4. The total score of angry behaviors was calculated with adding 2 items’ responses that ranged from 1 to 4. Therefore, the highest score was 8 and the lowest one was 2.

[56] Angry reaction (e.g., “I am infuriated when I get a poor evaluation,” “I am furious when criticized,” “I am annoyed when not given recognition,” and “I am angry when slowed down by others).

C. Intention to hack other nations[58]

The purpose of this index was to measure hackers' intention to hacking attack against opposing nations when they feel threatened by other countries. Subjects were asked to check on a scale of ("strongly disagree" = 1, "disagree" = 2, "agree" = 3, "strongly agree" = 4) for the items (e.g., "If another country criticizes my country, I would hack that country's web sites with my hacking skills," "If another country threatens my country, I would hack that country's web sites with my hacking skills," "If another country tries to invade my country, I would hack that country's web sites with my hacking skills," "If I hear that another country's hackers have broken into my government's web sites, I would hack that country's government web sites in return," "If I found an enemy country's web sites in the INTERNET, I would hack the country's web sites with my hacking skills"). After performing a promax with Kaiser Normalization (oblique) rotated principal component factor, there were no reduced items. The index "hacking against other nations" had unidemsionality and explained 62.1% of total variance with an eigenvalue of 3.10. The Chronbach's alpha reliability coefficients of 5 items were .84.

To check the relationship between hackers' psychological variables such as hackers' narcissism, aggressiveness, motivation levels, flow, cultural worldviews, and demographic variables and their hacking intention against other nations, respondents' responses concerning hacking intention against other nations were summed. The total score of hacking intention against other nations was calculated with adding 5 items'

[57] Other angry items (e.g., "When I get mad, I say nasty things," "When frustrated, feel like hitting").

[58] Although the index was constructed by the nationalism index and previous hacking studies, the results using this index should be treated with caution because validity and reliability of the indices were unknown.

responses that ranged from 1 to 4. Therefore, the highest score was 20 and the lowest one was 5.

CHAPTER 5

RESULTS

Sample Description[59]

The majority of the respondents were male (88 %). Female hackers in this study were only 4.3%. Hacker communities are still male dominated. About 8 % of the subject did not check their sex.

About a half of the sample belonged to less than 19 years old age group followed by 20 to 25 years old (32.9%); 26 to 30 years old (11.4%); 31 to 35 years old (3.4%); 36 to 40 years old (0.7%); 41 to 45 years old (0.4%); 46 to 50 years old (0.3%) and more than 51 years old (0.4%). This indicated that children or adolescent hackers are an active group in hacker communities. About 98% of the sample belonged to less than 35 years old.

About 40% of the sample did not have religion. Among hackers who checked a religion item, Christianity (24.7%) was the major religious group, followed by Buddhism (19.3%); Catholic (8.2%); Moslem (2.1%); Judaism (0.8%); Hinduism (0.4%). 5.1% of the sample checked “other.”

The majority respondent’s ethnic status was Asian (60.4%); followed by Caucasian (18.8%); Arabian (9.7%); Hispanic (1.6%); Black (0.7%); Native American (0.7%); Jewish (0.4%); Other (7.7%).

The majority respondent’s final education level was college-4 year (26.6%); followed by high school (25.2%); Elementary school (15.2%); College-2 year (13.9%);

Middle school (11.8%); Graduate school-master's degree (4.7%); Graduate school-Ph.D. (2.6%).

The major respondent's mother language was Korean (48.6%); followed by English (29.2%); Afghan (8.4%); Spanish (1.5%), Japanese (1.4%).[60]

The most likely target of hackers was investigated. About 70% of the respondent have experienced to breaking into personal homepages; followed by university web sites (56.5%); small business web sites (47.2%); big business web sites (42.2%); other country government web sites (38%); porn sites (35.9%); other ethnic web sites (31.8%); military web sites (27.8%); transnational corporations' web sites (27.7%); secret agency sites (26.5%); other religion web sites (22.6%); bank computer systems (21.9%).[61]

Hackers' Narcissistic Personality and Aggressiveness

To assess relationships between hackers' narcissism and their aggressiveness, three hypotheses were proposed. Hypothesis 1-1 predicted that hackers with high narcissism would report a more angry temperament than hackers with low narcissism. To test this hypothesis, mean levels of hackers' angry temperament scores were compared across the three different hacker groups representing different levels of narcissism. A one-way ANOVA was performed (Table 5.1) and supported hypothesis 1-1 ($p < .001$). Hackers who have high narcissism ($M = 9.88$) reported higher angry temperament scores than hackers with medium ($M = 8.83$) and low levels of narcissism ($M = 7.82$). A *Tukey* test was revealed that there was a statistical difference between each level.

[59] See table 1 in Appendix A.
[60] See table 2 in Appendix A.

[61] See table 3 in Appendix A.

Hypothesis 1-2 stated that hackers with high narcissism would report more angry reaction scores than hackers with low narcissism. As above, mean levels of hackers' angry reaction scores were compared across hacker groups representing the three different levels of narcissism. A one-way ANOVA indicated a significant difference in hackers' angry reaction scores across the three levels of hackers' narcissism (Table 5.2) and supported hypothesis 1-2 (p < .001). Hackers who belong to the high narcissism category scored the highest (*M* = 10.55), followed by the medium level of narcissism (*M* = 9.24) and the low level of narcissism (*M* = 8.40). A *Tukey t* test was indicated that all three groups were statistically different from one another.

Hypothesis 1-3 stated that hackers with high narcissism would report higher angry behavior scores than hackers with low narcissism. To test this hypothesis, mean levels of computer hackers' angry behavior scores were compared across hacker groups representing the three different levels of narcissism. Once again one-way ANOVA indicated significant difference in hackers' angry behavior scores across the three levels of hackers' narcissism (Table 5.3) and supported hypothesis 1-3 (p < .001). Hackers who belong to the high narcissism category showed the highest score (*M* = 5.27), followed by the medium level of narcissism (*M* = 4.79) and the low level of narcissism (*M* = 4.31). A *Tukey's t* test revealed that there was statistically different from one another.

The first research question concerned what kinds of factors in hackers' narcissism scores affected their aggressiveness. A multiple regression analysis was performed to examine which of the four factors of narcissism (F1: Center of attention; F2: Inflated confidence; F3: Control of others; F4: Fantasies of personal greatness) was associated with the dependent variable, aggressiveness as measured by the ten items mentioned earlier (e.g., I have a fiery temperament; I am infuriated when I get a poor evaluation; When I get mad, I say nasty things, etc). The findings indicated that all regression models revealed significant relationships between the four factors and the dependent variables (Table 5.4). The center of attention factor was positively correlated with all 10 items in angry temperament, reaction, and behavior items. Only two of the 10 items for the inflated confidence factor were significant. Of the two significant standardized betas, the fiery temperament item was positively related with inflated confidence factor while the hitting item was negatively related to inflated confidence. The control of others factor was positively correlated with the six items of all aggressiveness items. Nine of the 10 items for the fantasies of personal greatness were significant. Concerning the relationship between hackers' narcissism and their aggressiveness, the center of attention and fantasies of personal greatness factors have relatively stronger influence on their anger temperament, reaction, and behaviors than other two factors (inflated confidence and control of others).

Hackers' Motivations and Aggressiveness

Hypothesis 2-1 stated that hackers with extrinsic motivations should exhibit more aggressiveness than hackers with intrinsic motivations. To assess this prediction, a 2 (intrinsic motivation: low and high) x 2 (extrinsic motivation: low and high) ANOVA was conducted on hackers' angry temperament, reaction, and behavior scores. For the angry temperament scale (Table 5.5), the results yielded a significant main effect of extrinsic motivation (p < .001). Hackers with a high level of the extrinsic motivation scored higher on the angry temperament score than those at the low level. In addition, there was an interaction effect (p < .01) but no main effect of intrinsic motivation.

Interaction between both motivations affected hackers' score on the angry temperament scale. For the angry reaction scale (Table 5.6), the findings indicated that there was a significant main effect of intrinsic motivation (p < .01) and extrinsic motivation (p < .01). In addition, there was an interaction effect (p< .05). The mean matrix in table 5.6 revealed that the higher intrinsic and extrinsic motivations, the higher the score on the angry reaction measure. For the angry behavior scores (Table 5.7), there was a significant main effect of extrinsic motivation (p < .01). In addition, an interaction effect (p < .05) was found. Although there was no main effect of intrinsic motivation, interaction between the motivations had an impact on the measure of angry behavior. The matrix of means indicated that the higher the extrinsic motivation, the more angry the behaviors. The mean score representing an interaction between high intrinsic and high extrinsic motivations was the highest on the angry behavior measure. Overall, these results partially supported the hypothesis 2-1.

Hypotheses 2-2 and 2-3 stated that some hacking activities, particularly non-reward hacking activities for no particular reason, curiosity, or boredom, etc. would be associated with intrinsic motivation and that the other hacking activities (such as reward oriented hacking to make money, hacking transnational corporations, or military web sites, etc.) would be related to extrinsic motivation. A multiple regression was performed to examine the relationship between the two different motivations and a variety of hacking activities (Table 5.8). Both motivations were strongly related with hacking activities on bank computer systems. The higher the extrinsic motivations, the more frequently hacking on bank computer systems while the higher intrinsic motivations, the less frequently hacking on bank computer systems. Both motivations were positively associated with hacking activities that attempted to get peer recognition. Both motivations were positively related with hacking for fun. Both motivations were positively correlated with no particular reason for hacking and were significantly related with hacking to check security on others' computer. Hacking for boy/girl friends was positively related to extrinsic motivation while intrinsic motivation was not associated with showing off their skills to boy/girl friends. Hacking against other nations, other religions, other ethnicities, and hacking for stopping porn sites revealed that extrinsic motivation was positively related with those hacking activities while intrinsic motivation was not associated with them. Both motivations were positively associated with hacking for demonstrating information should be free. Computer hacking for earning money was explained by only extrinsic motivation not by intrinsic motivation. Both motivations were positively associated with hacking for curiosity and boredom. Only extrinsic motivation was positively related with hacking against transnational corporations, secret agencies, and military web sites. Both motivations were positively related with hacking against university web sites and personal homepages. Only extrinsic motivation was correlated with hacking against big companies, designing computer viruses, and small companies.

Hackers' Levels of Flow and Hacking Involvement

Hypothesis 3-1 proposed that hackers who feel a high level of flow would be more frequently involved in hacking activities than hackers with a low level of flow. To assess the relationship between hackers' flow levels and hacking frequency and hacking activities, a one-way ANOVA was performed (Table 5.9). The results indicated that there were significant differences in the frequency of the breaking into somebody else's computer systems across the three levels of flow ($p < .001$). Hackers who feel a high level of flow (*M* = 2.16) did most frequently break into others' computer systems, followed by hackers with a medium level of flow (*M* = 1.27) and a low level of flow (*M* = 0.88). A post hoc test (*Tukey*) revealed that high flow group was significantly different from each level. Table 5.10 shows a one-way ANOVA result on the frequency of changing others' web sites. The findings revealed that there were significant differences in the frequency of changing others' web sites across the three levels of flow ($p < .001$). Hackers who feel a high level of flow (*M* = 1.23) did most frequently change others' web sites, followed by hackers with a medium level of flow (*M* = 0.72) and a low level of flow (*M* = 0.35). A post hoc test (*Tukey*) revealed that flow group means were significantly different from each other level. Table 5.11 also indicated that there were statistically significant differences in a variety of hacking activities (22 different hacking activities) across the three different levels of flow ($p < .001$). All 22 items regarding hacking activities revealed that there were significantly different among different flow levels. A series of post hoc test was performed to differentiate one level from the other (See table 5.11).

The second research question concerned what dimensions of flow make hackers get involved in hacking activities. A series of multiple regression analyses was performed between the dependent variable (22 hacking activities) and the independent variables (the four factors of flow: challenge-skill balance, concentration on task at hand, loss of self consciousness, autotelic experience). The results (Table 5.12) indicated that the challenge-skill balance factor was significantly related with all hacking activities. Only three of the 22 hacking activities for concentration on tasks at hand were significant. The loss of self-consciousness factor was associated with only one hacking activity (hacking against other religions). Eight out of 22 hacking activities were closely related with autotelic experience factor. Interestingly, non-reward oriented hacking activities such as just for fun, curiosity, and boredom were positively associated with autotelic experience whereas reward oriented hacking activities such as breaking into banking systems, transnational corporations, secret agency, military web sites, and hacking against other nations were negatively related with this factor. That is, the more frequently hackers pursue reward oriented hacking activities (extrinsic motivated hacking activities), the lower they feel the autotelic experience while the more frequently they pursue non-rewarded hacking (intrinsic motivated hacking activities), the more they feel the autotelic experience.

