

The Dark Visitor

Inside the World of Chinese Hackers

Scott J. Henderson

The Dark Visitor

By Scott J. Henderson

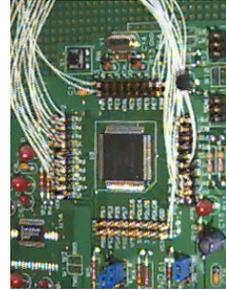
October 2007

The Dark Visitor: Copyright © 2007 by Scott Henderson. All rights reserved. No part of this book may be used or reproduced in any manner whatsoever without written permission except in the case of brief quotations embodied in critical articles or reviews.

First Edition

Library of Congress Cataloging-in-Publication has been applied for.

About the Cover



The cover design, by Mr. Charles A. Martinson III, is a composite consisting of three major elements: the rendering of an ancient Chinese copper helmet; the opera mask of Jiang Wei; and computer circuitry. The combination is a blending of ancient and modern that attempts to capture the character and nature of the Red Hacker Alliance. It depicts the competing elements that superimpose themselves over the lives of these young nationalists and how it shapes their future.

The helmet represents the spirit of the warrior and the hackers' belief that they are the acting in defense of their nation. It is also meant to convey the idea of cultural traits passing from one generation to the next, the old transforming and reawakening anew.

The opera mask of Jiang Wei was used for similarities in character. Jiang Wei was a commander of the Shu Army and considered one of the greatest men of the Three Kingdoms era. His mentor, Zhuge, was so fond of him that he bequeathed him all of his books on strategy.¹ Jiang Wei was thought to have special knowledge of the universe that melds with the Red Hacker Alliance's understanding of the cyber world. The color blue was added to the mask to bring in the attributes of fierceness; the color red already

¹ <http://www.paulnoll.com/China/Opera/China-opera-set-10.html>

present in the mask for loyalty, symbolizing nationalism; and white, the element of deceit that exists in the darker intent of their intrusions.²

The infusion of circuitry and binary numbers shows the extent of their immersion in a world in which many of us are unfamiliar. This extreme devotion to an alternate realm brings easily to mind the stuff of movies, the combination of man and machine -- the cyborg.

² The attributes assigned to the colors are based off those given by the Beijing Opera and thus may seem out of sync with traditional Western ideas.
<http://www.paulnoll.com/China/Opera/China-opera-colors.html>

Contents

Acknowledgements.....	1
Preface.....	2
Chinese Hacker Timeline.....	6
Chapter One: History.....	8
Beginning and Expansion (1994-1996).....	11
<i>Green Army Founded</i> (1997).....	12
<i>China Eagle</i> Early Years (1997).....	14
Leaps, Horses, and Riots (1998).....	15
Indonesian Riots (1998).....	16
Birth of Commercialism (1999).....	20
Taiwan “Two-States” Conflict (1999).....	20
Japanese Denial of Nanjing Massacre (2000).....	22
Taiwan Election (2000).....	25
<i>China Eagle</i> Founded (2000).....	32
<i>Honker Union</i> Founded (2000).....	35
<i>Javaphile</i> Founded (2000).....	36
Japanese Incidents (2001).....	38
Japanese War Memorial (2001).....	40
Diaoyu Islands Conflict (2004).....	41
<i>Honker Union</i> Disbands (2004).....	42
Chapter Two: Chinese Hacker Present Day.....	51
Methodology.....	52
Net Hierarchy.....	57
Numbers Game.....	58
Demographics.....	62
Location, Location, Location.....	62
Who They Are, What They Are.....	66
<i>Friendly Download Site</i>	66
<i>New Hacker Alliance</i>	69
<i>Student Hacker Union</i>	72

<i>Yaqu163</i>	74
<i>Hx99</i>	76
Chapter Three: Exploits and Money	79
Wooden Horse.....	79
Korean Game Theft.....	82
eBay Hijacked.....	86
Bank Fraud.....	87
Blackmail.....	88
Musical Hacks.....	90
Hacking for Fame and Fortune.....	92
Publish or Perish.....	93
It Pays to Advertise.....	94
Pornography.....	97
Chapter Four: Government Affiliation.....	102
Black and White Do Not Exist.....	102
Intelligence and Economics.....	105
Political.....	108
Recruiting.....	112
Communications.....	118
Appendix I. Hacker Terminology.....	122
Appendix II. List of All Hacker Web sites in Study.....	131
Index.....	137

Acknowledgements

Thanks to the extreme patience and support of Dr. Jacob Kipp and Mr. Karl Prinslow, I have been able to spend the last year living inside of and studying the world of Chinese hackers. It has been the opportunity of a lifetime and one that would have been impossible without their belief in the project.

My heartfelt appreciation goes out to Mrs. Susan Craig, Dr. Geoff Demarest, and Mr. Tim Thomas for taking the time to edit this manuscript. For those attempting their first book, the best recommendation I can make is to find the brightest group of people you can to review, critic, and evaluate the work.

To Mr. Hommy Rosado and Mr. Kevin Freese, bless you for giving so freely of your technical knowledge and not throwing me off a cliff for constantly asking, “Could you please explain that to me just one more time?” Without their guidance in this area, the embarrassments would have been too numerous to mention.

Mr. Merle Miyasato, simple words alone are insufficient in expressing my gratitude for all you have done to contribute to this work. Your tireless efforts in assisting with the research are greatly appreciated but I thank you most of all for your friendship.

For my father and mother, J.B. and Irene Henderson, you two have always been my bedrock and strength. The examples you have set and the guidance you have given me all my life have been invaluable. I just pray that I am able to set those same fine examples for my family.

Finally, to my wife Li-Yun and daughter Jade, being able to experience all that life has to offer with the two of you is the greatest joy of my life. The accomplishments would mean nothing if I did not have such a beautiful wife and darling daughter to share them with. Jade, this book is dedicated to you, there is never a day that goes by that I don't thank God for letting me view the world renewed through your eyes.

Preface

This book attempts to analyze the history, ideology, organization, exploits, and political motivations of the Chinese hacker network. Whenever possible, the information contained herein has been taken directly from the Chinese hacker organization itself or from interviews with individual members.

During the course of this research several interesting questions have arisen, one being, does the idea of national sovereignty include cyber sovereignty? While there are many definitions of sovereignty, most include the description, in one form or another, of the absolute power, right, or authority of the state to govern the territory within its borders.³ In essence, the state owns or controls what happens inside the nation. The key word that appears to be missing in all of these definitions is the *ability* to exercise authority. If one accepts the premise that it is the right, combined with the ability of a nation to control its internal workings that define sovereignty, then is there a loss of sovereignty when the state fails in either of these two capacities? Specifically, can there be cyber sovereignty if we cannot secure our digital borders?

With the onslaught of hackers from other nations breaching the firewalls with impunity, how can we retain uncontested ownership? One method is to rely on the cooperation of other nations to mutually assist in the enforcement of laws related to Internet crime. What if, on the other hand, the nation in question provides tacit, if not active support of these attacks? What recourse is then available to combat these assaults? The Chinese hacker network presents just such a dilemma and can easily be viewed as a threat to US infrastructure, security, information, economics, and individual citizens.

One of the unique aspects of the Chinese hacker organization is their nationalism, which is in stark contrast to the loner/anarchist culture many associate with the stereotypical Western hacker. They are especially active during periods of political conflict with other nations and until very recently have maintained a strict code of never hacking inside China. Their sense of patriotism in defending their national honor and their stringent codes have

³ Multiple definitions supplied by Answer.com, as downloaded on 8 August 2005, <http://www.answers.com/sovereignty&r=67>

helped bolster their reputation among the Chinese people and aided in recruiting thousands of members. Indeed, a strong argument can be made that it was political activism that initially brought the group together. A central question surrounding the organization is what type of relationship/affiliation if any it has with the government? Is it an officially authorized apparatus of the state or is it merely used as a surrogate to enforce Beijing's political view? Are there two groups working inside China, one a civilian organization and the other a branch of the People's Liberation Army? Is it possible that they work in conjunction with one another or does the civilian organization serve as a cover to disguise military operations?

The next most important series of questions that need to be answered concern the connection of the group to criminal activities. Is this the same set of Chinese hackers that media headlines claim are involved in Internet crimes such as phishing,⁴ pharming,⁵ and blackmail? How are they financed? Is there a darker side to this seemingly patriotic group?

Honker vs. Red Hacker Alliance

The organization of Chinese hackers is often referred to as the *Honker Union of China* by most open-source reporting to include the Chinese themselves. This report will instead refer to the organization as the "Red Hacker Alliance" as it is in the author's opinion, truer to the original Chinese. Hopefully, this will not cause confusion for those readers who are familiar with the subject matter and accustomed to seeing the organization referred to as the *Honker Union of China*. There are three main reasons for this shift away from the term Honker:

⁴ In computing, phishing is a form of social engineering, characterised by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an email or an instant message. The term *phishing* arises from the use of increasingly sophisticated lures to "fish" for users' financial information and passwords. Definition supplied by Wikipedia

<http://en.wikipedia.org/wiki/Phishing>

⁵ Pharming is the exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect traffic there and then to another web site. DNS servers are the machines responsible for resolving Internet names into their real addresses - the "signposts" of the Internet. Definition supplied by Wikipedia <http://en.wikipedia.org/wiki/Pharming>

1) The term Honker has little or no meaning in the English language. It can refer to a person who honks a horn; a slang term for the nose; or a goose.⁶ None of these definitions apply. Furthermore, it fails to provide the average Western reader with the undertones contained in the Chinese characters.

2) The Chinese use a combination of two characters to form a transliteration of the English word hacker. The first is 黑 (pronounced the same as the English word hay) and the second is 客 (pronounced the same as the hard C sound in could). The character 黑 means “dark” or “black” and the character 客 means “visitor” or “guest”. So in Chinese, hacker is represented as 黑客, or the “dark visitor.” There is a Romanization system developed to assist non-native speakers learn Chinese, called Pinyin, that assists in forming the sounds for these characters. In Pinyin, 黑客 is written as Heike. Chinese hackers later decided to change the 黑 to 红, which means “red” and is written in Pinyin as Hong. Thus, the group’s name became 红客 (Hongke). The term Honker is probably derived from a contraction of the Pinyin Hongke to Honker. The use of the Pinyin in this instance does not convey the true meaning of the characters. Substituting the color Red for Honker in the title also gives it a more patriotic feel to the translation that is much closer to the meaning and expresses the ideology of the alliance.

3) Adding more confusion to the term Honker is the way in which it has been applied over time. Initially, it seems to have been used to describe all the associated groups and individuals making up the alliance and may have actually been an umbrella moniker for this loose association. As the nature of the group took on greater form and substance, it became tied to one set in the group more than the others. To suggest that there is only one group is inaccurate. It is certainly an alliance, but it is an alliance of independent groups and not subject to the dictates of an individual leader or organization. Think of it as the evolution of a rock band. We will call it the “John Smith” Band. In the beginning the name covers all members and is simply billed as the John Smith Band. However, as time goes on and the lead singer, who we will call Tony (*Honker Union of China*), moves into the spotlight and gets greater press coverage, the band is now billed as “Tony and the John Smith Band.” More time elapses, Tony’s popularity increases and now the entire

⁶ Definitions supplied by Wordnet as downloaded on 24 Jan 06 from wordnet.princeton.edu/perl/webwn

group headlines as “Tony.” This is what appears to have happened with the Red Hacker Alliance.

NOTE: In this text, when the reader sees the term *Honker Union of China* it refers to only the one web site and its associated members, not the larger organization. When referring to the collection of all web sites the term Red Hacker Alliance will be used.

When asked to give a distinction between regular hackers and Red Hackers, the “Godfather”⁷ of Chinese hacking gave the following explanation:

*“Years ago, it was OK to be a hacker, when it simply referred to someone who would break into systems. But over the past decade, the attributes of hackers have become somewhat darker. Chinese hackers coined the word "Red Hacker", which means someone's a patriotic hacker. Unlike our Western counterparts, most of who are individualists or anarchists, Chinese hackers tend to get more involved with politics because most of them are young, passionate and patriotic. Most of them are politically motivated, as they need a way to protest against foreign matters. There's a lack of such an outlet in real Chinese society.”*⁸

⁷ While not named in the article, the “Godfather” probably refers to a man named Wan Tao, the leader of *China Eagle Union* who will be discussed later. Wan Tao has been dubbed the “Godfather” of Chinese hackers in other articles.

⁸ Vivien Cui, “‘Godfather’ of hackers fights for Web security”, *Hong Kong Sunday Morning Post*, 29 May 05, as translated by FBIS reference CPP20050530000043

Chinese Hacker Historic Timeline

Year	Major Incidents
1994-1996	Formation, Expansion, and Exploration
1997	1) The <i>Green Army</i> (China's first hacker group) is formed 2) <i>China Eagle Union's</i> preliminary web site registered as <i>Chinawill</i> and titled " <i>Voice of the Dragon</i> "
1998	Anti-Chinese riots in Indonesia ignite retaliation from Chinese hackers and provide the catalyst for the creation of the Red Hacker Alliance
1999	1) Cyber conflict between People's Republic of China and Taiwan over "Two-States-Theory" 2) Commercialism is introduced into the Green Army
2000	1) Denial of Nanjing Massacre leads to attacks on Japanese web sites 2) Taiwanese elections sparks conflict with mainland hackers 3) Beginning of "reckless desires" within the alliance 4) The <i>Green Army</i> falls apart over financial dispute 5) <i>Honker Union of China</i> founded by Lion 6) <i>China Eagle Union</i> founded by Wan Tao 7) <i>Javaphile</i> founded by Coolswallow and Blhuang
2001	1) The Red Hacker Alliance attacks Japan over "incidents" 2) Japanese web sites hit over Prime Minister's visit to controversial war memorial
2002	Attack on Taiwanese company <i>Lite-On</i> by <i>Javaphile</i>
2004	1) Chinese hackers hit Japanese government sites over disputed Diaoyu Islands 2) Lion announces the disbandment of the <i>Honker Union of China</i>
2005	<i>Honker Union of China</i> reforms

Definition of Red Hacker Alliance: A Chinese nationalist hacker network, made up of many independent web sites directly linked to one another in which individual sites educate their members on computer attack and intrusion techniques. The group is characterized by launching coordinated attacks against foreign governments and entities to protest actual and perceived injustices done to their nation. There is a growing trend that suggests monetary motivations are becoming as important as patriotic passion.

Criteria for Designating a Web site as a Member of the Red Hacker Alliance: An individual web site is designated as a member of the Red Hacker Alliance based off of the design, function, and content of its webpages. While they share many similar characteristics, three key elements must be present for inclusion in the Alliance:

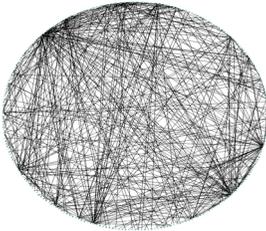
- 1) The primary function is to teach individual members computer attack and intrusion techniques
- 2) Must have an active membership architecture that allows new members to sign up, post articles, and exchange information internally
- 3) The site must be connected by hyper-links to one or more members of the alliance

Chapter 1

Chinese Hacker History

中国黑客历史

From Nationalism to Commercialism



Depiction of the 250+ web sites making up this study of the Chinese hacker network

The headlines in most major papers that cover Chinese hackers paint them as ethereal beings, invisible, coming from nowhere, invading, attacking, and then returning to their void. Media reports are filled with “Chinese hackers” involvement in one type of exploit or another, speculations about government affiliation, and the types of online crimes they have committed. What they fail to provide is background on just who comprises this secretive organization. Certainly, these spirits from a land as unfathomable as China must be impossible to locate, much less study. The reality turns out to be considerably less mysterious and much more mundane. Chinese hackers are incredibly easy to find and provide more information about themselves than anyone reading the news could imagine. The problem is not a lack of information but an overabundance of it. The Red Hacker Alliance is producing thousands of internal documents just waiting to be translated and studied. No special computer skills are required and you do not need the ability to detect and track an intruder over countless Internet connections or jumps between satellites. It doesn’t require a government clearance with access to classified documents. The information has been sitting in the open since the very founding of the organization and it is this very information we will use to examine their history, structure, exploits, political agenda, and possible government affiliations.

While not an unbroken historic timeline, we will trace the birth of Chinese hackers on the Internet from a purely nationalistic organization, to their current situation that is rapidly expanding into commercialization and criminal activity. Before looking directly at the history of the Chinese Red Hacker Alliance, it is perhaps vital that we have an understanding of China’s past and how it affects its population’s current psyche in order to get greater

insight into why these groups are so much more nationalistic than their Western counterparts.

Historically, China has endured numerous outside threats to its sovereignty and what it views as insults to national honor. This has perhaps produced a mindset more sensitive to actual and perceived injustices. Having the ability to protest against these humiliations, as is the case with Chinese hackers, must be a very potent source of empowerment. The majority of the alliance is comprised of males in their 20's that hold the passions of youth. Being somewhat prohibited from protesting against their own society's injustices, they are quick to retaliate against both major and minor offenses from outside sources. William Callahan's work on the rise of Chinese nationalism stemming from the "Century of Humiliation" provides a very detailed look at these motivators pushing the rise of nationalism:

"Chinese nationalism is not just about celebrating the glories of Chinese civilization; it also commemorates China's weakness. This negative image comes out most directly in the discourse of China's Century of National Humiliation (Bainian guochi). Chinese books on the topic generally tell the tale of China going from being at the center of the world to being the Sick Man of Asia after the Opium War (1840), only to rise again with the Communist Revolution (1949). To understand how Chinese nationalism works, we need to reverse Paul Kennedy's famous thesis about 'the rise and fall of the great powers' to examine the 'fall and rise' of China: Many of the titles of these books include the phrase 'from humiliation to glory.' The discourse of national humiliation shows how China's insecurities are not just material, a matter of catching up to the West militarily and economically, but symbolic. Indeed, one of the goals of Chinese foreign policy has been to 'cleanse National Humiliation.'"⁹

Indeed this very sentiment was reflected to near perfection on the web site *Iron and Blood Union*, which is linked to several of the Red Hacker Alliance web sites. They articulated their philosophy as follows:

⁹ William A. Callahan, "National Insecurities: Humiliation, Salvation, and Chinese Nationalism," *Centre for Contemporary Chinese Studies, Department of Politics, University of Durham, Durham, UK*, 2004, as downloaded on 24 Aug 2005 from <http://www.humiliationstudies.org/documents/CallahanChina.pdf>

“The goal of this community: Is to grieve for the prior generation and to never forget the nation’s shame; to use history as an example for facing the future.”¹⁰

While the case can be made that the government has the ability to fan the flames of patriotic zeal inside the Red Hacker Alliance, it is apparent that it already exists within the group and is not fabricated. It is also doubtful that the Chinese government is overly enthusiastic about causing major unrest in large numbers of students, who comprise a substantial portion of the hacker organization. Student led demonstrations during the May 4th Movement of 1919 and Tiananmen Square in 1989 are deeply ingrained in their memory. The case can also be made that nationalism provides a certain shield against government scrutiny and possible interference. By Chinese government standards, this is a large group of individuals with common ties that are not easily monitored or controlled. If the Chinese hacker alliance did not set very strict internal guidelines or failed to clearly show its support of the government/people, it might quickly find itself censored and broken apart. The political activist nature of the groups making up the alliance has also bolstered their reputation within China and may have perpetuated their nationalistic character.¹¹

CAUTION: The historical account that follows has been primarily pieced together from documents obtained off of Red Hacker web sites and expresses their perspective on how events began and unfolded. This note of caution should not and is not intended to cause the reader to discount the Chinese rendering of events. To the contrary, the descriptions they provide are quite compelling and introspective. As with any story, there is always the possibility of exaggeration and misinformation (not to be confused with disinformation¹²). The major sin that may have been committed would be that

¹⁰ *Iron and Blood* is a military enthusiast site but has links to the Red Hacker Alliance. It is also heavily anti-Japanese. <http://www.tiexue.net/>

¹¹ Unknown, “The Growth of the Chinese Computer Hacker,” *KKER Union of China*, 20 Nov 2004, as downloaded on 23 Aug 2005 from <http://www.kker.cn/book/list.asp?id=1264>

¹² Disinformation: in the context of espionage, military intelligence, and propaganda, is the spreading of deliberately false information to mislead an enemy as to one's position or course of action. It also includes the distortion of true information in such a way as to render it useless. Definition supplied by *Wikipedia* <http://en.wikipedia.org/wiki/Disinformation>

of omission and not commission. The Chinese hackers have presented us with the portion of their history that shows the strong patriotic side of the alliance and has chosen to delete that portion that did not. When deemed appropriate, comments and analysis have been added.

The Beginning and Expansion (1994-1996)

According to Chu Tianbi, the author of *Chinese Hacker History/Looking Back on the Chinese Hacker History*, the origin of Chinese hacking began in 1994 when the Internet was first made available to the public. Chu describes this as a period of familiarization, when even the term “Internet” was not widely understood by the general populace and related terminology was only found in “highly specialized publications.”¹³ Even with the opening up of the Internet, access was primarily confined to “science and technology research personnel” and “rich young people.” Users operated off of 9,600 bit/second modems and dialed directly into Bulletin Board System (BBS) servers. The programs they were exposed to fascinated Chinese users who immediately began to decode them. The year 1995 marked an escape from the dialup BBS, as mid-sized cities in China began to provide Internet portals. Chu Tianbi captures this preliminary step by stating:

“In their view, moving from BBS to the Internet was an expansion of their stage and allowed them to see a bit more.”¹⁴

Chu also tells us that this period was discernible by a rapid acceleration in technical skills for the Chinese “crackers.”¹⁵ One of the most famous crackers

¹³ Chu Tianbi, “Chinese Hacker History/Looking Back on Chinese Hacker History,” *Blog China News*, as downloaded on 9 Aug 2005 from <http://www.blogchina.com/news/source/310.html>

¹⁴ *Ibid*

¹⁵ Cracker - An individual who attempts to gain unauthorized access to a computer system. These individuals are often malicious and have many means at their disposal for breaking into a system. Crackers often like to describe themselves as hackers. Cracking does not usually involve some mysterious leap of hackerly brilliance but rather persistence and repetition of a handful of fairly well known tricks that exploit common weaknesses in the security of target systems. Definition supplied by www.infosec.gov.hk/english/general/glossary.htm

during this time was Gao Chunhui,¹⁶ whose homepage, dedicated to cracking software codes and registration codes, received the largest number of hits in China for that time period. In 1996, favorable Internet policy shifts by China Telecom brought the Internet into the homes of ordinary Chinese.

The *Green Army* Founded (1997)

In 1997, there were only seven rudimentary Chinese hacker web sites and the contents contained in them were primarily copied from overseas. Indigenously produced attack methods were almost nonexistent during this time and most Chinese hackers relied on e-mail bombs supplied in prepackaged toolkits.¹⁷ The year 1997 also saw the establishment of the *Green Army*, sometimes referred to as the “Whampoa Military Academy,” claimed to be one of China’s earliest hacker organizations. The *Green Army* took on the nickname Whampoa Academy in tribute to the original academy established in 1924 as a training facility for Chinese military officers by Dr. Sun Yat-sen and the Communist Party of China. Funding for the training facility was provided by the former Soviet Union.¹⁸

¹⁶ According to an article posted on the site *ITHACK*, Gao Chunhui was born in March of 1975 in Liaoning Province.
<http://www.ithack.net/Articles/iter/20050318972.html> The originator of the article is not cited.

¹⁷ Unknown, “The Growth of the Chinese Computer Hacker,” *KKER Union of China*, 20 Nov 2004, as downloaded on 23 Aug 2005 from
<http://www.kker.cn/book/list.asp?id=1264>

¹⁸ History and photo of the Whampoa Military Academy downloaded from the Guangdong University of Technology web site.
http://web.gdut.edu.cn/~draw/ICGG2004/GUANGZHOU/attr_05.htm



Gate at Huangpu Leading into the Whampoa Military Academy, now a tourist site.

The *Green Army* was founded by a Shanghai hacker going by the online name of Goodwill,¹⁹ it was reported to have had a membership of around 3,000 people from Shanghai, Beijing, and Shijiazhuang. The other four key members of the group went by the pseudonyms Rocky²⁰, Dspman (HeHe), Solo, and LittleFish. It also attracted others, considered to be part of China's first generation hackers, the likes of Xie Zhaoxia, Brother Peng, PP (Peng Quan), Tian Xing (Cheng Weishan), IceWater (Huang Lei), and Little Rong. The group disbanded in 2000 and its rise and fall was described as “confusing” by insiders who consider it one of the enduring symbols of the Chinese hacker movement. The *Green Army* is said to have hacked “uncountable foreign web sites.” Indeed, many of China's top hackers were past members of this group.²¹

¹⁹ Goodwill has also been rendered as Goodwell and Goodwel. All versions could be possible transliterations of the Chinese characters 龚蔚 (Gong and Wei) reported to be the founder's true surname. Photo of Goodwill downloaded from *China Eagle* web site on 8 Feb 06 <http://www.chinaeagle.org/about/lc.html>. The picture refers to him as Goodwell.

²⁰ Rocky was later killed in a traffic accident <http://bbs.isbase.net/search.php?searchid=161772>

²¹ Li Zi, “The Chinese Hacker Evolution,” *Times Weekly Personality Report*, 10 Mar 2005, downloaded on 9 Aug 2005 from <http://net.chinabyte.com/386/1920386.shtml>



left unknown, center Wan Tao, right Goodwill

China Eagle Union the Early Years (1997)

This was also the “gestation period” for *China Eagle Union*, founded by Wan Tao and currently one of the strongest groups active in the Red Hacker Alliance. His site was initially registered under the name *Chinawill* and titled “*Voice of the Dragon.*” Wan Tao’s views on this preliminary step in the history of the *China Eagle Union*:

“I registered the international domain and space for CHINAWILL way back on June 26, 1997, with a view to creating a web site for investigating Chinese history and China’s future. The meaning of CHINAWILL is: China’s will to be; China will be what; China will be where. The name of the web site was “Voice of the Dragon,” and had topics such as the dragon’s dreams and my love for my family, etc. But I didn’t have sufficient experience, and due to reasons such as a lack of help, the plan never came to fruition. But, I believed that as the frequency of people going online went up

*there would be more excellent participants coming in—China will be great!*²²

Leaps, Horses, and Riots (1998)

The year 1998 was considered the “Great Leap Forward” in Chinese hacking and coincided with the US hacker group Cult of the Dead Cow’s²³ release of their Back Orifice program²⁴ and its source code. This software was the catalyst that began the rapid use of the Trojan horse program as a means of attack and its subsequent spread to Chinese hacker organizations. However, Back Orifice itself did not become very popular in China for two reasons: first, the network was still developing and second, Back Orifice was a foreign product that was difficult for Chinese hackers to use. The release of the CIH Virus²⁵ by a Taiwanese programmer also had a profound effect on the mainland hackers. The CIH virus caused significant financial losses to the Chinese nation and was viewed as an outside threat and attack on the country.²⁶ Rumors circulated in China that it had been written by a “mentally unstable” Taiwanese soldier that specifically targeted simplified Chinese characters (the Taiwanese use traditional characters). Reports stated that

²² Unknown (the author is more than likely Wan Tao), Untitled, *China Eagle*, downloaded on 8 Feb 06 from <http://www.chinaeagle.org/about/lc.html>

²³ Cult of the Dead Cow (cDc) is a high-profile computer hacker organization founded in 1984 in Lubbock, Texas. Definition of organization supplied by wikipedia on 23 Aug 2005, http://en.wikipedia.org/wiki/CULT_OF_THE_DEAD_COW

²⁴ Back Orifice and Back Orifice 2000 (BO2k) are controversial computer programs designed for remote system administration. They enable a user to control a computer running the Microsoft Windows operating system from a remote location. The names are a pun on Microsoft’s BackOffice Server software. Definition supplied by wikipedia on 23 Aug 2005, http://en.wikipedia.org/wiki/Back_Orifice

²⁵ CIH, also known as *Chernobyl* or *Spacefiller*, is a computer virus written by Chen Ing Hau of Taiwan. It is considered to be one of the most harmful widely circulated viruses, destroying all information on users’ systems and in some cases overwriting the system BIOS. Definition supplied by wikipedia on 23 Aug 2005, http://en.wikipedia.org/wiki/CIH_virus

²⁶ Unknown, “The Growth of the Chinese Computer Hacker,” *KKER Union of China*, 20 Nov 2004, as downloaded on 23 Aug 2005 from <http://www.kker.cn/book/list.asp?id=1264>

damages from the virus exceeded 1 Billion Renminbi (approximately US \$123 million).²⁷

The Indonesian Riots (Cyber Conflict of 1998)

Up until this point, although groups were forming such as the *Green Army* and communications were taking place between individuals, a unified group or ideology binding these loose confederations of hackers had yet to occur. The event that seems most responsible for coalescing these relatively independent cells was the 1998 riots that occurred in Jakarta, Indonesia. During this period, the Indonesian populace unfairly blamed their ethnic Chinese community for the country's out of control inflation. Indonesian citizens turned on the Chinese living among them and committed murders, rapes, and the destruction of their businesses.²⁸ While the incidents were not reported in Chinese domestic news, the stories and pictures of the atrocities were broadcast over the Internet and viewed by Chinese hackers.²⁹ Individual outrage over the violence needed an outlet, which in turn caused an almost spontaneous gathering of hacker groups in Internet Relay Chat (IRC)³⁰ rooms. In retaliation for these ethnic attacks, the groups formed the "Chinese Hacker Emergency Conference Center"³¹ and worked in concert to send e-mail bombs to Indonesian government web sites and mailboxes, while at the same time

²⁷ "China: Information Security," *US Embassy China*, Jun 99, downloaded on 9 Jan 06 from <http://www.usembassy-china.org.cn/sandt/infscju99.html>. Exchange rate of 8.08 Renmenbi to the US dollar used for this calculation.