Hackers' Cultural Worldviews and Aggressiveness

Hypothesis 4-1 stated that hackers with high nationalism would display more aggressiveness than other hackers with low nationalistic ideology when the hackers feel any threat to their own worldview from other sources. A one-way ANOVA was conducted to assess computer hackers' angry temperament, reaction, and behavior scores across the three different levels of nationalism (Table 5.13). The results indicated that there were significant differences in the measures of angry temperament ($p < .001$), angry reactions ($p < .05$), and angry behaviors ($p < .01$) across the three levels of nationalism. The mean matrix of computer hackers' nationalism and aggressiveness revealed that hackers who have high nationalism (*M* = 9.95) showed the highest angry temperament scores, followed by the medium group (*M* = 9.28) and the low group (*M* = 8.07). A post hoc test (*Tukey*) indicated that the low group was different from the other two groups, but there was no difference between the medium and the high nationalism group. For the angry reaction scale, hackers who have high nationalism (*M* = 10.26) showed the highest angry reaction, followed by the medium group (*M* = 9.57) and the low group (*M* = 9.02). A post hoc test (*Tukey*) indicated that the high group was different from the low and medium groups, but there was no difference between the low and the medium groups. For the angry behavior scale, hackers who have high nationalism (*M* = 5.27) showed the highest angry behavior score, followed by the medium group (*M* = 4.99) and the low group (*M* = 4.39). A post hoc test (*Tukey*) indicated that the low group was different from the medium and high groups, but there was no difference between the medium and the high groups.

Hypothesis 4-2 stated that hackers with high religious pride would have more aggressiveness than other hackers with low religious pride when the hackers feel any threat to their own worldview from other religions. A one-way ANOVA was conducted to assess computer hackers' angry temperament, reaction, and behavior scores across the three different levels of religious pride (Table 5.14). The results indicated that there were significant differences on the angry temperament ($p < .01$) and angry reaction ($p < .01$) scales across the three levels of religious pride. However, there was no significant result concerning angry behavior scores. The mean matrix of hackers' aggressiveness and religious pride revealed that hackers who have high religious pride (*M* = 10.15) showed the highest angry temperament scores, followed by the medium group (*M* = 8.76) and the low group (*M* = 8.68). A post hoc test (*Tukey*) indicated that the high group was different from the other two groups, but there was no difference between the low and the medium groups in the religious pride index. For the angry reaction measure, hackers who have high religious pride (*M* = 10.64) showed the highest angry reaction score, followed by the medium group (*M* = 9.79) and the low group (*M* = 9.17). A post hoc test (*Tukey*) indicated that the high group was different from the low and medium groups, but there was no difference between the low and the medium groups. For the angry behavior measure, there were no significant results.

Hypothesis 4-3 stated that hackers with more ethnic coercion would display more aggressiveness than the other hackers with less ethnic coercion when hackers feel any threat to their own worldview from other ethnic groups. A one-way ANOVA was conducted to assess hackers' angry temperament, reaction, and behavior scores across the three different levels of ethnic coercion (Table 5.15). The results indicated that there were significant differences in only the angry reaction index across the three levels of ethnic coercion (p < .01). There were no significant results concerning angry temperament and behavior scores. The mean matrix of hackers' aggressiveness and ethnic coercion revealed that hackers who have high ethnicity coercion (*M* = 10.20) showed the highest angry reaction, followed by the low group (*M* = 9.06) and the medium group (*M* = 9.04). A post hoc test (*Tukey*) indicated that the high group was different from the other two groups, but there was no difference between the low and the medium groups in ethnic coercion.

The third research question examined which psychological mindset was closely associated with the dependent variable, hacking intention against other nations. Along with demographic variables of gender, age, and education, the psychological variables such as narcissism (center of attention, inflated confidence, control of others, and fantasies of personal greatness), aggressiveness (angry temperament, angry reaction, and angry behaviors), motivations (intrinsic and extrinsic motivations), flow (challenge-skill balance, concentration on task at hand, loss of self-consciousness, and autotelic experience) and cultural worldviews (nationalism, religious pride, and ethnic coercion) were entered into the regression equation. A multiple regression was performed to investigate which factors significantly predicted hacking intention against other nations. The results of the regression are presented in Table 5.16. The findings revealed that demographic variables did not correlate with the intention to hack against other nations. Of the narcissism index, only the fantasy of personal greatness dimension was positively correlated with hacking intentions against other nations. Of the aggressiveness index, only the angry behavior factor was positively correlated with the dependent variable. Of the motivations index, only extrinsic motivation was positively correlated with hacking intentions against other nations. Of the flow index, concentration on task at hand factor was positively correlated with hacking intentions against other nations while autotelic experience was negatively associated with the dependent variable. In cultural worldview index, only nationalism was positively correlated with the hacking intention against other nations.

Table 5.1 One-way ANOVA for hackers' angry temperament by their narcissism levels

Source	SS	*df*	MS	*F*	*P*
Between group	388.46	2	194.23	17.16	< .001
Within group	6641.22	587	11.31		
Total	7029.68	589			

Mean matrix of computer hackers' narcissism and angry temperament

	Narcissism levels					
	Low		Medium		High	
Variable	*M*	*SD*	*M*	*SD*	*M*	*SD*
Angry temperament	7.82[a] (*n*=178)	2.95	8.83[b] (*n*=223)	3.40	9.88[c] (*n*=189)	3.66

Note. The higher the mean, the more angry the temperament. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the following items (e.g., I have a fiery temperament; I am quick-tempered; I am a hot-headed person; I fly off the handle). The angry temperament scores in above four items were summed. The total angry temperament score was ranged from 4 to 16. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test.

Table 5.2 One-way ANOVA for hackers' angry reaction by their narcissism levels

Source	SS	*df*	MS	*F*	*P*
Between group	388.46	2	215.35	19.98	< .001
Within group	6324.72	587	10.77		
Total	6755.43	589			

Mean matrix of computer hackers' narcissism and angry reaction

	Narcissism levels					
	Low		Medium		High	
Variable	*M*	*SD*	*M*	*SD*	*M*	*SD*
Angry reaction	8.40^{a} (*n*=175)	2.83	9.24^{b} (*n*=225)	3.33	10.55^{c} (*n*=190)	3.58

Note. The higher the mean, the more angry the reaction. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the following items (e.g., I am infuriated when I get a poor evaluation; I am furious when criticized; I am annoyed when not given recognition; I am angry when slowed down by other). The angry reaction scores in above four items were summed. The total angry reaction score was ranged from 4 to 16. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test.

Table 5.3 One-way ANOVA for hackers' angry behaviors by their narcissism levels

Source	SS	*df*	MS	*F*	*P*
Between group	84.67	2	42.33	10.91	< .001
Within group	2303.39	594	3.87		
Total	2388.07	596			

Mean matrix of computer hackers' narcissism and angry behaviors

	Narcissism levels					
	Low		Medium		High	
Variable	*M*	*SD*	*M*	*SD*	*M*	*SD*
Angry reaction	4.31^{a} (*n*=236)	1.88	4.79^{b} (*n*=185)	1.98	5.27^{c} (*n*=161)	2.02

Note. The higher the mean, the more angry the behavior. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the following items (e.g., When I get mad, I say nasty things; When frustrated, feel like hitting). The angry behavior scores in above two items were summed. The total angry behavior score was ranged from 2 to 8. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test.

Table 5.4 Multiple regression for predicting hackers' aggressiveness by narcissism sub-factors

Items	F1	F2	F3	F4	R^2	AR^2	*F*	*df*
Angry temperament								
I have a fiery temperament	$.12^{**}$	$.08^{*}$	.05	$.16^{**}$	.09	.08	14.56^{***}	4,596
I am quick-tempered	$.18^{***}$	-.04	.04	$.10^{*}$	.06	.06	9.72^{**}	4,596
I am a hot-headed person	$.14^{**}$	-.03	$.09^{*}$	$.10^{*}$	.05	.05	8.35^{***}	4,593
I fly off the handle	$.15^{**}$	-.07	.04	.09	.04	.03	6.10^{***}	4,591
Angry reaction (I am angry~)								
when I get a poor evaluation	$.16^{***}$	-.06	$.11^{**}$	$.12^{*}$	.07	.06	11.23^{***}	4,592
when criticized	$.16^{***}$	-.08	.06	$.12^{*}$	.05	.04	8.54^{***}	4,595
when not given recognition	$.27^{***}$	-.00	$.09^{*}$	$.11^{*}$	.13	.12	21.27^{***}	4,593
when slowed down	$.15^{**}$	-.04	$.13^{**}$	$.12^{**}$	.08	.07	12.32^{***}	4,596
Angry behaviors								
When I get mad, I say nasty things	$.09^{*}$	-.00	$.09^{*}$	$.08^{*}$	.04	.03	5.36^{***}	4,596
When frustrated, feel like hitting	$.15^{***}$	$-.12^{**}$	$.08^{*}$	$.17^{***}$	.08	.07	11.14^{***}	4,593

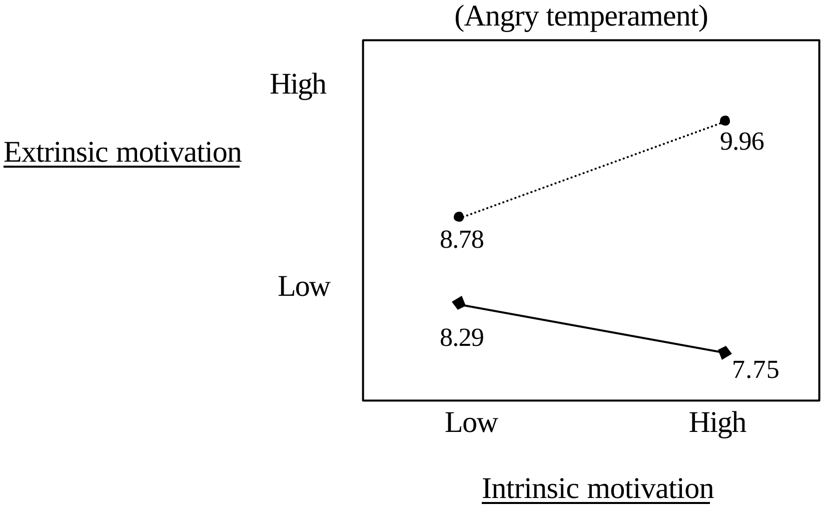
* $p < .05$
** $p < .01$
*** $p < .001$

Note. F1= Center of attention in a narcissism construct; F2= Inflated confidence in a narcissism construct; F3= Control of others in a narcissism construct; F4= Fantasies of personal greatness. AR^2= Adjusted R square. The numbers in a cell are standardized coefficients betas.

Table 5.5 Two-way ANOVA for hackers' angry temperament by intrinsic and extrinsic motivations

Source	SS	*df*	MS	*F*	*eta*^{2}
Intrinsic motivation	14.51	1	14.51	1.32	.002
Extrinsic motivation	259.11	1	259.11	23.68***	.038
Interaction	106.34	1	106.34	9.72**	.016
Error	6619.29	605	10.94		
Total	53922.00	609			

$^{*}p < .05$
$^{**}p < .01$
$^{***}p < .001$



Mean matrix of computer hackers' angry temperament and motivations

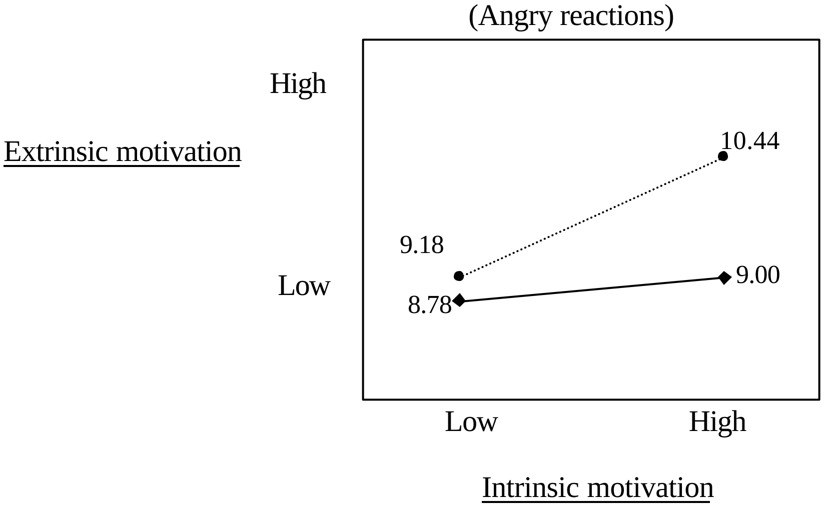
		Intrinsic motivation	
		Low	High
Extrinsic motivation	Low	8.29 (*n*=204)	7.75 (*n*=110)
	High	8.78 (*n*=120)	9.96 (*n*=175)

Note. The higher the mean, the more angry the temperament. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the following items (e.g., I have a fiery temperament; I am quick-tempered; I am a hot-headed person; I fly off the handle). The angry temperament scores in above four items were summed. The total angry temperament score was ranged from 4 to 16. Each intrinsic and extrinsic motivation scores also were summed and the resulting distribution was divided by two levels: "low" = 1 and "high" =2.