²⁸ "Anti-Chinese riots continue in Indonesia," *CNN News CNN.com/World*, 29 Aug 1998, as downloaded on 23 Aug 2005 from <http://www.cnn.com/WORLD/asiapcf/9808/29/indonesia.riot>

²⁹ Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

³⁰ Internet Relay Chat is a chat system that enables people connected anywhere on the Internet to join in live discussions. To join an IRC discussion, you need an IRC client and Internet access. Definition provided by www.saol.com/glossary.asp

³¹ There are differing accounts of the date this group was established. One of those accounts claimed that the group was formed on 9 May 1999 in response to the Chinese Embassy bombing. It is likely that during each of the incidents, a "Chinese Hacker Emergency Conference Center" was established to assist in communications among the groups.

carrying out Denial-Of-Service (DOS) attacks³² on Indonesian domestic sites. The coordinated efforts brought about a strong sense of unity to the organization and were instrumental in persuading many others to join in the activity.³³ On 7 August 1998, the chief-editor of *China Byte*³⁴ discovered a new posting, declaring that Chinese hackers had been able to gain access and penetrate Indonesian web sites. Along with the posting, the hackers attached the address of the defaced web site that was still un-repaired.³⁵ After verifying the story, the editor of *China Byte* decided to include it in an update to their e-mail news subscribers. The update contained only two sentences from the defacement but conveyed the essential information that the Chinese had posted on the Indonesian web site:

*“Your site has been hacked by a group of hackers from China. Indonesian thugs, there can be retribution for your atrocities, stop slaughtering the Chinese people.”*³⁶

This update was mailed to tens of thousands of subscriber mailboxes within minutes and the *China Byte* story was picked up on the 10th of August in a newspaper headline stating that Indonesian atrocities had enraged Chinese hackers. The attack had actually been put into motion prior to the 7th, when Chinese hackers gained administrators’ rights to Indonesian web sites by

³² A denial-of-service attack is an attack on a computer system or network that causes a loss of service to users, typically the loss of network connectivity and services by consuming the bandwidth of the victim network or overloading the computational resources of the victim system. Definition supplied by Wikipedia
http://en.wikipedia.org/wiki/Denial_of_service

³³ Unknown, “The Growth of the Chinese Computer Hacker,” *KKER Union of China*, 20 Nov 2004, as downloaded on 23 Aug 2005 from
<http://www.kker.cn/book/list.asp?id=1264>

³⁴ *China Byte* is one of China’s leading IT online media and wireless service providers and is a joint venture with the *People’s Daily*.
<http://www.chinabyte.com/TLimages/cbweb/about.htm>
http://english.people.com.cn/english/200104/18/eng20010418_67993.html

³⁵ The Indonesian web site was only identified as kobudi.co.id, Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

³⁶ Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from
<http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

breaking their passwords. The main web pages were plastered with slogans such as:

“My fellow countryman, I weep for your grief and indignation”
and *“Severe punishment for the thugs! Severe punishment for the murderers! There is a blood debt and the blood must be repaid!”*³⁷

The hackers would strike again on the 17th August, Indonesia’s National Day, reminding the Indonesians of the atrocities committed against the Chinese.³⁸ The Indonesian government protested these incidents and claimed that they were state sponsored by the People’s Republic of China. Bundi Rahardjo, from the Indonesian Computer Emergency Response Team, had this to say:

*“Vandals from Taiwan, China are doing low-tech attacks (such as mailbomb), they are mad with Indonesia's policy and blamed Indonesians for the riot in [May] (which was targeted against Chinese-descendants).”*³⁹

Giving some specifics of the attack, Mr. Rahardjo further elaborated that the e-mail bombs were large in size and sent in volumn. In a clear reminder to be careful what you wish for, Mr. Rahardjo went on to say:

*“‘Why don't they create their own Web sites?’ Most of the attacks (attackers) are known, [t]he origin of mailbombs are also known.”*⁴⁰

The Indonesian riots mark one of the most important points in Chinese hacker history and cannot be stressed enough; it is in this period where we truly see the beginning outline of the Red Hacker Alliance. As Sharp Winner, a current member of the Red Hacker Alliance put it:

“A group of patriotic youth active on the net engaged in attacks on Indonesian government web sites, under the alias ‘China

³⁷ Ibid

³⁸ Ibid

³⁹ James Glave, “Cyber Vandals Target Indonesia,” *Wired News*, 18 Aug 98, as downloaded on 15 Nov 2005 from <http://wired-vig.wired.com/news/politics/0,1283,14483,00.html>

⁴⁰ Ibid

Redhackers.’ This patriotic action received a great deal of reporting and praise in the domestic and overseas media. The name China redhackers began here.’⁴¹

From the standpoint of the Chinese hackers, the organization had been formed. They suddenly realized the power their group could wield and that this power was an independent voice from their government. As a collective, they were no longer left feeling impotent in the face of world events. The alliance had made an impact; local and foreign officials had responded openly to their protests and they were not forced to swallow indignation. The publicity generated by their actions also attracted large numbers of recruits and brought with it a certain amount of fame inside the country.



One of the Indonesian web sites defaced by Chinese hackers

One other observation about this event is worth noting: while some have described this type of activity as rioting on the Internet or “cyber rioting,” there is a difference here. The Chinese, even though outraged by these crimes, maintained some degree of restraint. They did not slash and burn every system they could penetrate, as evidenced by the above

⁴¹ “The Ever-Changing Red Hacker Sharp Winner,” Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, 13 Sep 2005, as downloaded on 17 Oct 2005 from <http://forum.gd.sina.com.cn/cgi-bin/viewone.cgi?gid=51&fid=1359&itemid=8191>

defacement. The bottom sentence left instructions on how to return the site back to its original form.

The Birth of Commercialism (1999)

Commercialization of these nationalist hackers first began on 23 January 1999, when the *Green Army* held its first annual conference at No. 6, 128 Nong, Yanan East Road, Shanghai (Xingkong Net Cafe). The network security market was in the process of becoming a financial powerhouse inside China and it was reasoned that Chinese hackers, who understood attack techniques, could create and claim a portion of the market. Enter Shen Jiye, a venture capitalist/entrepreneur from Beijing, who was introduced to the *Green Army* by one of its members Zhou Shuai (online name of Coldface).⁴² Shen Jiye was able to meet with Goodwill and other key members of the organization and convince them to go commercial. The *Green Army* would later change its approach and create its own network security company – the Shanghai Green Alliance.⁴³ While this initial foray into the financial market did not shatter the group or stifle the nationalist tone, it did introduce an additional motivation for their activities...money.

The Taiwan “Two-States-Theory” (Cyber Conflict of 1999)

In July of 1999, Taiwanese President Li Deng-Hui advocated the “Two-States-Theory,” advancing the concept of Taiwan as a separate nation state, independent of mainland China. This openly defied the “One-China” policy of the People’s Republic of China, which stated there is only one China. This perceived threat to Chinese sovereignty ignited a round of attacks between PRC and Taiwanese hackers. The strikes began on 7 August, with mainland hackers hitting more than 10 Taiwanese government web sites and posting such messages as:

⁴² Li Zi, “The Chinese Hacker Evolution,” *Times Weekly Personality Report*, 10 Mar 2005, downloaded on 9 Aug 2005 from <http://net.chinabyte.com/386/1920386.shtml>.
<http://sys.asiaic.org/> Chinese version on Wuhan Netbar

⁴³ Li Zi, “The Chinese Hacker Evolution,” *People in Focus Weekly*, 10 Mar 2005, as downloaded on 9 Aug 2005 from <http://net.chinabyte.com/386/1920386.shtml>

“There is only one China in the world and the world only needs one China.”⁴⁴

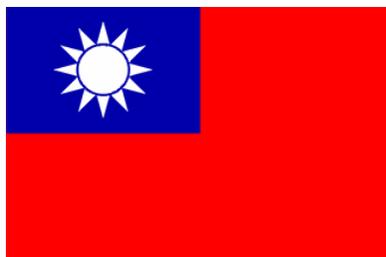
Taiwanese hackers immediately launched a counter-attack on 8 August posting:

“Taiwan is a permanent separate entity from China. You dare to strike, we dare to be independent.”⁴⁵

The mainland hackers posted the 5-Star Flag of the People’s Republic of China and the Taiwanese posted their national flag with the blazing sun.⁴⁶ Newspaper headlines in Hong Kong and Taiwan led with banners titled “Wild Web site War Between Hackers on Both Sides of the Strait,” “Internet War Shows No Signs of Weakening,” and “Opening Shots in Internet War: an Unavoidable War.” The mainland hackers even criticized some of the reporting as “reckless” and cited the following as an example: “Armies on Both Sides of the Taiwan Strait Continue to Threaten Each Other and Monitor Troop Movements, but the Prologue to a Computer Information War by civilians has Already Begun.”⁴⁷



National Flag of the PRC



National Flag of Taiwan

This episode played a pivotal role in the way mainland Chinese hackers fought and would fight future conflicts. It was during this conflict that a Chinese security programmer named Huang Xin designed the first prototype of the “Glacier” Trojan horse. No longer were the Chinese relying

⁴⁴ Ibid

⁴⁵ Ibid

⁴⁶ Ibid

⁴⁷ Ibid

on hacker tools produced outside the country for attacks; they were beginning to develop methods of their own. This is also the same time that the Trojan horse “NetSpy” was developed. With improvements to the construction of Glacier’s code and the release of the 2.2 Edition, Glacier quickly became one of the Chinese hackers’ favorite tools. It is claimed that Glacier inspired the production of more domestically produced hacker software such as “Black Hole,” “NetThief,” “Gray Pigeon,” “XSan,” and “YAI.”⁴⁸

Toward the end of August, a temporary truce occurred between the mainland and Taiwanese hackers. However, Taiwanese hackers threatened that they would launch large-scale attacks on mainland web sites on October the 1st and in response, the mainland hackers said that if that happened they would counterattack on October the 10th.⁴⁹ The August 1999 fight between the two groups set a tone of antagonism between the two groups that lasts until this very day. It was said that the “war is a never-ending war, and any irritant can incite attacks.”⁵⁰

The Japanese Denial of the Nanjing Massacre⁵¹ (Cyber Conflict of 2000)

The year 2000 would bring both highs and lows for the Red Hacker Alliance. From late January to mid-February, a group calling themselves the “Ultra Right-Wing Chinese Hackers Opposed to Japan Alliance”⁵² claimed to have attacked some 30 Japanese web sites “belonging to the ministries, the prime minister, parliament, and the state planning agency.”⁵³ This was in

⁴⁸ Unknown, “The Growth of the Chinese Computer Hacker,” *KKER Union of China*, 20 Nov 2004, as downloaded on 23 Aug 2005 from <http://www.kker.cn/book/list.asp?id=1264>

⁴⁹ Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

⁵⁰ Ibid

⁵¹ At the end of 1937 the Japanese military seized control of Nanjing and it is reported that during a 6-week period killed upwards of 300,000 Chinese civilians.

⁵² Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

⁵³ “Chinese ‘Right-Wingers’ Vow To Hack Japanese Web sites,” *Hong Kong AFP*, 14 Feb 00, as transcribed by FBIS reference number *CPP20000214000027*

retaliation for what the hackers perceived as a denial of the Nanjing Massacre following the loss of a Japanese court case by Azuma Shiro.⁵⁴ Azuma Shiro was a Japanese soldier who maintained a diary during WWII that recounted Japanese atrocities in Nanjing. The diary was published and his former superior immediately sued Shiro for libel. Shiro lost the case and subsequent appeals in 1998 and 2000. Their web site, located at <http://www.bsptt.gx.cn/public/badboy/hack/>, posted an open letter to the Japanese government that stated:

*“Let it be known that the objective of this alliance is to carry out savage attacks on the small number of Japanese mad-dogs on the net. The alliance is comprised completely of fervent patriotic Chinese net-worms.”*⁵⁵

The site provided over 300 Japanese government URLs,⁵⁶ the e-mail addresses of over 100 Japanese representatives, and dozens of the most effective hacker attack tools. Furthermore, the site explained how to use these tools to attack Japanese web sites.⁵⁷ In an online interview with *Computer Journal*, a hacker calling himself “ROOT,” admitted that the paralysis of the web sites for the prime minister’s office, the Bureau of Statistics, and the Bureau of Science and Technology were his doing. ROOT complained that the attacks on Japanese web sites occurred because of dissatisfaction with the Japanese government’s far right denial of the historical facts of the Nanjing Massacre:

⁵⁴ “Canadian Conference on Preventing Crimes Against Humanity: Lessons from the Asia Pacific War (1931-1945),” 21-22 Mar 2003, as downloaded from <http://www.aplconference.ca/descriptions.html> on 27 Oct 2005

⁵⁵ Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>; The translation net-worms comes from the characters 网虫 (net and insect/bug/worm) and may NOT be an accurate translation of the term. It is possible that this is slang and generally understood to carry a different meaning, something along the lines of geek.

⁵⁶ A Uniform Resource Locator, URL, or Web address, is a sequence of characters, conforming to a standardized format, that is used for referring to resources, such as documents and images on the Internet, by their location. Definition provided by Wikipedia http://en.wikipedia.org/wiki/Uniform_Resource_Locator

⁵⁷ Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

*“I did absolutely everything by myself. The payback for little Japan didn’t require anyone else. I think I’ve done what anyone should have done as a Chinese person, and anyone else would have done this. I hope they connect what I’ve done with what happened in Osaka, giving a warning to the Japanese devils.”*⁵⁸

The year 2000 would also see the ranks of those that could access the net swell, as Internet cafes opened up all over the country. This upswell in the ranks brought in a new group of hackers that had “reckless desires.” This radical fringe element would ultimately lead to disorder within the alliance. Exuberant youth, in an effort to become a part of the group, went to extremes and acted outside of the norms of the community.

Once again, Chu Tianbi:

*“Of course, during this year, the expansion of hacker groups led to the appearance of many false hackers. Among these false hackers, Man Zhou’s plagiarism of ‘Secrets of Guarding against Hacker Attacks’ was the most notable. This high-school-aged youth, who called himself the China Security General, plagiarized a large number of Chinese hackers’ essays and writings and then grandiosely placed his own name on them and submitted them to an electronic publication company for publication. This small handbook, full of errors and only to be considered an electronic publication, pushed false hacker behavior in China toward the extreme. After this, many false hackers, not knowing the first thing about technology, jumped up on stage, presenting one farce after another using various methods. Not only did this pollute the hacker spirit in China, it also became the most sordid corner of Chinese hacker history.”*⁵⁹

“After we entered the new century, Japan’s anti-Chinese sentiment grew increasingly rampant, and the Mitsubishi incident, the Japan Airlines incident, the textbook issue, and the ‘Taiwan Theory’ angered Chinese hackers. With several Chinese hacker web sites in the lead, they organized a number of large-scale hacker activities against Japan. During this time, some of the foolish hacker software also appeared, the most well known of which included ‘China Boy’ by Janker. The lowering of technological barriers had

⁵⁸ Ibid

⁵⁹ Chu Tianbi, “Chinese Hacker History/Looking Back on Chinese Hacker History,” as downloaded on 9 Aug 2005 from <http://www.blogchina.com/news/source/310.html>

led to the appearance of many young hackers, and off-the-shelf tools and software armed these youths who knew nothing about network technology, but were also a cause of later young hackers' ignorance and underestimation of technology."⁶⁰

Chu Tianbi's essay further explains that:

*"In addition, it was also in this year that the entirely new concept of 'Blue Hackers' arose. During this time, Chinese hackers could essentially be divided into three categories. One was hackers with a political and nationalistic bent represented by the Chinese Red Hackers. Another was the technical hackers purely interested in Internet security technology and not concerned with other issues, represented by the Blue Hackers. The last type was the original 'Black' Hackers who were entirely concerned with pursuit of the original hacker spirit and did not focus on politics or the frenzied pursuit of technology."*⁶¹

The Taiwanese Election (Cyber Conflict of 2000)

The evening of 18 March 2000 would see another wave of offensive attacks against the Taiwanese following the election of pro-independence presidential candidate Chen Shuibian. A hacker calling himself Sky Talk left the following message:

"Sky Talk here. I'm from Zhejiang, but I am working outside of the province. My monthly salary is 800 Renmenbi (RMB).⁶² I'm not poor, and not rich. I wear warm clothes and eat well enough. I'm a normal person, one of the common herd, of no social standing at all. I didn't even go to high school! Altering the pages of a few Taiwanese web sites was done completely out of rage! If you want to split up China, I think every Chinese person feels just like me when it comes to this attitude! You're attacking our web sites in China, and last night there was even a 'cute' so-called 'hacker' who was interested in the HTTPD of my personal computer. Ha ha...his IP address was (address deleted). You can see that I don't

⁶⁰ Chu Tianbi, "Chinese Hacker History/Looking Back on Chinese Hacker History," as downloaded on 9 Aug 2005 from <http://www.blogchina.com/news/source/310.html>

⁶¹ Ibid

⁶² The exchange rate of 8.08 works out to 99 dollars/month US.

need to explain the intensity of your attack on me! Let me give a warning! I have stopped cracking Taiwanese host computers, but when I heard about your counterattacks and the destruction of several Chinese web sites, my patience has limits. Last night I entered your host computers for National Defense. I'd planned to do a deltree/y c:\, but then I thought that this might start a hacker war! Considering that this would benefit no one, I exited Telnet and closed the port, and may have closed port 80 at the same time (I'm terrible at this! :)) I'm putting up a gallery! I hope that you can leave this dispute behind!!”⁶³



Hack of Tawanese Web Site by Sky Talk

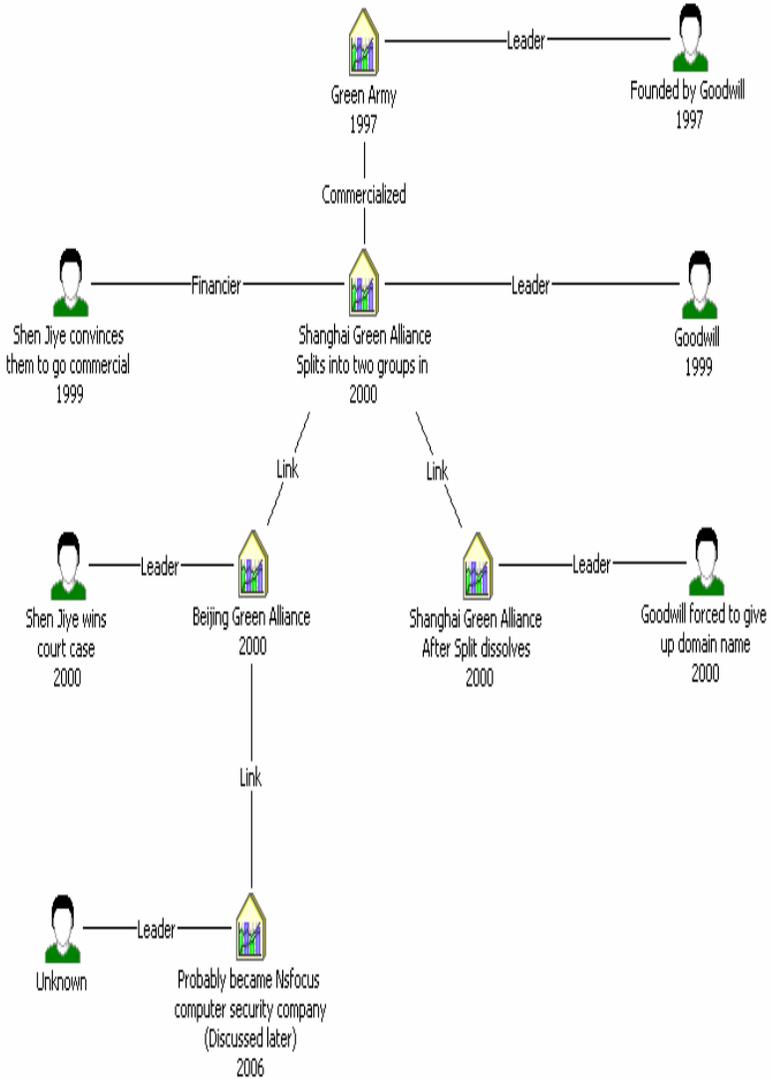
Commercialism Heats Up

March of 2000 witnessed the breakup of the *Green Army*, the organization that started the Chinese Red Hacker movement. In July, cooperation between controlling parties deteriorated and their commercial enterprise ended up in court with both parties suing. The legal battle also saw mutual hacking attacks against one another. In August, the legal case was decided in favor of the Beijing Green Alliance and Shen Jiye. The Shanghai Green Alliance, led by founder Goodwill, owed the Beijing faction 300,000

⁶³ Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

Yuan (approximately US \$36,720) and was forced to turn over the domain isbase.com. Regarding the cause of the break-up, there are two versions of the story.

The first version is that Beijing Green Alliance was well along in commercialization and did not want to turn back to freelance hacking that was advocated by members of the *Green Army* of the Shanghai Green Alliance. Apparently, Goodwill wanted to be the first non-profit network security organization in China but others (probably Shen Jiye), saw it as a commercial venture. Eventually, the profit motive won out.



Flow chart showing the Green Army from its founding in 1997 by Goodwill until it is taken over by Beijing Green Alliance in 2000 and probable transformation to NSFOCUS Computer Security Company

Another version of the break-up also involves finances. Goodwill and other key members saw themselves as the founders of the *Green Army* and therefore reasoned that they should have a greater share of the company. Shen Jiye argued that the organization was already commercialized and should follow the company's principles of letting the capital decide. In an interview with *People In Focus Weekly*, Shen Jiye said:

*"It was primarily because of individual profit. It's because Goodwill was being too selfish. The degree of one's reputation on the Internet can't be the standard of one's commercial value to the company."*⁶⁴

Zhou Shuai confirmed that the entire dispute was earnings driven and others involved said they felt that Goodwill was partially responsible for the break-up. Afterwards, the *Green Army* had many setbacks, lost their web site and dismissed all members. According to Zhou Shuai, the *Green Army* remains in existence but it is nothing more than a loose academic alliance.

The *Green Army* is one of the organizations that has managed to stand the test of time and moved toward more legitimate enterprises. Its offspring appears to be the computer security company NSfocus. While the name NSfocus is used in the English translation of the web site, the Chinese name Green Alliance still appears on the Chinese side. The company web site also maintains a list of all its founding members, which reads much like a Who's Who of Chinese hackers.⁶⁵

The member site shows that all the primary founding members of the Green Army are listed on the NSfocus company web site: Goodwell (Goodwill), Solo, Little Fish, and Cold Face

⁶⁴ "The Ever-Changing Red Hacker Sharp Winner," Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, 13 Sep 2005, as downloaded on 17 Oct 2005 from <http://forum.gd.sina.com.cn/cgi-bin/viewone.cgi?gid=51&fid=1359&itemid=8191>

⁶⁵

http://bbs.nsfocus.net/index.php?act=Members&max_results=10&filter=ALL&sort_order=asc&sort_key=joined&keyword=&page=1
<http://bbs.nsfocus.net/index.php?act=Members> 20 Sep 06



绿盟科技
NSFOCUS

MIRACLES EVERYDAY

www.nsfocus.com

★ 首页

★ 企业版 ★ 技术版 ★ ENGLISH

紧急通告 安全公告 安全漏洞 业界动态 安全文摘 工具介绍 绿盟原创 绿盟月刊 安全论坛

欢迎您 游客 ([登陆](#) | [注册](#))

[搜索](#) | [用户列表](#) | [帮助](#)

[绿盟安全论坛](#) -> [用户列表](#)

共 57481 用户 分页 (5748) < [1] 2 3 4 5 6 ... >

用户名	用户组	注册时间	发帖数	Email
feeling	注册用户	1970-01-01	92	-
solo	注册用户	1999-08-24	115	-
小鱼儿	注册用户	1999-08-25	45	-
littlefish	注册用户	1999-08-25	0	-
goodwell	注册用户	1999-08-25	88	-
张影	注册用户	1999-08-25	57	-
郑敬	注册用户	1999-08-25	0	-
hwj	注册用户	1999-08-25	0	-
LOTUS	注册用户	1999-08-25	0	-

显示 按 - 排列 每页 个用户 关键字

共 57481 用户 分页 (5748) < [1] 2 3 4 5 6 ... >



MIRACLESEVERYDAY

www.nsfocus.com

★首页

★企业版 ★技术版 ★ENGLISH

绿盟科技
NSFOCUS

紧急通告 安全公告 安全漏洞 业界动态 安全文摘 工具介绍 绿盟原创 绿盟月刊 安全论坛

欢迎您 游客 ([登陆](#) | [注册](#))

[搜索](#) | [用户列表](#) | [帮助](#)

绿盟安全论坛->用户列表

共 57481 用户 分页 (5748) < [1](#) [2](#) [3](#) **[4]** [5](#) [6](#) [7](#) [8](#) [9](#) ... >

用户名	用户组	注册时间	发帖数	Email
coldface	注册用户	1999-08-25	69	-
明波	注册用户	1999-08-25	2	-
wangqi	注册用户	1999-08-25	5	-
aming	注册用户	1999-08-25	1	-
yandou	注册用户	1999-08-25	0	-
flyfly	注册用户	1999-08-25	290	-
ck	注册用户	1999-08-25	118	-
quack	老油条	1999-08-25	371	-
gj	注册用户	1999-08-25	60	-
oldboy	注册用户	1999-08-25	0	-

显示 [所有用户](#) 按 [注册日期](#) - [正序](#) 排列 每页 [10](#) 个用户 关键字

共 57481 用户 分页 (5748) < [1](#) [2](#) [3](#) **[4]** [5](#) [6](#) [7](#) [8](#) [9](#) ... >

The Beginning of *China Eagle Union*

"I solemnly swear to put the interests of the Chinese nation above everything else. I am willing to do everything in my power to make the Chinese nation rise up."

- China Eagle Union Pledge

In April of 2000, Wan Tao joined sina.com's Naval and Merchant Ships Forum with the online name of *China Eagle* in response to a posting by a person named Bailing who called for the establishment of a *China Eagle* club. Between the 19th and 21st of May, he made postings about the delay tactics used by advocates of Taiwanese independence and organized the "Anti-Taiwanese Movement of *China Eagle Union*."⁶⁶ In September, he participated in China's first network security hobbyist conference at the Dragon Spring Hotel in Beijing and gave a speech called "Building Hacker Culture with Chinese Characteristics," that was said to have defined the goals and direction of the Chinese hacker culture. The *Chinawill* web site was redesigned in October of 2000, and the members of the *China Eagle Union* finally had "a home online."⁶⁷ In December, Wan Tao attended the "Network Era Patriotism Discussion" held in Nanjing.⁶⁸

⁶⁶ Unknown, No Title, *China Eagle*, as downloaded on 9 Aug 2005 from <http://bbs.chinaeagle.org/archive/index.php/t-98075.html>

⁶⁷ Unknown, No Title, *China Eagle*, as downloaded on 9 Aug 2005 from <http://bbs.chinaeagle.org/archive/index.php/t-98075.html>

⁶⁸ "The Ever-Changing Red Hacker Sharp Winner," Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, 13 Sep 2005, as downloaded on 17 Oct 2005 from <http://forum.gd.sina.com.cn/cgi-bin/viewone.cgi?gid=51&fid=1359&itemid=8191>



China Eagle defacement of “Taiwan Independence Party” web site

Captioning on the defaced web site reads:

“Sing the national anthem at the top of our voices so that it surrounds the five continents. Swear to annihilate the forces of Taiwan independence and retrieve Taiwan. Our fervor drives us to the battlefield for our country. And we will die on the battlefield.”