Table 5.6 Two-way ANOVA for hackers' angry reaction by intrinsic and extrinsic motivations

Source	SS	*df*	MS	*F*	eta^2
Intrinsic motivation	77.96	1	77.96	7.26^{**}	.012
Extrinsic motivation	121.04	1	121.04	11.27^{**}	.018
Interaction	39.68	1	39.68	3.69^{*}	.006
Error	6486.92	604	10.74		
Total	60271.00	608			

* p < .05
** p < .01
*** p < .001



Mean matrix of computer hackers' angry reaction and motivations

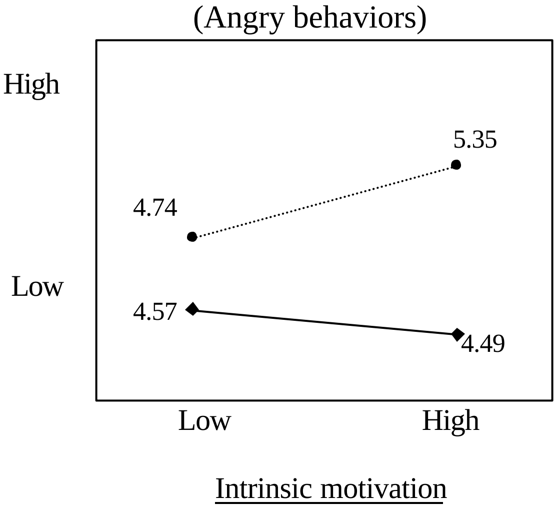
		Intrinsic motivation	
		Low	High
Extrinsic motivation	Low	8.78 (*n*=203)	9.00 (*n*=110)
	High	9.18 (*n*=121)	10.44 (*n*=174)

Note. The higher the mean, the more angry the reaction. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the following items (e.g., I am infuriated when I get a poor evaluation; I am furious when criticized; I am annoyed when not given recognition; I am angry when slowed down by others). The angry reaction scores in above four items were summed. The total angry reaction score was ranged from 4 to 16. Each intrinsic and extrinsic motivation score also was summed and the resulting distribution was divided by two levels: "low" = 1 and "high" = 2.

Table 5.7 Two-way ANOVA for hackers' angry behaviors by intrinsic and extrinsic motivations

Source	SS	*df*	MS	*F*	*Eta*^{2}
Intrinsic motivation	9.96	1	9.96	2.58	.004
Extrinsic motivation	38.74	1	38.74	10.04**	.016
Interaction	17.41	1	17.41	4.51*	.007
Error	2361.72	612			
Total	16718.00	616			

* p < .05
** p < .01
*** p < .001



Mean matrix of computer hackers' angry behaviors and motivations

		Intrinsic motivation	
		Low	High
Extrinsic motivation	Low	4.57 (*n*=205)	4.49 (*n*=114)
	High	4.74 (*n*=122)	5.35 (*n*=175)

Note. The higher the mean, the more angry the behaviors. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the following items (e.g., when I get mad, I say nasty things; when frustrated, feel like hitting). The angry behavior scores in above two items were summed. The total angry behavior score was ranged from 2 to 8. Each intrinsic and extrinsic motivation score also was summed and the resulting distribution was divided by two levels: "low" = 1 and "high" = 2.

Table 5.8 Multiple regression for predicting hacking activities by intrinsic and extrinsic motivations

Hacking activities	Banking systems	Peer recognition	Just for fun	No particular reason	Security checking	Boy/Girl friends
Intrinsic	$-.14^{***}$	$.13^{**}$	$.19^{***}$	$.13^{**}$	$.13^{**}$	.07
Extrinsic	$.41^{***}$	$.35^{***}$	$.29^{***}$	$.27^{***}$	$.14^{**}$	$.38^{***}$
R^2	.14	.18	.16	.12	.05	.17
Adjusted R^2	.14	.17	.15	.11	.05	.16
F	53.72^{***}	70.40^{***}	60.96^{***}	41.74^{***}	17.98^{***}	64.63^{***}
Df	2,647	2,648	2,649	2,645	2,648	2,650

Hacking activities	Other nations	Other religions	Other ethnicities	Stopping porn sites	Information should be free	Making money
Intrinsic	-.03	-.02	.01	-.02	$.19^{***}$	-.02
Extrinsic	$.33^{***}$	$.39^{***}$	$.37^{***}$	$.23^{***}$	$.21^{***}$	$.43^{***}$
R^2	.10	.15	.14	.05	.12	.18
Adjusted R^2	.10	.15	.13	.05	.11	.18
F	37.19^{***}	57.83^{***}	53.17^{***}	17.13^{***}	42.25^{***}	70.53^{***}
Df	2,646	2,647	2,645	2,643	2,647	2,642

Hacking activities	Curiosity	Boredom	Transnational corporations	Secret agency	Military web sites
Intrinsic	$.27^{***}$	$.16^{***}$	-.02	-.06	-.04
Extrinsic	$.15^{***}$	$.28^{***}$	$.45^{***}$	$.45^{***}$	$.41^{***}$
R^2	.13	.14	.19	.18	.16
Adjusted R^2	.12	.13	.19	.18	.15
F	46.04^{***}	50.15^{***}	77.44^{***}	72.76^{***}	59.36^{***}
Df	2.645	2,638	2,645	2,646	2,646

Hacking activities	University web sites	Personal home pages	Big company	Designing computer virus	Small company
Intrinsic	$.11^{**}$	$.09^{*}$	-.00	.06	.05
Extrinsic	$.26^{***}$	$.30^{***}$	$.39^{***}$	$.29^{***}$	$.35^{***}$
R^2	.10	.12	.15	.11	.15
Adjusted R^2	.09	.12	.15	.10	.15
F	36.43^{***}	43.99^{***}	56.10^{***}	37.49^{***}	56.08^{***}
Df	2,644	2,646	2,647	2,642	2,645

$^{*}p < .05$
$^{**}p < .01$
$^{***}p < .001$

Table 5.9 One-way ANOVA for hackers' frequency of breaking into computer systems by different flow levels

Source	SS	*df*	MS	*F*	*P*
Between group	170.62	2	85.31	26.37	< .001
Within group	1749.65	541	3.23		
Total	1920.27	543			

Mean matrix of the frequency of hackers' breaking into computer systems and flow levels

	Flow levels					
	Low		Medium		High	
Variable	*M*	*SD*	*M*	*SD*	*M*	*SD*
Breaking into Computer systems	0.82^a (*n*=185)	1.46	1.27^b (*n*=178)	1.70	2.16^c (*n*=181)	2.16

Note. The higher the mean, the more the frequency of breaking into others' computer systems. Subjects were asked to check on a scale: "never" = 0, "1-2" = 1, "3-5" = 2, "6-10" = 3, "11-20" = 4, "21-30" = 5, "more than 31" =of the items (e.g., In the last month, how often did you break into somebody else's computer systems?). The flow scores were summed and the resulting distribution was trichotomized to form three levels: "low" = 1, "medium"= 2," and "high" = 3. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test.

Table 5.10 One-way ANOVA for hackers' frequency of changing others' web sites by different flow levels

Source	SS	*df*	MS	*F*	*P*
Between group	72.35	2	36.17	17.01	< .001
Within group	1150.45	541	2.12		
Total	1222.81	543			

Mean matrix of the frequency of hackers' web site alteration and flow levels

	Flow levels					
	Low		Medium		High	
Variable	*M*	*SD*	*M*	*SD*	*M*	*SD*
Changing others' web sites	0.35[a] (*n*=185)	1.01	0.72[b] (*n*=178)	1.39	1.23[c] (*n*=181)	1.85

Note. The higher the mean, the more the frequency of changing others web sites. Subjects were asked to check on a scale: "never" = 0, "1-2" = 1, "3-5" = 2, "6-10" = 3, "11-20" = 4, "21-30" = 5, "more than 31" =of the items (e.g., In the last month, how often did you alter or change others' web sites?). The flow scores were summed and the resulting distribution was trichotomized to form three levels: "low" = 1, "medium"= 2," and "high" = 3. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test.

Table 5.11 One-way ANOVA for frequency of hacking activities by three different flow levels

Items	Mean scores of the frequency of hacking activities by different flow levels				
	Low	Medium	High	*F*	*df*
Banking systems	0.18^{a} (0.63)	0.31^{a} (0.78)	0.61^{b} (1.12)	11.69^{***}	2,538
Peer recognition	0.47^{a} (0.87)	0.77^{b} (0.97)	1.38^{b} (1.35)	33.05^{***}	2,537
Just for fun	1.13^{a} (1.10)	1.40^{a} (1.16)	2.02^{b} (1.46)	24.16^{***}	2,539
No particular reason	0.73^{a} (1.03)	0.77^{a} (1.02)	1.48^{b} (1.53)	21.46^{***}	2,534
Security checking	1.11^{a} (1.22)	1.55^{b} (1.27)	2.26^{c} (1.42)	35.43^{***}	2,536
Boy/girl friends	0.49^{a} (1.00)	0.44^{a} (0.87)	0.87^{b} (1.35)	8.35^{***}	2,539
Other nations	0.36^{a} (0.81)	0.77^{b} (1.23)	1.15^{c} (1.41)	20.27^{***}	2,537
Other religions	0.23^{a} (0.75)	0.29^{a} (0.79)	0.77^{b} (1.35)	15.41^{***}	2,537
Other ethnicities	0.21^{a} (0.70)	0.60^{b} (1.10)	1.05^{c} (1.42)	25.39^{***}	2,536
Stopping porn sites	0.43^{a} (0.92)	0.64^{a} (1.12)	1.08^{b} (1.53)	13.36^{***}	2,533
Information should be free	0.83^{a} (1.12)	1.27^{b} (1.42)	2.23^{c} (1.56)	49.00^{***}	2,536
Making money	0.15^{a} (0.53)	0.27^{a} (0.75)	0.67^{b} (1.21)	17.01^{***}	2,532
Curiosity	1.28^{a} (1.16)	1.84^{b} (1.33)	2.16^{b} (1.45)	20.52^{***}	2,535
Boredom	0.95^{a} (1.17)	1.19^{a} (1.24)	1.71^{b} (1.51)	15.20^{***}	2,528
Transnational corporations	0.26^{a} (0.81)	0.45^{a} (1.04)	0.93^{b} (1.36)	18.02^{***}	2,534
Secret agency	0.24^{a} (0.80)	0.40^{a} (0.95)	0.79^{b} (1.30)	13.33^{***}	2,536
Military web sites	0.25^{a} (0.77)	0.37^{a} (0.88)	0.82^{b} (1.29)	15.96^{***}	2,535
University web sites	0.71^{a} (1.04)	1.03^{a} (1.23)	1.67^{c} (1.47)	26.92^{***}	2,533
Personal home pages	1.00^{a} (1.16)	1.33^{b}(1.23)	1.91^{c} (1.45)	22.93^{***}	2,536
Big company	0.47^{a} (0.96)	0.75^{a} (1.25)	1.31^{b} (1.47)	23.36^{***}	2,537
Designing computer virus	0.71^{a} (1.06)	1.18^{b} (1.24)	1.63^{c} (1.43)	23.97^{***}	2,532
Small company	0.58^{a} (1.03)	0.93^{b} (1.17)	1.38^{c} (1.46)	19.30^{***}	2,535

* p < .05
** p < .01
*** p < .001

Note. The higher the mean, the more the frequency of hacking activities. The numbers in parentheses are standard deviations. Subjects were asked to check on a scale: “never” = 0, “a few” = 1, “sometimes” = 2, “frequently” = 3, “very frequently” = 4 on the 22 items concerning diverse hacking activities. The flow scores were summed and the resulting distribution was trichotomized to form three levels: “low” = 1, “medium”= 2,” and “high” = 3. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*’s *t* test.