*Chen Shui-bian, class is over!*⁶⁹

China Eagle even composed a theme song for their organization titled *Power of the Night*.⁷⁰

⁶⁹ Unknown, No Title, *China Eagle*, as downloaded on 9 Aug 2005 from <http://bbs.chinaeagle.org/archive/index.php/t-98075.html>

⁷⁰ LiZi, “Power of the Night,” *China Eagle*, downloaded on 1 Nov 05 from www.chinaeagle.org/ceu2002/html/darkpower0918.htm

黑夜的力量

Power of the Night

词:中国鹰派栗子

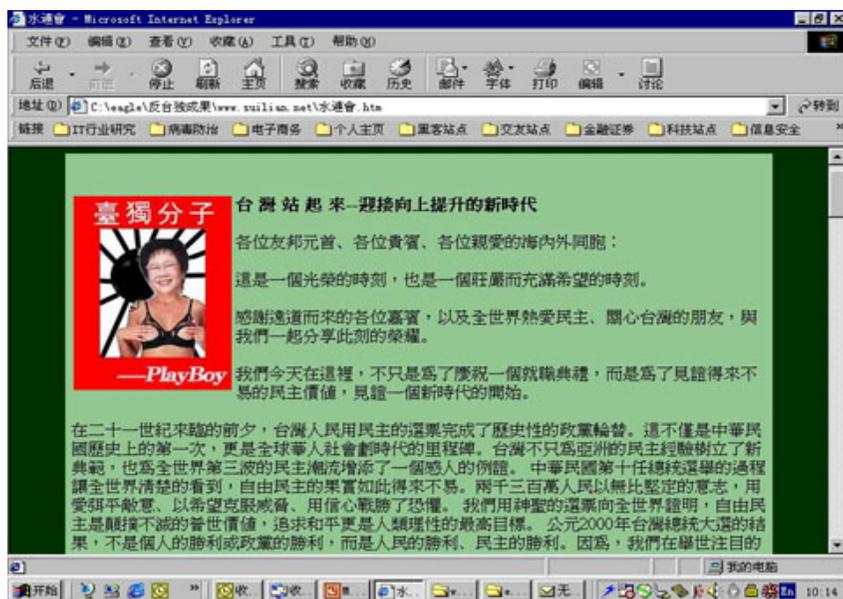
Lyrics: By *China Eagle Union's* LiZi

我们在黑夜里逆风飞行 我们是黑夜里的中国之鹰 我们用黑夜里黑色的眼睛迎接光明的来临 我们在网络里自由飞行我们是网络里的中国之鹰我们用网络里寂寞的黑夜迎接黎明的来临感受黑夜的力量用我黑色的眼睛热血在黑夜里慢慢凝聚希望在黑夜中寻觅我们是中国的鹰派我们要做中国的精英不管敌人的盾牌是多么的坚硬我们要让他知道我们的锐利我们是中国的鹰派我们要做民族的精英所有正义的人们给了我们力量和勇气我们会永远战斗不息

“We are flying against the wind in the night. We are the China Eagles of the night. We use our black night eyes to greet the approaching light. We are flying freely through the net. We are the China Eagles of the net. We use the lonely nighttime of the net to greet the approaching daybreak. Feel the power of the night. Use my black eyes. The hot-blood slowly thickens in the night. Searching for hope in the middle of the night. We are the China Eagles. We want to be the elite of China. It doesn't matter how hard the enemy's shield is, we want him to know our sharpness. We are the China Eagles. We want to be the elite of the nation. All the just people have given us strength and courage. We can fight forever and never rest.”



Wan Tao (万涛) founder and leader of *China Eagle Union* (see footnote 86)



China Eagle forced the shutdown of the “Water Lily Association,” a web site for Taiwanese independence, after placing a defacement showing Taiwanese Vice President Lu’s head pasted on a Play Boy

The Founding of Honker Union of China (2000)

A hacker going by the online name of Lion (true name Lin Yong), at the age of 22, established the *Honker Union of China* in 2000. At that time, he had only a little over one year of Internet experience. He was also responsible for coining the word “Honker” as a term to identify the group to Westerners.⁷¹

⁷¹ “The Ever-Changing Red Hacker Sharp Winner,” Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, 13 Sep 2005, as downloaded on 17 Oct 2005 from <http://forum.gd.sina.com.cn/cgi-bin/viewone.cgi?gid=51&fid=1359&itemid=8191>

Founding of Javaphile (2000)

The group *Javaphile* was established in September 2000 by two Chinese hackers going by the online names of Coolswallow and blhuang (Liang Huang). All members of the group were said to be students of Jiaotong University in Shanghai. The group was later joined by thomasyuan who specialized in Unix programming. Initially the group was merely for Java language enthusiasts as the name implies. This attracted few members, since the Java language had only just been introduced to the country. Coolswallow joined the Red Hacker Alliance following the 2001 collision between the US reconnaissance aircraft and the PRC fighter. Coolswallow and thomasyuan would later initiate a program to reorganize the group into a hacker web site.⁷² Some notoriety was gained by the group in 2002 for the defacement of *Lite-On*, a Taiwanese IT company.⁷³

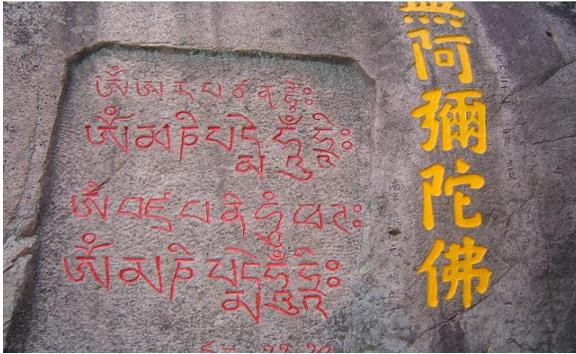
An examination of *Javaphile*, from the introduction of its web site to the defacements of Lite-On, Fox T.V., and others attacks show something slightly different from the normal Red Hacker Alliance cell. The graphics, language, and structure used by the group are not typical when compared to the majority of Chinese hacker web sites. The group's homepage shows a picture of a Buddha head surrounded by tree roots, probably taken at Ayuthaya, Thailand. Coolswallow's personal blog also contains references to Buddha and his/her personal translations and explanation of Tibetan Pali Buddhist engraved incantations.

⁷² Coolswallow (posted by PLL), Bulletin Board Posting, 20 May 03, Jiaotong University web site
http://bbs.sjtu.edu.cn/bbsanc?path=/groups/GROUP_1/IS/D94135E28/D92461686/M.1053442333.A. The *Javaphile* web site picture taken from
<http://www.javaphile.org/>

⁷³ Defacement taken from
http://www.geocities.com/liteonmoemoe/LiteOnHack/liteon_hack.html

酷燕造 || 渗透艺术与佛教极端主义

The Art of Penetrating and Buddhism Extremism



Top graphics are comments from Coolswallow's blog on Buddhism and graphics on bottom are the Pali Buddhist incantations from <http://other.mblogger.cn/coolswallow>



Defacement of Taiwan's Lite-On Corporation



The Japanese Incidents (Cyber Conflict of 2001)

The year 2001 would see a dramatic turn in Chinese attacks on Japanese web sites. Citing incidents involving Mitsubishi, Japan Airlines, Japanese textbooks, the Taiwan Theory, and then Japanese Prime Minister Koizumi's visit to the Yasukuni Shrine, politically motivated attacks increased from 63 events in 2000 to 650 events in the first five months of 2001.⁷⁴ The first wave of attacks by the Red Hacker Alliance occurred in February and included "government web sites, large web sites, and other important sites, along with critical DNS systems."⁷⁵ In approximately 10 days of attacks, mostly Japanese companies were hit including "the well-known telecommunications company NTT, the large printing company in the West of Japan, DNP, a subsidiary of NSK, and Nippon Shortwave Broadcasting." Using their favored method of tagging targeted web sites, Chinese flags were used to alter most of the homepages. The attacks in March transpired due to the textbooks incident and involved both Chinese and Korean hackers.

⁷⁴ Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

⁷⁵ Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

Koreans were said to be responsible for the attacks against “web sites for provincial education, culture, athletics and science and technology.”⁷⁶

Mitsubishi Vehicle Incident

In December 2000, a Mitsubishi vehicle in China was involved in a serious traffic accident due to brake failure. The Chinese victim suffered a critical brain contusion and Mitsubishi’s appearance of not taking action incited discontent among the Chinese.

Japan Airlines Incident

In January 2001, it was reported that Chinese passengers on a Japan Airlines flight were treated rudely. A strong response arose within China once the story was reported by the news media. Japan Airlines issued an apology for its less than satisfactory service and denied that there had been any racial discrimination involved in the incident.

Textbook Incident

In April 2001 the Japanese Ministry of Education and Sciences announced approval of history textbooks containing distortions of historical facts. The textbooks largely removed mention of comfort women, the “Sanko Policy,” and the Nanjing Massacre.

⁷⁶ Ibid.

Japanese War Memorial (Cyber Conflict of 2001)

August of 2001 would again see attacks on Japanese web sites in response to former Prime Minister Junichiro Koizumi's visit to the controversial Yasukuni war memorial. Chinese hackers struck first on 13 August, attacking the server for the Japan Meteorological Agency. Following that, a large number of Japanese government web sites were attacked, such as "the Chemicals Evaluation and Research Institute, the Strategic Materials Research Center, the Defense Systems Research Committee, the Central Convention Service, Inc., the Fire and Disaster Management Agency, the Defense Facilities Administration Agency, the Communications Research Laboratory, and web sites for members of Parliament."⁷⁷ On 14 August, the *Honker Union of China* issued the following statement:

"Japanese Prime Minister Koizumi, in defiance of the protests across Asia and of those seeking peace within Japan, made a public visit to the Yasukuni Shrine, a shrine which symbolizes Japanese militarism. This error by a Japanese leader has been gravely hurtful to the peoples of Asia, especially to the feelings of the people of China, who were harmed most deeply. Together with the issue of the textbooks, this stain is embodied by how the Japanese authorities treat this error without the slightest sense of repentance. Immediately upon learning of this the Honkers Union convened a portion of its members to a meeting to discuss a strategy in response to this sudden incident. The final decision, taken prior to our country having expressed its protest to Japan, was to use our skills to express the solemn and just protest of this youthful Internet generation against the new Japanese government, and its strong dissatisfaction with the leaders of Japan. The Honkers Union, in this emergency action, has replaced the main pages of the following government web sites in Japan. This is in no way inconsistent with our efforts to promote the Honker spirit. The Honkers Union expresses its regret that this matter has occurred, and takes responsibility for the attacks on the web sites listed below. History

⁷⁷ Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

should not be ignored. How can the truth be changed? We win respect by counterattacking. We are in the right!”⁷⁸

One of the prominent members of the organization, Sharp Winner,⁷⁹ was said to have defaced one web site leaving the message “hacked by Sharp Winner.”



Photo SHARPPWINNER



Solemn and just protest of Japanese Prime Minister Koizumi's visit to the Yasukuni Shrine! China Internet Unified Action League

Japanese and Chinese Dispute Over the Diaoyu Islands (Cyber Conflict of 2004)

Japan Times reported that the territorial dispute between China and Japan over the Diaoyu Islands had instigated a massive retaliatory attack by Chinese hackers on Japanese government web sites in August of 2004. The paper said that as many as 1,900 Chinese hackers were responding to an earlier defacement of the China Federation of Defending Diaoyu Islands web site; a Japanese hacker had left the message,

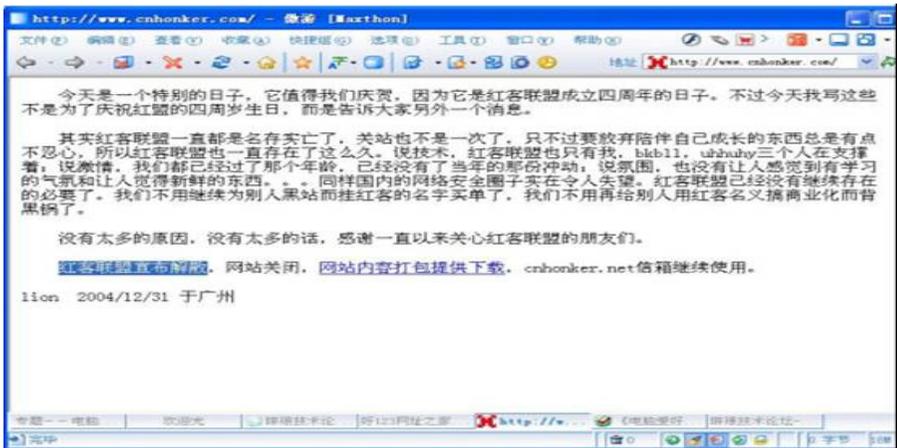
“The Uotsuri Island belongs to Japan.”⁸⁰

⁷⁸ Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

⁷⁹ Photo downloaded from www.redhacker.cn/Photo/ShowPhoto.asp?PhotoID=57 on 17 Oct 2005

The Disbanding of the *Honker Union of China* (2004)

Reading the news at the very end of 2004 seemed to signal the demise of the *Honker Union*. The purported leader of the group, going by the online name of Lion,⁸¹ announced the disbandment of the 80,000-member group. Lion said that there were only a handful of people supporting it and they didn't hold the same passion as in the beginning. The final message from Lion:



The farewell message posted by Lion on 31 Dec 2004

今天是一个特别的日子，它值得我们庆贺，因为它是红客联盟成立四周年的日子。不过今天我写这些不是为了庆祝红盟的四周岁生日，而是告诉大

⁸⁰ Senkaku is the Japanese name for the islands. They are called the Diaoyu (Fishing) Islands by the Chinese. “Organized Chinese hackers hit official Japan sites”, *Japan Times*, 7 Aug 04, as downloaded from <http://www.japantimes.co.jp/cgi-bin/getarticle.pl5?nn20040807a3.htm>

⁸¹ There are many references to Lion 狮 on the web however it is often preceded by an extra Chinese character 酷 that has never translated into English. The character in this case is not taken as its literal meaning of Cruel or Strong but is slang for Cool. The combination therefore would be translated as Cool Lion. There are also numerous web sites with references to 酷狮工作室 “The Cool Lion Work Room”.