Table 5.12 Multiple regression for predicting hacking activities by flow sub-dimensions

Items	Flow 1	Flow 2	Flow 3	Flow 4	R^2	AR^2	F	df
Banking systems	$.37^{***}$	.05	.11	$-.21^{***}$	.14	.13	22.49^{***}	4,535
Peer recognition	$.32^{***}$	-.01	.07	.08	.16	.15	24.47^{***}	4,535
Just for fun	$.20^{***}$	.12	-.08	$.16^{**}$	.12	.11	17.80^{***}	4,537
No particular reason	$.15^{**}$	$.14^{*}$	-.05	.06	.07	.07	10.38^{***}	4,532
Security checking	$.45^{***}$	.03	.08	-.06	.22	.22	38.07^{***}	4,534
Boy/girl friends	$.18^{***}$	-.02	-.01	.01	.03	.02	4.35^{**}	4,537
Other nations	$.37^{***}$	.11	.05	-12^{*}	.17	.16	26.56^{***}	4,535
Other religions	$.27^{***}$	.06	$.12^{*}$	-.09	.11	.10	15.78^{***}	4,535
Other ethnicities	$.38^{***}$	$.14^{*}$	.03	-.11	.18	.17	29.02^{***}	4,534
Stopping porn sites	$.31^{***}$	.01	-.01	-.02	.09	.08	13.18^{***}	4,531
Information should be free	$.30^{***}$	.08	.07	.05	.17	.16	27.05^{***}	4,534
Making money	$.22^{***}$	.04	.04	.04	.08	.07	11.74^{***}	4,530
Curiosity	$.12^{*}$	.08	-.03	$.19^{**}$	.09	.08	13.21^{***}	4,533
Boredom	$.18^{***}$	.03	-.05	$.15^{**}$	.08	.07	10.61^{***}	4,536
Transnational corporations	$.38^{***}$	.06	.03	$-.13^{*}$	.14	.13	21.28^{***}	4,532
Secret agency	$.38^{***}$	.08	.01	$-.14^{*}$	.13	.13	20.57^{***}	4,534
Military web sites	$.35^{***}$	.09	.03	$-.13^{*}$	.13	.12	19.50^{***}	4,533
University web sites	$.27^{***}$	.11	.02	-.01	.12	.11	17.19^{***}	4,531
Personal home pages	$.22^{***}$	.11	.02	.02	.08	.08	12.85^{***}	4,534
Big company	$.40^{***}$	.07	.02	-.09	.17	.16	26.35^{***}	4,535
Designing computer virus	$.29^{***}$	$.17^{**}$	-.01	-.08	.13	.12	18.87^{***}	4,530
Small company	$.29^{***}$	.05	-.02	-.06	.12	.11	18.14^{***}	4,533

* p < .05
**p < .01
***p < .001

Note. Flow 1= Challenge-skill balance; Flow 2= Concentration on task at hand; Flow 3= Loss of self consciousness; Flow 4= Autotelic experience. AR^2= Adjusted R square. The numbers in a cell of the factor columns are standardized coefficients betas.

Table 5.13 One-way ANOVA for hackers' aggressiveness by different levels of nationalism

Items	Source	SS	*df*	MS	*F*	*p*
Angry temperament	Between group	252.13	2	126.07	11.14	< .001
	Within group	4628.31	409	11.31		
	Total	4880.45	411			
Angry reaction	Between group	104.87	2	52.43	4.69	< .05
	Within group	4575.81	410	11.16		
	Total	4680.69	412			
Angry behaviors	Between group	56.19	2	28.09	7.20	< .01
	Within group	1617.90	415	3.89		
	Total	1674.09	417			

Mean matrix of hackers' aggressiveness and nationalism levels

	Nationalism					
	Low		Medium		High	
	M	*SD*	*M*	*SD*	*M*	*SD*
Angry temperament	8.07^{a}	3.38	9.28^{b}	3.22	9.95^{b}	3.48
	(*n*=152)		(*n*=138)		(*n*=122)	
Angry reaction	9.02^{a}	3.18	9.57^{a}	3.11	10.26^{b}	3.74
	(*n*=152)		(*n*=138)		(*n*=123)	
Angry behaviors	4.39^{a}	1.98	4.99^{b}	1.87	5.27^{b}	2.07
	(*n*=154)		(*n*=142)		(*n*=122)	

Note. The higher the mean, the more angry the temperament, reaction, and behaviors. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the 4 items concerning angry temperament; 4 items concerning angry reactions; 2 items concerning angry behaviors. All items of each aggressiveness factor were summed, respectively. The total score of angry temperament was ranged from 4 to 16; The total score of angry reaction was ranged from 4 to 16; The total score of angry behaviors was ranged from 2 to 8. Nationalism index also was summed and the resulting distribution was trichotomized to form three levels: "low" =1, "medium" = 2, and "high" = 3. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test. The slightly differences in *N*s are due to missing variables.

Table 5.14 One-way ANOVA for hackers' aggressiveness by different levels of religious pride

Items	Source	SS	*df*	MS	*F*	*p*
Angry temperament	Between group	141.38	2	70.69	5.80	< .01
	Within group	3826.75	314	12.18		
	Total	3968.13	316			
Angry reaction	Between group	124.19	2	62.09	5.26	< .01
	Within group	3646.98	309	11.80		
	Total	3771.17	311			
Angry behaviors	Between group	14.51	2	7.25	1.84	*ns*
	Within group	1237.85	315	3.93		
	Total	1252.36	317			

Mean matrix of hackers' aggressiveness and religious pride levels

	Religious pride					
	Low		Medium		High	
	M	*SD*	*M*	*SD*	*M*	*SD*
Angry temperament	8.68^{a}	3.31	8.76^{a}	3.26	10.15^{b}	3.88
	(*n*=141)		(*n*=76)		(*n*=100)	
Angry reaction	9.17^{a}	3.21	9.79^{a}	3.17	10.64^{b}	3.90
	(*n*=141)		(*n*=73)		(*n*=98)	
Angry behaviors	4.67	2.06	4.93	1.81	5.17	1.98
	(*n*=142)		(*n*=77)		(*n*=99)	

Note. The higher the mean, the more angry the temperament, reaction, and behaviors. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the 4 items concerning angry temperament; 4 items concerning angry reactions; 2 items concerning angry behaviors. All items of each aggressiveness factor were summed, respectively. The total score of angry temperament was ranged from 4 to 16; The total score of angry reaction was ranged from 4 to 16; The total score of angry behaviors was ranged from 2 to 8. Religious pride index also was summed and the resulting distribution was trichotomized to form three levels: "low" =1, "medium" = 2, and "high" = 3. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test. The slightly differences in *N*s are due to missing variables.

Table 5.15 One-way ANOVA for hackers' aggressiveness by different levels of ethnic coercion

Items	Source	SS	*df*	MS	*F*	*p*
Angry temperament	Between group	15.72	2	7.86	0.66	*ns*
	Within group	4740.01	403	11.76		
	Total	4755.73	405			
Angry reaction	Between group	101.43	2	50.71	4.92	< .01
	Within group	4187.68	407	10.28		
	Total	4289.12	409			
Angry behaviors	Between group	8.85	2	4.42	1.12	*ns*
	Within group	1614.52	411	3.92		
	Total	1623.37	413			

Mean matrix of hackers' aggressiveness and ethnic coercion

	Ethnic coercion					
	Low		Medium		High	
	M	*SD*	*M*	*SD*	*M*	*SD*
Angry temperament	8.38	3.54	8.74	3.28	8.92	3.58
	(*n*=102)		(*n*=201)		(*n*=103)	
Angry reaction	9.04^{a}	3.06	9.06^{a}	3.14	10.20^{b}	3.46
	(*n*=102)		(*n*=204)		(*n*=104)	
Angry behaviors	4.65	2.05	4.67	1.92	5.00	2.02
	(*n*=103)		(*n*=205)		(*n*=106)	

Note. The higher the mean, the more angry the temperament, reaction, and behaviors. Subjects were asked to check on a scale "almost never" = 1, "sometimes" = 2, "often" = 3, and "almost always" = 4 of the 4 items concerning angry temperament; 4 items concerning angry reactions; 2 items concerning angry behaviors. All items of each aggressiveness factor were summed, respectively. The total score of angry temperament was ranged from 4 to 16; The total score of angry reaction was ranged from 4 to 16; The total score of angry behaviors was ranged from 2 to 8. Ethnic coercion index also was summed and the resulting distribution was trichotomized to form three levels: "low" =1, "medium" = 2, and "high" = 3. Post hoc tests of mean differences were also reported. The superscripts letter within each cell identifies significant differences from other cells at the .05 level via a *Tukey*'s *t* test. The slightly differences in *N*s are due to missing variables.

Table 5.16 Multiple regression for predicting hackers' intention against other nations by diverse psychological and demographic variables

Items	Hacking intention against other nations	*t*
Demographic		
Gender	.10	1.23
Age	.05	.49
Education	-.01	-.12
Narcissism		
Center of attention	-.02	-.18
Inflated confidence	-.04	-.49
Control to others	-.09	-.98
Fantasies of personal greatness	$.20^{*}$	2.09
Aggressiveness		
Angry temperament	.09	.89
Angry reaction	-.15	-1.45
Angry behaviors	$.20^{*}$	2.45
Motivations		
Intrinsic	.08	.79
Extrinsic	$.31^{**}$	3.53
Flow		
Challenge-skill balance	-.06	-.61
Concentration on task at hand	$.26^{*}$	2.11
Loss of self-consciousness	-.02	-.13
Autotelic experience	$-.25^{*}$	-1.97
Cultural worldview		
Nationalism	$.41^{***}$	3.99
Religious pride	.04	.35
Ethnic coercion	.02	.17
R^2	.51	
AR^2	.41	
F	5.12^{***}	
Df	19, 93	

$^{*}p < .05$
$^{**}p < .01$
$^{***}p < .001$

Notes. The numbers in hacking intention against other nations column are standardized coefficient betas. All independent variables in this regression model were subjected to "collinearity diagnostics" in order to check multicollinearity. Tolerance proportions in each independent variable ranged from .59 ~ .93. "Since tolerance is a proportion, its values range from 0 to 1. A value close to 1 indicates that an independent variable has little of its variability explained by the other independent variables. A value close to 0 indicates that a variable is almost a linear combination of the other independent variables. Such data are called multicollinear. If any of the tolerances are smaller than 0.1, multicollinearity may be a problem" (Norusis, n.d.).

CHAPTER 6

DISCUSSION

The purpose of this study was to investigate hackers' psychological structure and its impact on their activities in cyberspace. Narcissism, intrinsic and extrinsic motivation, flow, and terror management theory were used as theoretic rationales to describe, explain, and predict hackers' aggressiveness, hacking frequency, and intention to hack against opposing nations. The results indicated that hackers with high narcissism displayed more aggressiveness than hackers with low narcissism. Intrinsic motivation as well as extrinsic motivation was partially associated with aggressiveness when examining the relationship between hackers' motivation and aggressiveness. In addition, hackers with a high flow level were more likely to break into others' computer systems and alter others' web sites than hackers with a low level of flow. Hackers strongly tied with nationalism tended to score higher on the measure of angry temperament, reaction, and behavior than hackers with low a level of nationalism. Nationalistic hackers had more intentions to hack against opponent nations with their hacking skills than those with less nationalistic hackers.

One of the most important points in this study is that it examines the hacking phenomenon using empirical methods and conducting an on-line survey with hackers all over the world. Most existing research on hackers and cyberterrorism has been based upon interviews from a few former computer hackers, newspaper articles that report on computer viruses, and government warnings about cyber crimes. Existing studies have not attempted to describe, explain, and predict the hacking phenomenon in empirical ways.