家另外一个消息。其实红客联盟一直都是名存实亡了，关站也不是一次了，只不过要放弃陪伴自己成长的东西总是有点不忍心，所以红客联盟也一直存在了这么久。说技术，红客联盟也只有我，bkbll, uhhuhhy 三个人在支撑着；说激情，我们都已经过了那个年龄，已经没有了当年的那份冲劲；说氛围，也没有让人感觉到有学习的气氛和让人觉得新鲜的东西...同样国内的网络安全圈子实在令人失望。红客联盟已经没有继续存在的必要了。我们不用再继续为别人黑站而挂红客的名字买单了，我们不用再给别人用红客名义搞商业化而背黑锅了。没有太多的原因，没有太多的话，感谢一直以来关心红客联盟的朋友们。

“Today is a special day, a day worth celebrating for us, because today is the 4th Anniversary of the establishment of the Honker Union of China. However, today I am not writing this to celebrate the 4th Anniversary birthday of the Honker Union of China, it is to tell everyone about something else. To be truthful, the Honker Union of China has been surviving in name only. This is not the first time the site has been closed, it is just very difficult to let go of something that has been a part of you as you have grown; that is why the Honker Union of China has continued to exist for so long. Talking about the technical side, there have only been three people providing technical support for the Honker Union of China bkbll (online name), uhhuhhy (online name), and myself. Talking about the passion, we had already passed that age and no longer had the impulses of those years. Talking about the atmosphere, we haven't been able to get people into the mood to study or get them to feel freshly about things...Similarly, the country's Internet security situation is very disappointing and there is no reason for the Honker Union of China to exist. We do not need to continue so that other hacker sites can use our name. We do not need to let others once again use the Honker Union of China name for commercialization or to use it as a scapegoat. Not too many reasons and not too much left to say. Thank you to all of the friends who have continuously supported the Honker Union of China.”⁸²

An interview with one of the members of the alliance, giving his name only as K, gave the following account:

⁸² Long San, “Let’s look back on the days of the Red Hacker Alliance,” *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

"I suppose that people would still like to speculate on its remains, but it was a very small Internet group, a matter of only a few people. In fact, it would have been all the same whether it was disbanded or not. It is merely that others seem to be very mystified."

"I have no attachments to the Honker Union of China. That is because after I joined it, it was different than I had imagined, so I stayed for less than a year and then left. Moreover, it was certainly not anything good. The insiders treated it as a joke, while the outsiders felt that it was unfathomable."⁸³

When K was questioned about the 80,000 members and their organization, he responded:

"Truthfully, there were only five or six, and I was of course one of them. Very simply, those five or six people set up a web site and started a forum, and then many others said that they were members once they were registered. Of course, at the time, many young people wanted very much to be called honkers. Since 'honkers' had very many Chinese characteristics, it was very popular. As to the 80,000 number, I do not know how the counting was done for that report."⁸⁴

⁸³ Yan Ni, "China's Hackers Are Wandering on the Fringes of Law and Ethics," *Fuzhou Fujian Daily*, 8 Apr 05, as translated by FBIS reference number CPP20050421000148

⁸⁴ *Ibid*



85

Lin Yong (林勇) “Lion” founder and leader of the *Honker Union of China*

Just as quick as the demise of the *Honker Union of China* was its rebirth; headlines in official Chinese newspapers declared that in less than one month the group had reformed and was once again ready to take the stage. The group that had gone from 80,000 strong down to zero overnight had already attracted 8,000 to 20,000 members.⁸⁶ Yang, a sophomore at the Chengdu University of Electronic Science and Technology and majoring in computer sciences, was said to be the new leader. The group also formed a new supervisory committee to monitor membership activity and revoke membership for any personnel found violating alliance rules such as attacking other web sites. While not mentioned, this rule probably only applies to Chinese web sites within the country. In a statement from the new leader of the *Honker Union of China*, Yang said:

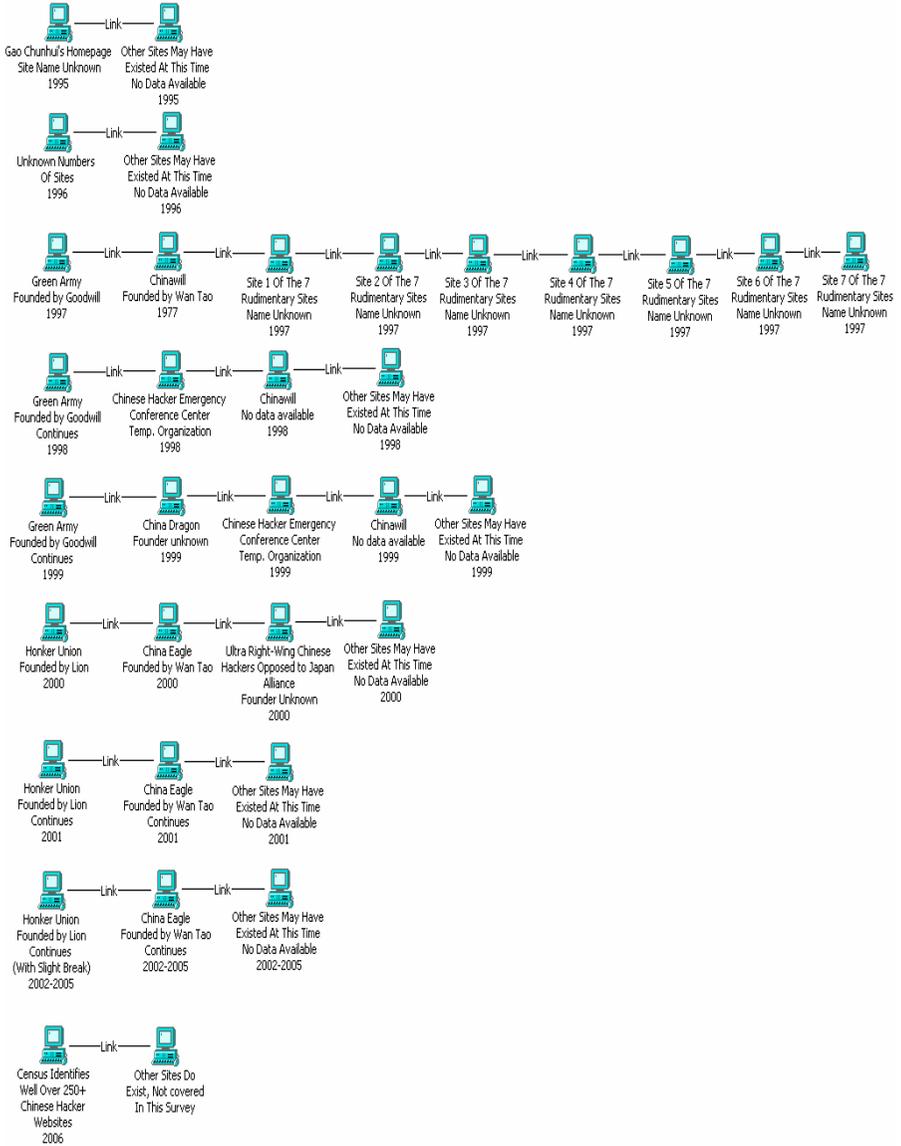
⁸⁵ Photograph of Lin Yong “Lion” taken from his personal Blog at <http://spaces.msn.com/members/n0p/Blog/cns!1p-Ts1tmHYdT66BaM9S-oLSg!173.entry>

⁸⁶ “China’s largest hacker organization regrouped,” *Xinhua*, 24 Apr 05, as downloaded on 16 Nov 05 from http://news.xinhuanet.com/english/2005-04/22/content_2864400.htm and “China’s Anti-Hacking Alliance Regrouped,” *China Daily*, 26 Apr 05, as downloaded on 17 Nov 05 as transcribed by FBIS reference number *CPP20050426000021*

“I can design a computer virus in a few minutes, which can dysfunction the use of mouse and computer, but I will not do this because the mission of a 'Red Hacker' member is to protect the Web sites from being attacked.”⁸⁷

⁸⁷ Ibid

Evolution of the Red Hacker Concept



Based on available data, it is the author's opinion that the Red Hacker Alliance first came into existence in 1998. This was the year that ethnic riots in Jakarta, Indonesia served as a catalyst to bring together existing independent hacker elements and fuse them into a cohesive unit under the banner of nationalism. During this time period, previously independent web sites actively formed connecting links with each other and coordinated attacks against Indonesian government web sites to protest the brutal treatment of ethnic Chinese. Sharp Winner's comments related to the event demonstrate that this is the earliest appearance of the concept and term Red Hacker:

*"A group of patriotic youth active on the net engaged in attacks on Indonesian government web sites, under the alias '**China Redhackers.**' This **patriotic action** received a great deal of reporting and praise in the domestic and overseas media. **The name China Redhackers began here.**"⁸⁸*

Chu Tianbi's historical account claims that it was after the 1999 US bombing of the Chinese Embassy in Yugoslavia that created the alliance and when their first web site appeared:

*"The second day after the bombing of the Chinese embassy, **the first Chinese Red Hacker web site appeared, and a new type of hacker was born – the Red Hacker.**"⁸⁹*

While there is room for argument about the conceptualized birth date of the Red Hacker Alliance, Sharp Winner and Chu Tianbi are in agreement that it predates Lion's founding of the *Honker Union of China* in 2000. Studying Chu Tianbi's words carefully also reveals that the alliance is not made up of one entity/web site, he clearly tells us that this was when "the first Chinese Red Hacker web site appeared," not the only, just the first.

⁸⁸ "The Ever-Changing Red Hacker Sharp Winner." Interview of Sharp Winner by *China Educational Television Satellite Channel (CETV-SD)*, 13 Sep 2005, as downloaded on 17 Oct 2005 from <http://forum.gd.sina.com.cn/cgi-bin/viewone.cgi?gid=51&fid=1359&itemid=8191> Emphasis added by author.

⁸⁹ Chu Tianbi, "Chinese Hacker History/Looking Back on Chinese Hacker History," as downloaded on 9 Aug 2005 from <http://www.blogchina.com/news/source/310.html>

The Years 1995-2006

The years 1995 and 1996 were far too tenuous for the neophyte hackers to be declared anything close to an alliance and there is nothing to suggest that communications and links were taking place with other hackers. Linkage between individual cells must be established in order to satisfy one of our primary preconditions for establishment of the Red Hacker Alliance. The only fixed web site we are told about during this time is Gao Chunhui's homepage that was dedicated to cracking software code. It is also difficult to cast them ideologically as an alliance in these formative years. Individuals from 1995 to 1996 likely held the same nationalistic views as current members but those views cannot be applied to a shared group mentality. The thinking was still "I" am a Chinese hacker not "we" are patriotic Chinese hackers.

Two key elements that disqualify the year 1997 as the birth date of the Red Hacker Alliance are once again the inability to definitively state that there is unifying nationalism and linkage. We are aware Goodwill has founded the Green Army and that there are at least seven other rudimentary hacker sites operating but little else is known about the relationship between these groups. Wan Tao has also registered the site *Chinawill* under the name "Voice of the Dragon." At this point in their history, there has not been that one galvanizing event that would spark their sense of "National Humiliation" and transform them into a collective organization.

By 1998 all the elements that define the current organization are present and functioning. The Jakarta riots have produced unity of spirit, which embodies the Red Hacker Alliance and the "Chinese Hacker Emergency Conference Center" was used as a conduit for communications. The emergency conference center provides us with further proof that additional hacker web sites existed at this time, as it would have been unnecessary to establish it for internal communications among its members. Therefore, we can only presume that the purpose of its construction was for external coordination with outside elements; perhaps the seven rudimentary sites that had been set up in 1997.

From 1999 to 2005, we see an expansion of the Red Hacker Alliance with the addition of the *Honker Union of China*, the reinvention of *Chinawill*

to *China Eagle*, *Javaphile*, and the *Ultra Right-Wing Chinese Hackers Opposed to Japan Alliance*. Not only are more names added to the roster but the frequency of attacks increases along with the publicity that the group attracts. It is highly likely that the actual number of Chinese hacker sites enlarges well beyond what is reported in the open press during this seven-year period. This is practically certain, given that by the middle of 2005 over 250 web sites were linked directly to the Red Hacker Alliance. What is also likely is that the Chinese hackers themselves are somewhat unaware of the extent and numbers of web sites making up the alliance. No information to date suggests that there has ever been a census performed by the Red Hacker Alliance on the composition of their group.

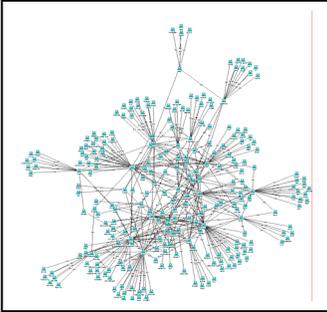
Hopefully, the arguments presented here will convince readers that this is the evolution of a movement and an organization, that there is merit in understanding the intrinsic nature of the body. Just as the moral contained in the ancient saga of the Blind Men and the Elephant, in which each man touches a different part of his body and comes away with a different view of the character of an elephant, we must look at the whole of a thing to fully understand it.

The following chapter will describe where they are today and identify who makes up the present organization. It will also refute the impression left by Lion and K that the group was dying out and only a few members remained.

Chapter Two

Chinese Hackers Present Day

当今的中国黑客



Linking Chart Depicting the
220+ Sites Making Up the
Red Hacker Alliance

The author's impetus for trying to locate the Red Hacker Alliance oddly enough came from the headlines announcing its disbandment. It was impossible to believe that this large organization, with such an extensive history, could simply disappear overnight. The group must still be around; in what shape or form it was impossible to tell but surely it continued to function in some capacity. Initially the idea for this project was far less ambitious. The hope was to find Chinese citizens on the web talking about the alliance or Chinese news articles that had not found their way into Western press. Then, if their ongoing

operations were confirmed, publish an article reporting those findings. What was ultimately uncovered was an extensive, well-organized, online community made up of 250+ Chinese hacker web sites. The amount of publicly available information pertaining to their activities was staggering. For example, the site *China West Hacker Union*⁹⁰ posted the following statistics on 3 January 2006:

⁹⁰ Statistical data taken from *China West Union* on 16 Jan 2006 from <http://www.hx99.net/bbs/>

本站现招核心人员 (2006-1-3 14:37:33)

欢迎您访问华西黑客联盟, 您还没有 [注册] 或 [登录]		共有 5518 位会员	新进来宾 [xszy]
用户名:	<input type="text"/>	今日发帖: 16 篇	主题总数: 2659 篇
用户密码:	<input type="password"/>	昨日发帖: 8 篇	帖子总数: 7461 篇
	<input type="button" value="不保存"/> <input type="button" value="登录"/>	最高日发帖: 117 篇, 发生时间: 2005-9-1 23:48:25	
查看新贴 ◆ 热门话题 ◆ 发帖排行 ◆ 用户列表			

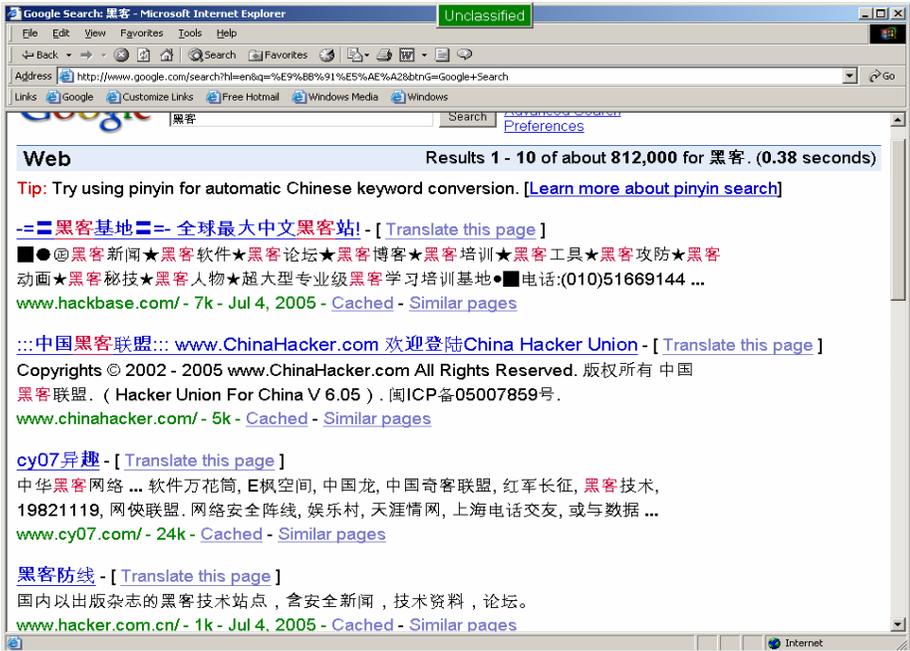
The site had 2,659 main topics and 7,461 postings referencing those subjects. Moreover, this was a fairly average number of documents for a Chinese hacker web site; some sites such as *KKER* had well over 20,000.

Methodology

A substantial amount of time will be spent explaining the methodology behind this research for several reasons; first, to give the reader greater confidence in who is providing the information; second, to better understand the organizational structure of the network; and finally, to identify the demographics of the group.

Online research in the Chinese vernacular is conducted exactly as it is in English, using keyword search strings to refine the search from the generic to the specific. One of the difficulties in developing Chinese keyword search strings is the newness of some computer terminology being introduced into the vocabulary. The first word needed was of course hacker. As discussed earlier, the Chinese use a combination of the two characters 黑 and 客 to make up a transliteration of the English word hacker; with the character 黑 meaning dark or black and the character 客 meaning visitor or guest. When

the word 黑客 was placed in a normal Google search it returned the following results:⁹¹



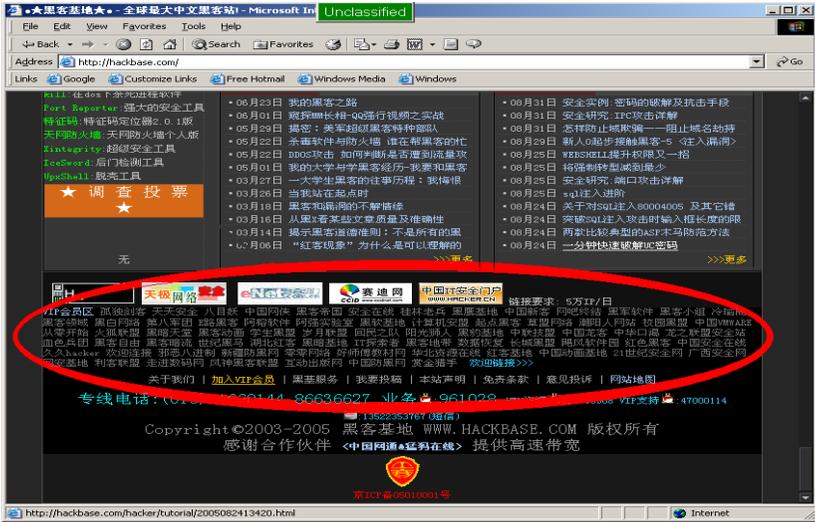
A translation of the Google summary for *Hackbase* (the first site listed in the search) contained topics on hacker: news, software, forum, blogs, training, tools, and attack/defense. It was not a security web site or an information and news outlet. *Hackbase* was almost exclusively devoted to teaching its members how to hack into other people's systems. Furthermore, the *Hackbase* web site claimed to have a membership of over 8,000 people and belonged to an even larger coalition called the Red Hacker Alliance.

⁹¹ A comparison was done between Google and the Chinese search engine Baidu to determine which one worked best for this subject. Google consistently returned more hits than Baidu. The sorting was roughly equivalent. Baidu did however return newer results before Google.



Hackbase Web site

This initial discovery of *Hackbase* was somewhat confusing. The press had never mentioned a group called *Hackbase* or the Red Hacker Alliance. Looking up the domain information for the site confirmed that the server was located inside the People’s Republic of China but that was all. The key to unlocking the Red Hacker Alliance came in the form of links to other web sites. While associations with other sites are not unusual, what was out of the ordinary was that these links, almost without exception, went to other Chinese hacker web sites. Materials found on each of these varied sites showed that *Hackbase* and all of the other associated links did in fact comprise the Red Hacker Alliance. And so began the process of mapping the net:



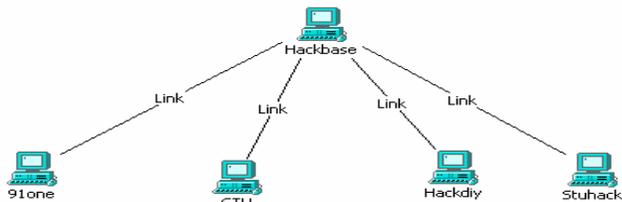
Red ellipse shows links to other Chinese hacker web sites

EXAMPLE: *Hackbase*

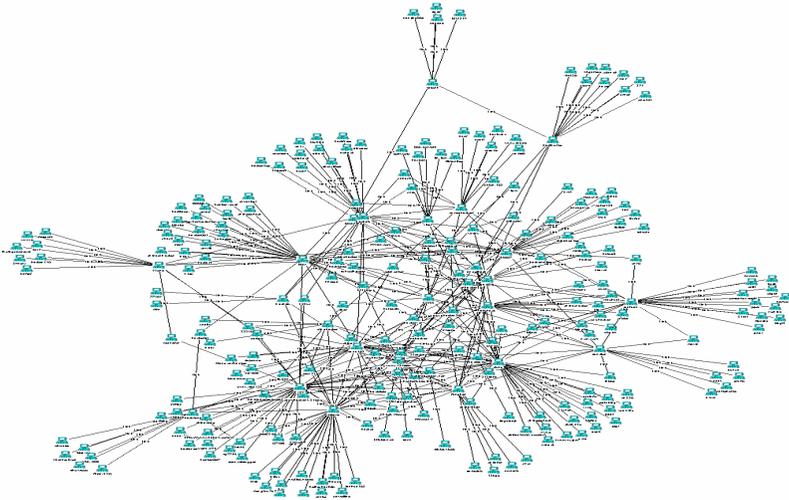
The first step was to use a computer icon to symbolize the web site and name it as our starting point *Hackbase*:



Next we find that *Hackbase* has links (those depicted inside the red ellipse) going out to sites named *91one*, *CTU*, *Hackdiy*, and *Stuhack*...etc. Lines are then drawn showing the connections between *Hackbase* and these outstations:



This process is then repeated for all of the links going out from *91one*, *CTU*, *Hackdiy*, and *Stuhack*. The process is continued for all sites in the study, producing the diagram seen at the beginning of this chapter and below:



This is by no means the entire extent of the network. The alliance is far too large for one study to cover and the landscape is constantly changing as some sites drop off and new ones are added. Fringe elements such as Chinese cyber punks, who are also involved in the hacker community, have not been included. A certain amount of Darwinism is at work inside the alliance, with the higher profile and more innovative sites surviving, while those less able to attract recruits are consigned to the dustbin. Some have also been shutdown for not registering in accordance with the new People's Republic of China state law requiring all sites to record their domain.⁹² Other sites such as *Xhacker* were at least temporarily terminated as of 17 October 2005 for not paying their domain fees.⁹³ We may therefore guess that the site

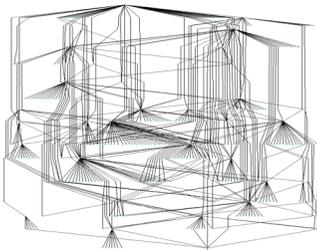
⁹² <http://uquq.1m.cn/> was shutdown due to noncompliance and <http://www.honker.co.sr/> contained a message saying that their site had been shutdown for failure to record their site

⁹³ Message posted on <http://xhacker.cn/> stated that the site was temporarily taken off line for not paying its fees and that the site needed to make reparations before being restarted

called *Honker Union of China* fell prey to this Darwinist effect inside the larger collective. This does not show a weakness in the alliance or signal its demise, it in fact demonstrates evolutionary strength. The better-organized and more flexible groups survive while the weaker are weeded out.

At the time this survey began, there were 253 sites chosen for the study. They were selected due to their placement within the hierarchy of the net, moving from the larger sites down through the smaller sites with fewer subordinate nodes. As an example, a member of the alliance, the *China Black Hawks Union*, has 39 nodes and one of its links connects to *Hack58* that has 16 downlink nodes of its own. One of *Hack58*'s links is *Hackhome* that has nine downlinks. Further linkage was discontinued at this point not for lack of additional connections but in order to keep the scope of the study to a manageable scale. While the process does show us an association between groups, it does not tell us anything about the nature of the relationships between those connections.

Net Hierarchy



Experimental Net Hierarchy Configuration

Discussing network hierarchy is difficult at best and involves speculation on relationships that have not been defined by any known source. Preliminary evidence suggests the network operates on a peer-to-peer basis, without a centralized control mechanism. Experiments with various configurations of the net were unsuccessful in providing a clear-cut top-down structure. Searching through the individual web sites failed to turn up documentation showing a definitive command and control group. There were however hints that a rudimentary

one might exist, or a least a deference to the older and larger organizations. These clues came from messages passed between the sites and in training conducted by the better-established organizations for their smaller downlinks. Despite these hints, all indications are that individual sites are maintained and run by separate entities and the aggregate is best defined as a peer-to-peer network.

The actions and interactions of the Red Hacker Alliance, as described in the previous chapter, support this organizational construct. Individual groups work in coordination with one another, but they do not act in response to orders from centralized leadership. During times of political conflict, when the alliance wanted to act in concert, they established the Chinese Emergency Conference Centers. But this was a cooperative and temporary collaboration. The individual sites should be viewed as independent cells within the larger organization. However, independence should not be confused with an absence of interaction. The various cells are in contact with one another and pass messages back and forth on a regular basis.

The Numbers Game

The number of people participating in these organizations is another subject that requires conjecture. This study provides only a very rough range of the numbers involved and should not in any way be construed as hard data. Of the 253 sites that were monitored, 90 were found to keep and post online records of the number of people registered with their organization. For example, below we see the number of members claimed by *China Black Hawk Union* circled in red on 14 May 2005:⁹⁴

共有 14358 位会员	新近来宾 [15y 帖子]
今日发帖: 79 篇	主题总数: 4235 篇
昨日发帖: 124 篇	帖子总数: 21568 篇
最高日发帖: 299 篇, 发生时间: 2005-5-14 23:55:09	

The number of members claimed by *China Black Hawk Union*

One of the mid-sized groups in the Red Hacker Alliance, the 14,358-member assertion should be examined closely. *China Black Hawk Union* leadership does not mention if these members are currently active or if a portion (maybe a large portion) simply registered and have minimal or no involvement in the group activities. Revisiting the site on 1 September 2005 showed the membership increasing to well over 17,000:

⁹⁴ Downloaded from *China Black Hawk Union* web site on 14 May 2005 from <http://www.cbhu.net/dvbbs/>

共有 17557 位会员		新近来宾 【東風破人】	
今日发帖: 12 篇		主题总数: 11 篇	
昨日发帖: 0 篇		帖子总数: 12 篇	
最高日发帖: 12 篇, 发生时间: 2005-9-1 23:05:01			

The number of members claimed by *China Black Hawk Union* on 1 Sep 2005

Visiting each of the 90 sites that kept statistics and then adding up the total number of registered members showed a total of 1,197,769 participants. This presented an extremely large number, one that called into question the credibility of the data. In January of 2006, China Internet Network Information Center released a report that gave the number of Chinese citizens accessing the Internet at 111 million.⁹⁵ That would mean that 1% of their online community was made-up of hackers. Fortunately, the web sites had another online tool that provided a better understanding of the actual number of active members. This counter (shown below) gives the current number of people active on the site at a given time. If another person were to log on during this period the counter would move up to 643 and if one of the members logged off the counter would move down. On 1 May 2005, the site *ICEHACK* furnished their online numbers as 642 and an all time high of online participants as 1,262. Their total claimed membership was 42,969:

■ 联盟论坛



冰点极限论坛

WWW.ICEHACK.COM

■ 在线用户 **642** 人在线 | 62 位会员(0 隐身), 580 位游客 | 最高纪录是 1262 于 2005-5-1.

⁹⁵ “China has 111 million Internet users,” *China View*, 17 Jan 06, downloaded on 17 Jan 06 from http://news.xinhuanet.com/english/2006-01/17/content_4066612.htm

By monitoring slightly more than 10% of the sites, at four different times throughout the day, over a one week period, it was determined that on average a site had approximately 2% of its stated membership visiting the site. The monitoring example below shows the numbers given on 11 October 2005 at approximately 11:00 pm in China. The time approximation is based off of survey start-time and the amount of time needed for the site to load (web sites in China are notoriously slow), to record the data from the selected site and move to the next site for collection. Note that the numbers recorded for this date and time were 1.6%, slightly lower than the week's norm of 2%. To maintain a fair representation of the organization as a whole, sites were selected for monitoring from three categories, those that posted high, medium, and low memberships.