Many researchers have subdivided hacker communities into several groups depending on what they did, their hacking skill levels, and different generations, etc. However, the results of this study underscore that hackers' psychological mindsets are a complicated structure that is made even more complicated when examining self-esteem, motivations, flow, cultural worldviews, and other psychological variables. Therefore, this study recommends that hackers should be analyzed not only by the consequences of their hacking but also by their psychological structures. The inner and external reasons why they are involved in hacking activities will provide us with more systematic and in-depth understandings on hacking and its impact on people, society, culture, and international relationships.

Some researchers have argued that more sophisticated and theoretic descriptions, explanations, and predictions are needed to understand the diverse characteristics of hackers. One of goals in this study was to find appropriate theoretic rationales in order to interpret hackers' psychological mindsets. Such theories as self-esteem, motivation, flow, and the terror management model are useful to understand the relationship between hackers' psychological mindsets and their activities in cyberspace.

First, the concept of self-esteem provides valuable insights for understanding hackers' aggressiveness. Unstable high self-esteem, particularly a narcissistic personality, in a hacker proves to be one of the best predictors to estimate hackers' aggressive tendencies. In addition, of the four factors in the narcissism construct, the center of attention and the fantasy of personal greatness dimensions are closely related to hackers' aggressiveness. This study replicates the findings of Baumeister, *et al.* (2000) who found that people with high self-esteem based on egotism (e.g., self-appraisal) might be prone to violence because self-appraisal is so sensitive to ego-threats while people with high self-esteem and self-worth have immunity to ego threats and are able to ignore them.

However, it is impossible to verify the causal relationship between hackers' narcissism levels and their aggressiveness. Naturally aggressive hackers may have more narcissistic personalities than the hackers who have less aggressiveness. Furthermore, in examining the relationship between hackers' narcissism levels and hacking intention against other nations, unlike the relationship between hackers' narcissism and their aggressiveness, there was not a significant relationship between the two variables. In this sense, Baumeister *et al.* (2000)'s arguments should be considered. That is, narcissism seemed not so much as a direct cause of aggression but a risk factor that can contribute to increasing a violent response to a provocation. Therefore, the following condition seems plausible: When hackers with narcissistic personalities are questioned, contradicted, or disputed, they may aggress against the source of the threat in order to protect their ego.

Second, the relationship between hackers' intrinsic and extrinsic motivations and their aggressiveness was more complicated than this study predicted. Unlike previous studies, intrinsic motivation was also an influential element in hackers' aggressiveness, particularly, in their scores on the angry reaction scale. Although extrinsic motivation was more strongly related to aggressiveness, intrinsic motivation also affected hackers' aggressiveness. This result suggests that even if a hacker's activity in cyberspace is led by intrinsic motivations, the hacker may feel anger in a certain situation and might behave aggressively for the simple pleasure of it.

Concerning the relationship between hacking activities and motivations, according to previous studies, intrinsic motivation propels behaviors that people perform when they are free from demands, constraints, or rewards. The only reward is the spontaneous experience of interest and enjoyment. Therefore, intrinsic motivation entails curiosity, exploration, spontaneity, and interest in one's surroundings. However, the results of this study indicate that non-reward hacking activities (e.g., just for fun, no particular reason, boredom, or curiosity, etc) are also associated with hackers' extrinsic motivations. At this point, we need to consider Csikszentmihalyi and Rathunde's suggestion (1992), "intrinsic and extrinsic motivations are not mutually exclusive, and they can be present in consciousness at the same time (p. 58)."

That is, a hacker breaking into a computer system may be intrinsically rewarded because he is enjoying and getting pleasure while he deals with hacking a site never hacked before. At the same time, he may receive attention from the media or be admired for it by other hackers. Finally, he could get a reputation as well as enjoy the challenge of breaking a tightly protected web site. This assumes that intrinsically motivated hacking may be changed into extrinsically motivated hacking depending on a given situation. So, intrinsic and extrinsic motivation may not naturally occur but are dependent upon hackers' unexpected situations when they are involved in hacking.

Third, flow is an important factor to explain why hackers continue to break into others' computer systems or alter some else's web pages. Almost all studies concerning a hacker's motivations note that computer hacking is due to external factors (e.g., money, peer recognition, and bragging their skills, etc.) around a hacker. Internal factors in a hackers' psychological structure have not been paid much attention. In this sense, that the optimal experience (flow) in a hacker's psychological state makes them keep hacking provides a reason for understanding addiction to hacking. More interestingly, however, the dimension of challenge-skill balance had more significant beta weights than did the autotelic experience dimension. This may indicate that the enjoyment dimension seems less central than other aspects of flow to hackers. Enjoyment or happiness during hacking would be maximally produced when a hacker successfully copes with given challenge in cyberspace. That is, hacking itself does not give any satisfaction. When the hacker's skill meets the challenge, the hacker is able to feel flow.

In addition, the results indicate that reward oriented hacking activities (e.g., hacking to bank system, other nations, transnational corporations, secret agency, and military web sites) were negatively related to autotelic experience dimension. When hackers frequently break into these computer systems for some particular reasons, the hackers do not feel these activities are worth doing for their own sake even if they feel high challenge-skill balance. This tendency suggests that even if hackers face a difficult challenge (the situation that would be needed a high level of hacking skills), flow in the hacker could be diminished if they have extrinsically motivated purposes. Consequently, flow can be maximized in the combined situation of a high level of challenge with hackers' intrinsically motivated goals. This confirms that flow is an intrinsically enjoyable state.

Finally, terror management theory gives a theoretic rational to explain the possibility of cyberterrorism or cyber-warfare in international levels. Threats to hackers' cultural worldviews can be a starting point of a war in cyberspace. Of all the hackers' cultural worldviews, nationalism was a strongly significant factor related to hackers' aggressiveness. This indicates that politically motivated hackers, when they feel any threat to their nation, may try to attack opposing countries in order to manage their own psychological terror. One main finding is that a regression equation makes it possible to estimate hacking intention against other nations. Fantasies of personal greatness, angry behaviors, extrinsic motivation, concentration on task at hand, autotelic experience, and nationalism in the regression model were significant factors in predicting a hacker's hacking intention to attack opposing nations. These factors can be used to build a portrait of the typical hacker who would be participated in cyberterrorism against other nations.

Concerning cyberterrorism toward a certain target, although cyber-warfare technique could in theory inflict great damage on civilian infrastructures such as power plants, financial systems, public transportations, and telecommunications, many critics have doubted to the possibility of a cyber-war. Until now, there is no evidence that a terrorist group or a nation has systematically attacked the opponent with computer hacking. Nonetheless, considering the relationship among dependency of computers in modern societies, international conflicts, and hackers' psychological mindsets, it is highly possible that cyber-war or cyberterrorism can happen.

This study, of course, had its limitations. The samples were not randomly selected. Samples depended on volunteers. The majority of the respondents were Korean hackers (48.6%) and hackers who speak English (29.2%). Only about 22% of the sample represented other countries.

Second, some caution should be exercised when interpreting the results. Particularly, in measurement to nationalism, religious pride, and ethnic coercion, the validity and reliability of the newspaper article produced for inducing a threat to the respondent was not systematically checked although some statistical significance was found in two pilot tests. The Index of hacking intention against nations was produced without checking the validity and reliability test in more systematic ways although pilot tests were carried out. The data used in this study was obtained by an online survey. This method has its own flaws because a researcher can’t control external variables.

Third, as in the case with all survey research, these data contain only partial evidence about cause and effect. The theoretic rationale for self-esteem, motivations, and terror management theory assumes that hackers with unstable high self-esteem, extrinsic motivations, high level of nationalism have more aggressiveness, but it is at least logically possible that causation might run the other way. Hackers who had more aggressiveness might be likely to have more narcissistic personality, reward oriented hacking intentions, or nationalistic ideologies.

Finally, future research concerning hackers and cyberterrorism should cover more hackers who represent each country with larger sample sizes. To explain the collective identities of hackers, more measurements or theoretic rationales should be developed and used. Particularly, this study mainly focused on the relationship between unstable high self-esteem (narcissism) and hackers’ aggressiveness, but the relationship between low self-esteem (e.g., frustration, feeling of inferiority, and unworthiness, etc.) and their aggression should also be checked to examine if the modified concept of self-esteem (i.e., people who have high self-esteem may have more aggressiveness than those who have low self-esteem) would be valid in explaining hackers’ aggressiveness.

To correctly examine hackers’ motivation, more sophisticated measurements should be needed. Although this research emphasized the dichotomy between intrinsic and extrinsic motivation, this dichotomy is insufficient to adequately depict hackers' hacking behaviors. Future study should use instruments to sensitively measure varying degrees of intrinsic and extrinsic motivation.

To explain why hackers keep getting involving in hacking in more detail, a challenge-skill balance factor in the flow state of a hacker should be investigated experimentally by establishing diverse situations: high skill-high challenge, high skill-low challenge, low skill-high challenge, and low skill-low challenge.

In terror management theory, this study did not measure mortal salience (fear of death, threats to the worldview, or insecurity of existence). If any, a produced newspaper article without systematic validity and reliability check was used to stimulate hackers' anxiety-provoking. Future research should develop a method to measure how mortal salience affects hackers' aggressive responses.

Because hacking in cyberspace is inevitably related to criminal activities, ethical issues and respect of laws would have to be considered. Although this study focused on hackers' psychological mindsets, the future research could add hacking technique issues such as their favorite hacking skills, how to break into a computer system, or how to write computer viruses to the next study.

REFERENCES

Adamski, A. (1999). Crimes related to the computer network. Threats and opportunities: A criminological perspective. Retrieved April 3, 2003, from www.infowar.com/new

Anderson, E. (1994, May). The code of the streets. *Atlantic Monthly, 273*, 81-94.

Arquilla, J., & Ronfeldt, D. (2001). *Networks and Netwars*. Santa Monica, Calif.: RAND.

Arquilla, J., & Ronfeldt, D. (Ed.). (1997). *IN ATHENA'CAMP*. Santa Monica, Calif.: RAND.

Arndt, J., Greenberg, J., Solomon, S., Pyszczynski, T., & Simon, L. (1997). Suppression, Accessibility of Death-Related Thoughts, and Cultural Worldview Defense: Exploring the Psychodynamics of Terror Management. *Journal of Personality and Social Psychology, Vol. 73*. No. 1, 5-18.

Baumeister, R. F. (1999). The Nature and Structure of the Self: An Overview. In R. F. Baumeister (Ed.), *The self in Social Psychology*. (pp.1-20). Philadelphia: Psychology Press.

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.

Baumeister, R. F., Smart, L., & Boden, J. M. (1996). Relation of threatened egotism to violence and aggression: The dark side of high self-esteem. *Psychological Review, 103,* 5-33.

Baumeister, R. F., & Tice, D. M. (1985). Self-esteem and responses to success and failure: Subsequent performance and intrinsic motivation. *Journal of Personality, 53*, 450-467.

Baumeister, R. F., Tice, D. M., & Huton, D. G. (1989). Self-presentational motivations and personality differences in self-esteem. *Journal of Personality, 57*, 547-579.

Becker, E. (1973). *The denial of death*. New York: Free Press.

Belcher, T., & Yoran, E. (2002). Riptech Internet Security Threat Report. Retrieved March 3, 2002 from http://www.riptech.com/newsevents/release020127.html

Blaine, B., & Crocker, J. (1993). Self-esteem and self-serving biases in reactions to positive and negative events: An integrative view. In R. Baumeister (Ed.), *Self-esteem: The puzzle of low self-regard* (pp. 219-241). New York: Plenum.

Branden, N. (1969). *The psychology of self-esteem*. New York: Bantam.

Brown, J. D. (1993). Motivation conflict and the self: The double-bind of low self-esteem. In R. Baumeister (Ed.), *The puzzle of low self-regard* (pp.117-130). New York: Plenum.

Bushman, B. J., & Baumeister, R. F. (1998). Threatened egotism, narcissism, self-esteem, and direct and displaced aggression: Does self-love or self-hate lead to violence? *Journal of Personality and Social Psychology*, *75*, 219-229.

Bushman, B. J., Baumeister, R. F., Phillips, C., & Gilligan, J. (1999). Narcissism and self-esteem among violent offenders in a prison population. Manuscript submitted for publication. (see Baumeister, R. F., Brad J. Bushman, & Caampbell, W. K., 2000).

California Task Force to Promote Self-esteem and Personal and Social Responsibility. (1990). Toward a state of self-esteem. Sacramento: California State Department of Education.

Campbell, J. D. (1990). Self-esteem and clarity of the self-concept. *Journal of Personality and Social Psychology, 59*, 473-505.

Campbell, J. D., & Lavallee, L. F. (1993). Who am I? The role of self-concept confusion in understanding the behavior of people with low self-esteem. In R. Baumeister (Ed.), *Self-esteem: The puzzle of low self-regard* (pp. 3-20). New York: Plenum.

Cha, A. E. (2001). Chinese Suspected of Hacking U.S. Sites. Retrieved April 23, 2001 from http://www.washingtonpost.com/wp-dyn/articles/A13431-2001Apr12.html.

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

Chantler, N. (1996). Profiles of a Computer hacker. Florida: Inforwar.

CNN.com (n.d.a). Q&A with Emmanuel Goldstein of 2600: The Hacker's Quarterly. Retrieved September 27, 2001 from http://www.cnn.com/TECH/specials/hackers/qandas/goldstein.html

CNN.com (n.d.). Japanese textbook dispute sparks cyber attack. Retrieved March 31, 2001 from http://asia.cnn.com/2001/WORLD/asiapcf/east/03/31/japan.korea.website/.

Colvin, C. R., Block, J., & Funder, D. C. (1995). Overly positive evaluations and personality: Negative implications for mental health. *Journal of Personality and Social Psychology*, *68,* 1152-1162.

Collin, B. (March 1997). The Future of Cyberterrorism. Crime and Justice International. 15-18.

Collin, B. C. (1998). CyberTerrorism From Virtual Darkness: New Weapons in a Timeless Battle. National Interagency Civil-Military Institute. Retrieved March 09, 2002, from http://www.nici.org/Research/Download_001.html

Computer Law Tip of the Week. (1999). Cyberterrorism. Retrieved March 08, 2002, from: http://www.mgrossmanlaw.com/articles/1999/cyberterrorism.htm

Coopersmith, S. (1967). *Self-esteem inventories*. Palo Alto, CA: Consulting Psychologists Press.

Critical Foundations: Protecting America's Infrastructures, The report of the President's Commission on Critical Infrastructure Protection, (1997 October). Retrieved February 14, 2001 from http://www/pccip.gov.

CSI, (2001). Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar. Retrieved March 31, 2002 from http://www.gocsi.com/prelea/000321.html

Csikszentmihalyi, M. (1990). *Flow: The Psychology of Optimal Experience*. New York: Harper & Row, Publishers.

Csikszentmihalyi, M., & Kubey, R. (1981). Television and the rest of life. *Public Opinion Quartely, 45*, 317-328.

Csikszentmihalyi, M., & LeFevre, J. (1989). Optimal experience in work and leisure. *Journal of Personality and Social Psychology, 56*, 815-822.

Csikszentmihalyi, M., & Rathunde, K. (1993). The measurement of Flow in Everyday Life: Toward a Theory of Emergent Motivation. In J. E. Jacobs, (Ed.), *Nebraska Symposium on Motivation* (1992): Vol. 40. Developmental perspectives on motivation. Current theory and research in motivation (pp. 57-97). Lincoln, NE: University of Nebraska Press.

Danitz, T., & Strobel, W. P. (2001). Networking Dissent: Cyber Activist use the Internet to Promote Democracy in Burma. In J. Arquilla, & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (pp.129-169). Santa Monica, Calif.: RAND.

Deci, E. L., & Ryan, R. M. (1991). Amotivational approach to self: Integration in personality. In R. Dienstbier (Ed.), *Nebraska symposium on motivation, Vol. 38*, Perspectives on motivation (pp. 237-288). Lincoln: University of Nebraska Press.

Deci, E. L., & Ryan, R. M. (1995). Human Autonomy: The basis for true self-esteem, in M. H. Kernis (Eds.), *Efficacy, Agency, and Self-Esteem* (pp. 31-29). New York: Plenum Press.

DEFCON. (n.d.). Upcoming Conventions 2001. Retrieved March 08, 2002, from http://www.defcon.org/other-conventions.html

Denning, D. E (1990). Concerning Hackers Who Break into Computer Systems. Retrieved June 30, 2001 from http://www.cpsr.org/cpsr/privacy/crime/denning.hackers.html

Denning, D. E. (2001) Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In J. Arquilla, & D. Ronfeldt, (Eds.), *Networks and Netwars*. Santa Monica, Calif.: RAND.

Denning, D. E. (1999). *Information warfare and Security.* Massachusetts: Addison-Wesley.

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, Vol. 76*, No. 4 Winter, 646-658.

Dunn, A. (1993), Crisis in Yugoslavia: Battle Spilling Over Onto the Internet, *Los Angeles Times*, April 3.

Gentile, C. J. (n.d.) Hacker war Rages In Holy Land. Retrieved January 30, 2001 from http://www.wired.com/news/politics/0,1283,40030,00.html.

Gondolf, E. W. (1985). *Men who batter*, Holmes Beach, FL: Learning Publications.

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

Greenberg, J., Pyszczynski, T., & Solomon, S. (1995). Toward a Dual-Motive Depth Psychology of Self and Social Behavior. In M. H. Kernis (Ed.), *Efficacy, Agency, and Self-Esteem*. (pp. 73-99). New York and London: Plenum Press.

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

Greenberg, J., Simon, L., Pyszczynski, T., Solomon, S., & Chatel, D. (1992). Terror management and tolerance: Does mortality salience always intensitfy negative reactins to others who threaten one's worldview? *Journal of Personality and Social Psychology, 63*, 212-220.

Greenberg, J., Solomon, S., & Pyszczynski, T. (1997). Terror management theory of self-esteem and cultural worldviews: Empirical assessments and conceptual refinements. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 29, pp. 61-139). San Diego, CA: Academic Press.

Graef, R., Csikszentmihalyi, M., & McManama Gianinno, S. (1983). Measuring intrinsic motivation in everyday life. *Leisure Studies*, *2*, 155-168.

Graef, R., McManama Gianinno, S., & Csikszentmihalyi, M. (1981). Energy conumption in leisure and perceived happiness. In J. D. Claxton et al. (Eds.), *Consumers and energy conservation* (pp. 47-55). New York: Praeger.

Hafner, K., & Markoff, J. (1995). *Cyberpunks: Outlaws and hackers on the computer frontier*. Toronto: Simon and Schuster.

Hollinger, R. (1988). Computer hackers follow a guttman-like progression. *Social Science Review, 72*, 199-200.

Hurwitz, J., & Peffley, M. (1999). International Attitudes. In Robinson J. P., Shaver, P. R., and Wrightsman, L. S. (Eds.), *Measures of Political Attitudes* (pp. 533-551). Vol. 2. San Diego: Academic Press.

IDefense. (n.d.). Israeli-Palestinian Cyber-Conflict (IPCC). Retrieved January 3, 2001 from http://www.idefense.com/

Itscurity (2001, April 26). Chinese Group Plans Cyberterrorism Attacks on U.S. Retrieved March 08, 2002, from: http://www.itsecurity.com/tecsnews/apr2001/apr524.htm

Itworld.com. (n.d.). What makes Johnny (and Jancy) write viruses? Retrieved March 16, 2001 from http://www.itworld.com/Net/3271/PCW01051534405/

Jackson, S. A., & Marsh, H. W. (1996). Development and Validation of a Scale to Measure Optimal Experience: The Flow State Scale. *Journal of Sport & Exercise Psychology*, *18*, 17-35.

Jankowski, M. S. (1991). *Islands in the street: Gangs and American urban society.* Berkeley: University of California Press.

Jenkins, S. (2002). Peaceful Games, Cold War Sentiment. (The Washington Post Online, p. D01). Retrieved February 25, 2001 from www.washingtonpost.com.

Jordan, T., & Taylor, P. (1998). A Sociology of Hackers. A presented paper at INet'98 Conference, Geneva, July 23. Retrieved April 3, 2003 from http://www.isoc.org/inet98/proceddings/2d/2d_1.htm.

Kabay, M. E. (2000). Studies and Surveys of Computer Crime. Retrieved December 12, 2000 from http://www.secuirtyportal.com/cover/coverstory20001211.html.

Kernis, M. (1993). The roles of stability and level of self-esteem in psychological functioning. In R. Baumeister, (Ed.), *Self-esteem: The puzzle of low self-regard* (pp.167-182). New York: Plenum.

Kernis, M. H. (Ed.). (1995). *Efficacy, Agency, and Self-esteem.* New York and London: Plenum Press.

Kernis, M. H., Granneman, B. D., & Barclay, L. C. (1989). Stability and level of self-esteem as predictors of anger arousal and hostility. *Journal of Personality and Social Psychology, 56*,1013-1022.

Kernis, M. H., Paradise, A. W., Whitaker, D. J., Wheatman, S. R., & Goldman, B. N. (2000). Master of One's Psychological Domain? Not Likely if One's Self-Esteem is Unstable. *Personality and Social Psychology Bulletin*, Vol 26, No. 10, October, 1297-1305.

Kubey, R., & Csikszentmihalyi, M. (1990). *Television and the quality of life*. Hillsdale, NJ: Lawrence Erlbaum.

Landreth, B. (1985). *Out of the inner circle*. Redmond: Microsoft Books.

Levy, S. (1984). *Hackers*. New York: Dell.

Libicki, M. C. (1995). What is Information Warfare? National Defense University.

Littman, J. (1997). *The Watchman: The twisted life and crimes of serial hacker Kevin Poulsen*. Toronto: Little Brown & Company.

Long, D. E. (1990). *The anatomy of terrorism*. New York: Free Press.

Luening, E. (n.d.). Mideast Hackers may strike U.S. sites, FBI warns. Retrieved January 1, 2001 from http://news.cnet.com/news/0-1007-200-3359667.html?tag=bplst.

McFarlin, D. B., & Blascovich, J. (1981). Effects of self-esteem and performance feedback on future affective preferences and cognitive expectations. *Journal of Personality and Social Psychology, 40*, 521-531.

McGregor, H. A., Lieberman, J. D., Greenberg, J., Solomon, S., Arndt, J., Simon, L., & Pyszczynski, T. (1998). Terror Management and Aggression: Evidence That Mortality Salience Motivates Aggression Against Worldview-Threatening Others. *Journal of Personality and Social Psychology, Vol. 74*, No. 3, 590-605.

Mruk, C. (1995). *Self-Esteem: Research, Theory, and Practice*. New York: Springer Publishing Company, Inc.

Nelson, L. J., Moore, D. L., Olivetti, J., & Scott, T. (1997). General and Personal Mortality Salience and Nationalistic Bias. *Personality and Social Psychology*. *Vol. 23*, No. 8, August, 884-892.

News Services (n.d.). FBI Investigates Threat. The Washington Post Online. p. D12. Retrieved February 21, 2002 from www.washingtonpost.com.

Norusis, M. J. (n.d.). *SPSS 6.1 Guide to Data Analysis*. New Jersey: Englewood Cliffs.

Oates, R. K., & Forrest, D. (1985). Self-esteem and early background of abusive mothers. *Child abuse and Neglect, 9*, 89-93.

O'Brien, E., & Epstein, S. (1983). MSEI: The multidimensional self-esteem inventory. Odessa. FL: Psychological Assessment Resources.

Park, H. S., Dailey, R., & Lemus, D. (2002). The Use of Exploratory Factor Analysis and Principal components Analysis in Communication Research. *Human Communication Research, Vol. 28*, No. 4, October 562-577.

Parker, D. (1998). *Fighting computer crime: A new framework for protecting information*. New York: John Wiley & Sons. Inc.

Paul, L. (n.d.). When Cyber Hacktivism Meets Cyberterrorism. Retrieved February 19, 2001 from http://www.sans.org/infosecFAQ/hackers/terrorism.htm.

Plummer, D. L. (1985). Help seeking as a function of perceived inadequacy level and self-esteem. Unpublished doctoral dissertation, University of Georgia, Athens.

Pollitt, M. M. (2000, Jan 10). CYBERTERRORISM-Fact or Fancy? Retrieved March 02, 2002, from http://www.cs.georgetown.edu/~denning/infosec/pollitt.html

Post, J. (1996). The dangerous information system insider: Psychological perspectives. Retrieved April 3, 2003 from http://www.inforwar.com

Post, J., Shaw, E., Ruby, K. (1998). Information terrorism and the dangerous insider. Paper presented at the meeting of InfowarCon'98, Washington, DC.

Power, R. (1998). Current and future danger. Computer Security Institute.

Power. R. (2000). Tangled web: Tales of digital Crime from the Shadows of Cyberspace. Que Corporation.

Raymond, E. S. (2001). How To Become A Hacker. Retrieved April 02, 2002 from http://www.tuxedo.org/~esr/faqs/hacker-howto.html

Renzetti, C. M. (1992). *Violent betrayal: Partner abuse in lesbian relationships*. Newbury Park, CA: Sage.

Rhodewalt, F., Madrian, J. C., & Cheney, S. (1998). Narcissism, self-knowledge, organization, and emotional reactivity: The effects of daily experiences on self-esteem and affect. *Personality and Social Psychology Bulletin, 24*, 75-86.

Riptech (2002). Riptech releases groundbreaking internet security threat report. Retrieved March 3, 2002 from http://www.riptech.com/newsevents/release020127.html.

Rist, O. (1998). Get To Know The Hakcer's Mind-Set. TechWeb. Retrieved April 3, 2003 from http://content.techweb.com/se/directlink.cgi?lNW19980921S0055.

Rogers, L. (2000c). Cybersleuthing: Means, Motive, and Opportunity. InfoSec Outlook, June. Retrieved March 8, 2002 from http://interactive.sei.cmu.edu/news@sei/columns/security_matters/2000…/security-sum-00.ht.

Rogers, M. (2000b). A New Hacker Taxonomy. Retrieved March 31, 2002 from http://www.escape.ca/mkr/.

Rogers, M. (2000d). A New Hacker Taxonomy (Revised version). Retrieved March 31, 2002 from http://www.escape.ca/mkr/.

Rogers, M. (2000). Psychological Theories of Crime and Hacking. Retrieved March 31, 2002 from http://www.escape.ca/mkr/.

Rogers, M. K. (2001). A social Learning Theory and Moral Disengagement Analysis of Criminal Computer Behavior: An Exploratory Study. Doctoral Disseration, Department of Psychology, University of Manitoba.

Rogers, R. (2000a). Internet & Society in Armenia and Azerbaijan? Web games and a Chronicle of an inforwar. First Monday, Volume 5, Number 9, September. Retrieved March 10, 2002 from http://firstmonday.org/issues/issue5_9/rogers/index.html.

Rose, P. (2001). A brief Narcissistic Personality Inventory. Unpublished raw data, State University of New York at Buffalo.

Rosenblatt, A., Greenberg, J., Solomon, S., Pyszczynski, T., & Lyon, D. (1989). Evidence for terror management theory. I. The effects of mortality salience on reactions to those who violate or uphold cultural values. *Journal of Personality and Social Psychology*, *57*, 681-690.

Ryan, R. M. (1993). Agency and organization: Intrinsic motivation, autonomy and the self in psychological development. In J. Jacobs (Ed.), *Nebraska symposium on motivation: Developmental perspectives on motivation, Vol. 40* (pp. 1-56). Lincoln: University of Nebraska Press.

Ryan, R. M. (1982). Control and information in the intrapersonal sphere: An extension of cognitive evaluation theory. *Journal of Personality and Social Psychology*, *43,* 450-461.

Ryan, R. M., & Frederick, C. M. (1994). A theory and measure of vitality. Unpublished manuscript. Rochester, NY: University of Rochester.

Schoenfeld, C. G. (1988). Blacks and violent crime: A psychoanalytically oriented analysis. *Journal of Psychiatry and Law, 16*, 269-3-1.

Shaw, G (2001). "Information Security News (ISN) mailing list archive: Hackers crack A&B site. InfoSec News. Retrieved May 21 2001 from http://lists.insecure.org/isn/2001/May/0028.html

Shimeall, T., Williams, P., & Dunlevy, C. (2001). Countering cyber war. *NATO review*. Winter 2001/2002. pp16-18.

Shrauger, J. S., & Rosenberg, S. E. (1970). Self-esteem and the effects of success and failure, and improvement as determinants of persistence. *Journal of Consulting and Clinical Psychology, 45*, 784-795.

Solomon, S., Greenberg, J., & Pyszczynski, T. (1991). A terror management theory of social behavior: The psychological functions of self-esteem and cultural worldviews. In M. P. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 24, pp. 91-159). San Diego, CA: Academic Press.

Spielberger, C. D., Jacobs, G., Russell, S. & Crane, R. S. (1983). Assessment of Anger: The State-Trait Anger Scale. In Butcher, J. N., and Spielberger, C. D. (Eds.), *Advances in Personality Assessmen, Vol 2,* (pp. 161-189).

Staub, E. (1989). *The roots of evil: The origins of genocide and other group violence*. New York and Cambridge, England: Cambridge University Press.

Sullvan, J. P. (2001). Gangs, Hooligans, and Anarchists-The Vanguard of Netwar in the street. In J. Arquilla, & D. Ronfeldt (Eds.), *Networks and Netwars: The future of Terror, Crime, and Militancy* (pp. 99-126). Santa Monica, Calif.: RAND.

Taggart, A (2001). The Digital Revolt: Resistance & Agency on the Net. Retrieved March 31, 2002 from http://georgetown.edu/papers/wtaggert.htm

Taylor, P. A. (1999). Hackers: Crime in the digital sublime. London: Routledge. The Center for the study of Technology and Society. (2001, March 16). Special Focus: Cyberwarfare. Retrievd March 08, 2001 from http://www.tecsoc.org/natsec/focuscyberwar.htm.

The Center for the study of Technology and Society (n.d.). Special Focus Cyberwarfare. Retrieved May 29, 2001 from http://www.tecsoc.org/natsec/focuscyberwar.htm.

The Japan Times (Oct 24, 2000). SDF prepareds to combat cyberterrorism. Retrived March 10, 2002 from http://www.japantimes.co.jp/cgi/bin/getarticle.pl5?nn20001024b5.htm

Thomas, D. & Loader, B. D. (2000). *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

UPI (October 29, 2002). China prevented repeat cyber attack on US. Retrieved October 29, 2002 from http://www.upi.com/view.cfm?StoryID=20021029-121924-5101r.

U.S. Defense.com. (May 10, 2000). China Accelerating Information Warfare Capabilities.
Retrieved March 10, 2000 from http://www.tecsoc.org/natsec/focuscyberwar.htm

Voiskounsky, A. E., Babaeva, J. D., & Smyslova, O. V. (2000). Attitudes towards computer hacking in Russia. In D. Thomas & D. L. Brian (Eds.), *Cybercrime: Law enforcement, security, and surveillance in the information age* (pp.56-84). London: Routledge.

Waltz, E. (1998). *Information Warfare: principles and operations*. Boston: ARTECH HOUSE, Inc.

Wells, E. L., & Marwell, G. (1976). *Self-esteem: Its conceptualization and measurement*. Beverly Hills, CA: Sage.

Woo, H. J., Kim, Y. R., & Dominick, J. R. (2002). Hackers: Chauvinists or Anarchists-A content Analysis of Defaced Web Pages. presented at Communication and Technology division, International Communication Association, Seoul, Korea, July.

Woo, H. J (2003). Propaganda War in Cyberspace: A content analysis of politically motivated hackers. Presented at Mass Communication division, International Communication Association, San Diego, USA, May.

APPENDICES

APPENDIX A: DEMOGRAPHIC RESULTS OF HACKERS

Table 1. Demographic data

	Frequency (%)
Gender	
Male	642 (88.1)
Female	31 (4.3)
Undetermined	56 (7.7)
Age	
Less than 19 years old	368 (50.5)
20-25 years old	240 (32.9)
26-30 years old	83 (11.4)
31-35 years old	25 (3.4)
36-40 years old	5 (0.7)
41-45 years old	3 (0.4)
45-50 years old	2 (0.3)
More than 51 years old	3 (0.4)
Religion	
Buddhism	141 (19.3)
Catholic	60 (8.2)
Christianity	180 (24.7)
Hinduism	3 (0.4)
Judaism	6 (0.8)
Moslem	15 (2.1)
Other	37 (5.1)
No religion	287 (39.4)
Race	
Arabian	71 (9.7)
Asian	440 (60.4)
Black	5 (0.7)
Caucasian	137 (18.8)
Hispanic	12 (1.6)
Jewish	3 (0.4)
Native American	5 (0.7)
Other	56 (7.7)
Education	
Elementary school	111 (15.2)
Middle school	86 (11.8)
High school	184 (25.2)
College-2 year	101 (13.9)
College-4 year	194 (26.6)
Master’s degree	34 (4.7)
Doctoral degree	19 (2.6)

Table 2. Hackers’ mother language

Language	Frequency	Percentage (%)
Afghan	61	8.4
Arabic	3	0.4
Bohemian/Czech	3	0.4
Chinese	2	0.3
Danish	1	0.1
Dutch	6	0.8
English	213	29.2
Finnish	3	0.4
French	8	1.1
German	7	1.0
Greek	0	0.0
Hebrew	1	0.1
Hindi	1	0.1
Hungarian	0	0.0
Indonesian	1	0.1
Iranian	1	0.1
Iraqi	0	0.0
Irish	0	0.0
Italian	1	0.1
Japanese	10	1.4
Korean	354	48.6
Kurdish	2	0.3
Latin	0	0.0
Lebanese	3	0.4
Malay	2	0.3
Norwegian	2	0.3
Polish	1	0.1
Portuguese	2	0.3
Russian	3	0.4
Spanish/Espana	11	1.5
Swahili	1	0.1
Swedish	5	0.7
Thai	0	0.0
Turkish	3	0.4
Vietnamese	2	0.3
Other	15	2.1
Missing	1	0.1
Total	729	100

Table 3. The most likely target of hackers

Hacking targets	Percentage (%)
1. Personal homepages	70.1
2. University web sites	56.5
3. Small business sites	47.2
4. Big business sites	42.2
5. Other government sites	38.0
6. Porn sites	35.9
7. Other ethnic sites	31.8
8. Military sites	27.8
9. Transnational corporation sites	27.7
10. Secret agency sites	26.5
11. Other religion sites	22.6
12. Bank computer systems	21.9

APPENDIX B: RESPONSES FROM PARTICIPANTS

Hyung-Jin Woo, a Ph.D. candidate at the University of Georgia, has asked us to tell you about an online survey he's put up to collect information for his thesis (titled "Hackers and Cyberterrorism: Self-esteem, Motivations, and Aggressiveness").

Personally I have a few problems with his study, namely that:
a) where he says "hacking" he actually means defacing websites
b) where he says "cyberterrorism" he actually means defacing websites
c) the study is hosted in the United States where any and all evidence gathered by it could be used to send you to prison for a very, very long time

So, if you're a website-defacing L337 h4X0R or cyber-terrorist head on over and check out the "Online Survey for World Computer Hackers". Your choice (but please don't hack his website on him ;-)

****

Re: Wanna Be Famous? (Score: 0)
by Anonymous on Sunday, September 29 @ 19:48:53 EDT
I read the questions in his questionaire, which were mostly humerous. Someone should educate people like him that hacking is not just about defacing the public face of various organisations (their web sites) but getting behind the public face to the muck behind it.

****

Hi. There must be a little misunderstanding: we have no hacker member, we are just reporting hackers crimes - call us white hats-.
There is a major mistake in your hacker overview: you have only english and 3 different east languages. If you are really interested in an online survey about computer hackers (or you meant defacers?) then you definetly have to post a page in Portuguese, Russian and Arabian so you would cover 90% of the possible ethnic groups.
By the way, we are desperately looking for chinese,korean and japanese members (whitehats). Does any of your staff, mates, affiliates want to join zone-h? We would like to create special sections in zone-h covering those languages . Why?
Easy to explain: in September we got
38.519 clicks from Japan
10.161 clicks from Hong Kong
7.180 clicks from Singapore
605 clicks from South Korea
and we have no far east language contents.
Thanks for the cooperation.
SYS64738 www.zone-h.org admin

APPENDIX C: ONLINE QUESTIONNAIRE

Online Survey for World Computer Hackers
Conducted by Hyung-Jin Woo
The University of Georgia

Welcome!

The purpose of this study is to compare world hackers' life and their hacking activities under the title of the research "The Hacking Mentality: Exploring the Relationships between Psychological Variables and Hacking Activities." This research is to examine 1) computer hackers' experience in cyberspace and 2) their psychological mindsets. The results of the study will be published for Hyung-Jin Woo's doctoral dissertation. If you are a computer hacker or a wanabe hacker, please participate in this online survey. This survey would take 10-15 minutes to complete.

Thank you in advance for your participation. If you have any questions, please feel free to contact Hyung-Jin Woo, primary researcher, 1-706-354-4181; E-mail: hyungjinw@hotmail.com; Department of Telecommunication, University of Georgia, Athens, GA 30606, USA. You can also contact Dr. Joseph R. Dominick, advisor of this research 1-706-542-4974; E-mail: joedom@arches.uga.edu; Department of Telecommunication, University of Georgia, Athens, GA 30606, USA.

Consent form for Participation in Research

Since hacking is an illegal activity, you will see some self-incriminating questions in this online questionnaire. If you feel uncomfortable, you don't have to answer the questions and remain blank. Because of online survey's technological shortcomings in regards to protecting the participant's identity, information could potentially be traced back to you directly. Any information submitted by you can be subpoenaed by law enforcement agencies. However, the researcher will take precautions to protect your confidentiality as much as possible. Any information that is obtained in connection with this study and that can be identified with you will remain confidential and will be disclosed only with your permission or as required by law. To protect participants' identity, the researcher has taken precautionary measures that will block most third party access to your answers; any link to identify participants (i.e., IP address) will be destroyed as soon as we receive information; a database file will be secured by firewalls; the data will be destroyed on Nov 01, 2002.

In order to participate, participant must 18+ years old.

Your participation is completely voluntary. You may withdraw from the study at any time without the risk of any penalty. You understand the reason for the study is to examine the relations between hackers' psychological mindsets and their hacking activities. Your participation will remain confidential. No discomforts or stresses are expected. There is a limit to the confidentiality that can be guaranteed due to the technology itself.

I agree to take part in a research study titled " The Hacking Mentality: Exploring the Relationships between Psychological Variables and Hacking Activities," which is being conducted by Hyung-Jin Woo, department of telecommunication, University of Georgia, USA, 1-706-354-4181 under the direction of Prof. Joseph R. Dominick, department of telecommunication, University of Georgia, USA, 1-706-542-4974. I do not have to take part in this study; I can stop taking part at any time without giving any reason, and without penalty. I can ask to have information related to me returned to me, removed from the research records, or destroyed.

By clicking on "I Agree" button below, you are giving your consent for the researcher to include your data. If you are a Computer Hacker, Please click below to go to a questionnaire about your hacking experience.

I AGREE

Research at the University of Georgia which involves human participants is overseen by the Institutional Review Board. Questions or problems regarding your rights as a participant should be addressed to Chris Joseph; Institutional Review Board; Office of V.P. for Research; The University of Georgia; 606A Graduate Studies Research Center; Athens, Georgia 30602-7411; Telephone (706) 542-6514.

INSTRUCTIONS: The following are related to your hacking activities in the last month.

(The following are kinds of self-incriminating questions. If you feel uncomfortable, you don't have to answer the questions and remain blank.)

1. In the last month, have you altered or otherwise changed any web sites belonging to others? (if you choose no, go to Q#4)

___Yes

___No

2. In the last month, how often did you break into somebody else's computer systems?

___Never
___1-2
___3-5
___6-10
___11-20
___21-30
___ more than 31

3. In the last month, how often did you alter or change others' web sites?

___Never
___1-2
___3-5
___6-10
___11-20
___21-30
___ more than 31

4. The following are statements about hacking. How much do they apply to you?

	Never	A few	Sometimes	Frequently	Very Frequently
1) I have hacked bank-computer systems.					
2) I have hacked in order to let other hackers know what I did.					
3) I have hacked web sites for fun.					
4) I have hacked web sites for no particular reason.					
5) I have hacked web sites in order to check the security of the sites.					
6) I have hacked web sites for my boy/girl friends.					
7) I have hacked of web sites of other nations' governments and businesses.					
8) I have hacked web sites of other religions.					
9) I have hacked web sites of other ethnicities.					
10) I have hacked web sites in order to stop the spread of pornography.					
11) I have hacked web sites because "information should be free in cyberspace."					
12) I have hacked web sites in order to earn money.					
13) I have hacked web sites out of curiosity.					
14) I have hacked web sites on account of boredom.					
15) I have hacked web sites to release secret codes from transnational companies such as Microsoft, Sony, or Coca Cola.					
16) I have hacked a country's intelligent agency sites.					
17) I have hacked military web sites.					
18) I have hacked university's web sites.					
19) I have hacked personal homepages.					
20) I have hacked big business companies' web sites.					
21) I have designed a computer virus.					
22) I have hacked small companies' web sites.					

Please rate the importance of each of the following reasons in relation to hacking. Use the following scale.

	Is not at all a reason						Is an extremely important reason
5. The reason why I hack....	0	1	2	3	4	5	6
1) I do hacking to avoid feeling guilty or anxious.							
2) I do hacking because I feel that hacking will help me grow or develop in a way that is personally important to me.							
3) I do hacking because something about my external situation forces me to do it.							
4) I do hacking because of the pleasure and fun of doing it.							
5) I do hacking because it ties into my personal values and beliefs.							
6) I do hacking because I am supposed to do it.							
7) I do hacking because of the interest and enjoyment of doing it.							
8) I do hacking because somebody else wants me to or because I will get something from somebody if I do.							

Below are a number of pairs of statements. Read each pair of statements and then indicate which statement comes closest to describing your feelings and beliefs about yourself.

6-1
___I really like to be the center of attention.

___It makes me uncomfortable to be the center of attention.

6-2
___I like having authority over people.

___I don't mind following orders.

6-3
___I prefer to blend in with the crowd.

___I like to be the center of attention.

6-4
___Being an authority doesn't mean that much to me.

___People always seem to recognize my authority.

6-5
___I am no better or no worse than most people.

___I think I am a special person.

6-6
___I am going to be a great person.

___I hope I am going to be successful.

6-7
___I am much like everybody else.

___I am an extraordinary person.

6-8
___When people compliment me, I sometimes get embarrassed.

___I know that I am good because everybody keeps telling me so.

6-9
___Sometimes I tell good stories.

___Everybody likes to hear my stories.

6-10
___People sometimes believe what I tell them.

___I can make everybody believe anything I want them to.

6-11
___I always know what I am doing.

___Sometimes I am not sure of what I am doing.

6-12
___I try not to be a show off.

___I am apt to show off if I get the chance.

6-13
___I insist upon getting the respect that is due me.

___I usually get the respect that I deserve.

6-14
___I expect a great deal from other people.

___I like to do things for other people.

6-15
___I find it easy to manipulate people.

___I don't like it when I find myself manipulating people.

6-16
___I am more capable than other people.

___There is a lot that I can learn from other people.

After you read the following news article, please check regarding your feelings about your nation, religion, and ethnic group.

"Recently, powerful countries act like an arrogant bully. They wield their power and threaten other countries. Sooner or later, a strong country which has taken all power from the rest of the world will be born. This powerful one will possess all benefits. The majority ethnic group of this country espouses that they should annihilate the small and uncultured ethnics as Nazis did in the 1940s. They plan to convert all different existing religions in order to construct a new world order (Sep 11, 2001: The Washington Post)."				
	Strongly disagree	Disagree	Agree	Strongly agree
7. I would never settle in another country.				
8. My country's flag is the best in the world.				
9. I think my country is the finest in the world.				
10. My country is the best country in the world.				
11. I would never change my religion.				
12. My religion is the best in the world.				
13. I think my congregation is the finest in the world.				
14. My religion is superior to other religions.				
15. I would never go along with the people of other nations.				
16. People in my country are the best in the world.				
17. I think my people are the finest in the world				
18. My people are superior to other ethic groups in the world				

Please rate the following statement regarding your temperament.

	Almost never	Sometimes	Often	Almost always
19. I have a fiery temperament				
20. I am quick-tempered				
21. I am a hot-headed person				
22. I fly off the handle				
23. I am infuriated when I get a poor evaluation				
24. I am furious when criticized				
25. I am annoyed when not given recognition				
26. I am angry when slowed down by others				
27. When I get mad, I say nasty things				
28. When frustrated, feel like hitting				

Please rate the following statements regarding your nation.

	Extremel y	Very	Somewhat	Not very
29. How angry does it make you feel when you hear someone criticizing your country?				
30. How proud are you to be a citizen of your country?				
31. How angry does it make you feel when people burn your nation's flag in protest?				
32. How strong is your love for your country?				
33. How proud do you feel when you hear your national anthem?				

Please rate the following statement regarding your intention.

(The following are kinds of self-incriminating questions. If you feel uncomfortable, you don't have to answer the questions and remain blank.)

	Strongly agree	Agree	Disagree	Strongly disagree
34. If another country criticizes my country, I would hack that country's web sites with my hacking skills.				
35. If another country threatens my country, I would hack that country's web sites with my hacking skills.				
36. If another country tries to invade my country, I would hack that country's web sites with my hacking skills.				
37. If I hear that another country's hackers have broken into my government's web sites, I would hack that country's government web sites in return.				
38. If I found an enemy country's web sites in the INTERNET, I would hack the country's web sites with my hacking skills.				

<table>
<tr><td colspan="6">INSTRUCTIONS: Please answer the following questions in relation to your hacking experience. These questions relate to the thoughts and feelings you may have experienced while hacking. There are no right or wrong answers. Think about how you felt during hacking and answer the questions using the rating scale below. Click button that best matches your experience.</td></tr>
<tr><td></td><td>Strongly disagree</td><td>Disagree</td><td>Neutral</td><td>Agree</td><td>Strongly agree</td></tr>
<tr><td>39. I was challenged, but I believed my hacking skills would allow me to meet the challenge.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>40. My hacking abilities matched the high challenge of the situation.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>41. I felt I was competent enough to meet the high demands of the situation.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>42. The challenge and my hacking skills were at an equally high level.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>43. My attention was focused entirely on what I was hacking.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>44. It was no effort to keep my mind on what was happening.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>45. I had total concentration.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>46. I was completely focused on the task at hand.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>47. I was not concerned with what others may have been thinking of me.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>48. I was not worried about my performance during hacking.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>49. I was not concerned with how I was presenting myself.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>50. I was not worried about what others may have been thinking of me.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>51. I was aware of how well I was hacking.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>52. The way time passed seemed to be different from normal.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>53. It felt like time stopped while I was hacking.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>54. At times, it almost seemed like things were happening in slow motion.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>55. I really enjoyed hacking experience.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>56. I loved the feeling of hacking performance and want to capture it again.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>57. The hacking experience left me feeling great.</td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>58. I found the hacking experience extremely rewarding.</td><td></td><td></td><td></td><td></td><td></td></tr>
</table>

INSTRUCTIONS: The following are related to your hacking contest experience. Please answer to your best ability.

59. Have you ever participated in the Hackerslab's free hacking zone? (if you choose no, go to Q#61)

___Yes

___No

60. What was your final level in the Hackerslab's free hacking zone?
___Level 0 ___Level 1 ___Level 2 ___Level 3 ___Level 4 ___Level 5 ___Level 6
___Level 7 ___Level 8 ___Level 9 ___Level10 ___Level 11 ___Level 12 ___Level 13
___Level 14 ___Level 15 ___Level 16 ___Level 17

61. Have you ever participated in other computer hacking contests? (if you choose no, go to Q#63)

___Yes

___No

62. What was your final level? (Choose one contest that you recently participated in).

___Top-10%
___11-30%
___31-50%
___51-70%
___71-100%

Here are some demographic questions.

63. Your gender
___Male

___Female

64. Your age?
___Less than 19 years old
___20 to 25 years old
___26 to 30 years old
___31 to 35 years old
___36 to 40 years old
___41 to 45 years old
___46 to 50 years old
___more than 51 years old

65 Religion
___Buddhism
___Catholic
___Christianity
___Hinduism
___Judaism
___Moslem
___Others
___No-religion

66. Race
___Arabian
___Asian
___Black
___Caucasian
___Hispanic
___Jewish
___Native American
___Others

67. Your final education
___Elementary school
___Middle school
___High school
___College - 2 year
___College – 4 year
___Graduate school – masters' degree
___Graduate school – Ph.d.

68. What language do you speak most often?
___Afghan ___Arabic ___Bohemian/Czech ___Chinese ___Danish ___Dutch ___English
___Finnish ___French ___German ___Greek ___Hebrew ___Hindi ___Hungarian
___Indonesian ___Iranian ___Iraqi ___Irish ___Italian ___Japanese ___Korean ___Kurdish
___Latin ___Lebanese ___Malay ___Norwegian ___Polish ___Portuguese ___Russian
___Spanish/Espana ___Swahili ___Swedish ___Thai ___Turkish ___Vietnamese ___others