Survey of 11 Oct 2005
11:00 pm
(Local time in China)

Registered Members	Number of Members Online	Site
6324	909	<i>Supcode</i>
61107	30	<i>Patching</i>
6362	45	<i>Mmbest</i>
42969	998	<i>ICEHACK</i>
14871	41	<i>Chinesehackers</i>
10000	21	<i>Cycycy</i>
50119	957	<i>Cnsafer</i>
342	3	<i>Chinaa</i>
858	2	<i>Anquanwu</i>
4398	60	<i>7747</i>
Total: 197,349	Total: 3066	Avg: 1.6%

Does this mean that we discount 98% of the claims as exaggerations? No, it would be highly unreasonable to expect every member of the organization to be visiting any given site at the same time. Furthermore, the 2% that were noted at 11:00pm would certainly be a different 2% depending on the time monitored. This does however give us a reasonable number to use as our minimum. The range therefore would be from a minimum of 24,000 to a maximum of around 1.2 million. Even at the minimum end of the scale, this

is a large group capable of organizing a variety of activities damaging to governmental and civilian organizations around the globe. It is probable that during times of political strife, these numbers rise dramatically higher and move closer to the upper ranges. Keep in mind that the range of 24,000 to 1.2 million only includes the sites that kept statistics and that the survey is limited in scope. Only 90 out of the 250 sites provided data on online members. This would obviously make both the minimum and maximum figures substantially higher; perhaps even double the range provided.

The alliance is young, it is dynamic, and the numbers it can rally against a problem on any given occasion are enormous. Given the right set of political circumstances, these numbers could swell to over one million. Even though the quality of participants may be highly suspect, the central core of 24,000 regulars should be able to direct them with excellent results.

In discussing more speculative numbers we can extend our minimum by taking the average time spent on the Internet by an individual and extend that over a conservative timeline. If we take the average time spent online by a Chinese user of approximately two and half hours per day, estimate they may use one hour of that on the site where they are a member and the rest for surfing, news, virtual gaming...etc, the hacker web site would change over a new two percent of users eight times in the same number of hours.⁹⁶ Eight hours is used as the normal amount of time a person would have in a day after work and sleep. Using the rotating population and doubling it for the lack online statistics of 160 sites and we could be looking at a floating population of some 380,000 hackers that maintain some sort of consistent contact with the organization. Given the difficulty of determining exact numbers, this is very much inline with Taiwanese estimates of 300,000 plus mainland hackers.⁹⁷

⁹⁶ Natalie Pace, "China Surpasses US In Internet Use," *Forbes.com*, 31 Mar 06, downloaded from http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html?partner=yahootix

⁹⁷ "Taiwan: Hacker Working for PRC Firm Arrested," *Taipei Times*, 26 Jun 02, as downloaded from FBIS reference number CPP20020626000139

Demographics

As expected, members in these organizations are relatively young people of the tech-era. The age range for the site *CYCYCY* is said to be between 20 and 45 years of age, with a large number of high school graduates, and income higher than average. This was according to a promotion for demographics posted on the site.⁹⁸ Gao Jianfei, a member of the *China Black Hawk Union* gives the average age of their membership at 19.⁹⁹ *China Eagle Union's* average age is from 20 to 27, with members as young as 12 years old. The majority are students all the way from primary school through college, with some even holding doctoral degrees. *China Eagles'* technical staff is somewhat older; the age range is from 30 to 50.¹⁰⁰ Bkbl1, one of the founding members of *Honker Union of China*, said that the average age for members of their organization was not 23 as reported by the media, but was even younger and 65% of the registered members were university students.¹⁰¹ The advertising of demographics also raises the question of numbers inflation to attract sponsors. It would be reasonable to suggest there are perhaps some exaggerations in this area to see a greater share of online advertising revenue.

Location, Location, Location

The most difficult question to answer is the location of the groups. For this survey, the answer to the question will be the location of the web sites' host servers.¹⁰² Does this mean that the people who manage the sites or

⁹⁸ Demographics promotion posted on the web site *CYCYCY* in order to attract advertisers to its site, downloaded from <http://www.cycycy.net/ads.html> on 5 Oct 2005

⁹⁹ "The Three Major Hackers' Organizations in the Hinterland", *Hong Kong Ping Pao*, 5 May 2001, as translated by FBIS reference number CPP20010505000034

¹⁰⁰ Unknown, No Title, *China Eagle*, as downloaded on 9 Aug 2005 from <http://bbs.chinaeagle.org/archive/index.php/t-98075.html>

¹⁰¹ Long San, "Let's look back on the days of the Red Hacker Alliance," *Juntuan*, 24 Oct 2005, as downloaded on 17 Nov 2005 from <http://www.juntuan.cn/user1/2334/archives/2005/9612.shtml>

¹⁰² Web hosting is a service that provides individuals, organizations and users with online systems for storing information, images, video, or any content accessible via the Web. Web hosts are companies that provide space on a server they own for use by their clients as well as providing Internet connectivity, typically in a data center. Web hosts can also provide data center space and connectivity to the Internet for servers

those that are members of the Red Hacker Alliance physically live in the same location as the host servers? No, the host server's location does not in any way make that connection. It is quite possible that these individuals live in completely different geographical areas. However, this is where they live on the net.

It is also vital to establish that these groups are operating inside of China and not some other country. Just because the web sites use Chinese characters does not necessarily mean they are from the People's Republic of China. They could well be in some other nation that uses Chinese characters such as Taiwan or Singapore. For that matter, they could be native speakers of Chinese in countries where the native language is other than Chinese.

There is another reason that location is important to establish and that is to take away some of the automatic skepticism that accompanies reports of hacker attacks originating from China. The argument raised by skeptics is usually something to the effect that, "just because the IP address originated in China doesn't mean that they aren't coming from somewhere else." This argument is absolutely valid. People or groups outside of China could easily be using unsecured Chinese servers as proxies to mount attacks in other countries. This report will not take away from that argument but perhaps it can change the tone. Hopefully this research will demonstrate that attacks may very well be coming from China. No one would suggest that the Chinese instantly be dubbed the perpetrators but by the same token they should not be given a free pass either. Neither is anyone implying that just because there are Chinese hacker groups using internal country servers that these groups are foolish enough to use these addresses to launch attacks. The only thing that is intended is to let the rest of the facts fall into place before we pass judgment either for or against the attacks being domestically grown.

Domain Information

To uncover server location a standard domain information pull was requested using the initial URL. To do this, the URL is first converted into an equivalent numerical address such as the one for www.hackbase.com or

they do not own to be located in their data center. Definition provided by Wikipedia http://en.wikipedia.org/wiki/Web_hosting

218.30.100.110.¹⁰³ The converted address is then placed in a domain information request and it returns information on the Internet Provider (IP) that the site is residing on including physical location of that server.¹⁰⁴

Example: Domain Information Return

Domain Information for *Hackback*

218.30.100.110
Blacklist Status: Listed - Cached Today (details)
Cached Whois: Cached today
Whois History: 9 records stored
Oldest: 2004-05-17
Newest: 2005-09-07
Record Type: IP Address
IP Location: China - Beijing - China - Chinanet Idc Center
Reverse IP: Web server hosts 39 web sites (reverse ip tool requires free login)
% Whois data copyright terms
<http://www.apnic.net/db/dbcopyright.html>
inetnum: **218.30.127.96.0 - 218.30.127.255**
netname: CHINANET-IDC-BJ
descr: CHINANET IDC center
descr: China Telecom
descr: Beijing 100088
country: CN
mnt-by: MAINT-CHINANET
mnt-lower: MAINT-CHINATELECOM-BJ
source: APNIC
address: Beijing Telecom
address: No. 107 XiDan Beidajie, Xicheng District
Beijing
phone: **+86-010-58503461**
fax-no: **+86-010-58503054**

Spamhaus Report

218.30.100.0/24 is listed on the Spamhaus Block List (SBL)

30-Aug-2005 07:54 GMT | SR04

Dirty block

Hosting multiple spam sites.

218.30.100.111/32
SBL31171 godgoogle.cn / Leo Hosting

218.30.100.27/32
SBL30908 www.bulletproof-hosting.com

218.30.100.162/32
SBL30672 guci.com.cn

218.30.100.109/32
SBL30317 scanworld.com.cn

218.30.100.101/32
SBL14574 bullet-proof-host.com

The return for *Hackbase* (above) showed that the site was under a blacklist status, indicating some sort of spamming¹⁰⁵ activity for the site or sites listed under its address block that extends from 218.30.96.0 - 218.30.127.255. The blacklist report on the right-hand side indicates that Spamhaus Project¹⁰⁶ has identified several other sites within *Hackbase*'s address range of 218.30.96.0 - 218.30.127.255 as being involved in spamming

¹⁰³ There are numerous online sites that supply automatic numerical conversions for URLs

¹⁰⁴ Domain information provided by DNSSTUFF
<http://www.whois.sc/218.30.100.110>

operations.¹⁰⁷ The domain information further tells us that the IP, Chinanet Idc Center, is located in Beijing and is a part of China Telecom. We are also given phone and fax contact numbers associated with the IP address.

Compiling the information for all of the sites revealed interesting statistics. Red Hacker Alliance servers are located in: three major municipalities; seventeen provinces; one autonomous region; and the Special Administrative Region of Hong Kong. Being one of China's most advanced cities in the Information and Technology industry; it is not surprising that the largest concentration of servers hosting hacker web sites, a total of sixty-one, would be in Shanghai. Around 25% of all hacker servers for this study were located there. Combined with Beijing, which housed fifty-three sites, these two cities alone contain 45% of all the hacker sites studied.

Over 60% of the sites resided in block addresses that were actively blacklisted or had been previously listed. This does not mean that the sites themselves were singled out and accused but that the address range they resided within had been placed there. This could simply mean that the block owner was unaware of the activity occurring on the sites or was made aware and did nothing to stop the activity. Think of a block owner as the landlord of a large complex of apartments and the block range as the address of the complex but not the individual apartments inside it. Just as each individual apartment within a complex will have its own distinct address, an individual web site will have an individual number within its range. The block owner rents out these individual numbers like apartments but is not necessarily familiar with the renter/tenant of the address. He also may or may not be

¹⁰⁵Spam by e-mail is a type of spam that involves sending identical (or nearly identical) messages to thousands (or millions) of recipients. Perpetrators of such spam ("spammers") often harvest addresses of prospective recipients from Usenet postings or from web pages, obtain them from databases, or simply guess them by using common names and domains. Definition provided by Wikipedia
http://en.wikipedia.org/wiki/E-mail_spam

¹⁰⁶ The Spamhaus Project is a largely volunteer effort founded by Steve Linford in 1998 that aims to track e-mail spammers and spam-related activity. It is named for the anti-spam jargon term *spamhaus*, a pseudo-German expression for an ISP or other firm which willingly provides service to spammers. Definition provided by Wikipedia <http://en.wikipedia.org/wiki/Spamhaus>

¹⁰⁷ Blacklist information provided by Spamhaus
<http://www.spamhaus.org/SBL/sbl.lasso?query=SBL31172>

aware of the activities taking place there. When complaints are made to the block owner about his renters, it is up to his own judgment on what action should be taken if any.

It is also interesting to note that these site addresses listed a relatively small number of people as the contacts. For instance, the sixty-one hacker sites operating off of servers in the Shanghai area are allocated to only nine people. Once again, there could be various reasons why this could occur and no connection was found between the owners of the block addresses and the hackers.

Server location also does not define linkage within the group. As an example, the web site *Hackfans* uses a server in the Guangdong area but has a downlink to a site called *Showpop* that is working off of a Beijing server.

Who They Are, What They Are

To provide a better understanding of the web sites and their activities, let's examine a few as examples. Given the size of the Red Hacker Alliance, it will be a very limited number from Shanghai, Beijing, and Sichuan.

The Friendly Download Site

One of the sites directly linked to the Red Hacker Alliance and operating out of the Green Power Bar is the *Friendly Download Site* (<http://www.xxijj.com>). It claims to have 69,951 downloads available, many of which are Trojan horses and attack tools. The *Friendly Download Site* also has the newest 2005 version of the Gray Pigeon Trojan. This is an updated version of the same Gray Pigeon Trojan that was discussed in Chapter One and used during the 1999 Cyber Conflict with Taiwan. Its design is based on the Glacier Trojan and is an indigenously produced product.

Knowing the types of malicious programs developed and used by certain hacker groups can assist us in pinpointing the source of attacks. Just as traditional criminals develop modus operandi, so do cyber criminals. They will favor one set of techniques and tools over others and just as in traditional law enforcement, these techniques can be used to identify the individuals or groups responsible for the crime. While not foolproof, profiling of groups

such as the Red Hacker Alliance may offer additional clues as to their involvement in cases of fraud or theft of sensitive materials.

In June of 2005, the National Infrastructure Security Co-ordination Centre (NISCC)¹⁰⁸ released a report detailing Trojan e-mail attacks targeting United Kingdom “government and companies.” The briefing noted that the attacks were coming from the “Far-East” and Trojans used in the attack included Gray Pigeon and Nethief.¹⁰⁹ Chinese hackers have taken credit for the creation of both of these two Trojan programs. Mark Sunner, the Chief Technical Officer for MessageLabs,¹¹⁰ said:

"MessageLabs can confirm that the source of the IP addresses originates in China. But there's a much bigger and broader problem here. The 'China' word is not meaningless but it doesn't mean they are the perpetrators."¹¹¹

¹⁰⁸United Kingdom Government: “NISCC was set up in 1999 and is an inter-departmental centre drawing on contributions from across government. Defense, Central Government Policy, Trade, the Intelligence Agencies and Law Enforcement all contribute expertise and effort.” Downloaded from

<http://www.niscc.gov.uk/niscc/index-en.html>

¹⁰⁹NISCC report released on 16 Jun 05 downloaded on 12 Jan 06 from

<http://www.niscc.gov.uk/niscc/docs/teea.pdf>

¹¹⁰MessageLabs is the world’s leading provider of messaging security and management services to business. Taken from company profile downloaded on 12 Jan 06 from

http://www.messagelabs.com/publishedcontent/publish/about_us_dotcom_en/company_profile/DA_114118.chp.html

¹¹¹Dan Ilett, “Trojans from China attacking UK,” *ZD Net UK*, 30 Jun 05, as downloaded on 12 Jan 06 from

<http://news.zdnet.co.uk/internet/security/0,39020375,39206464,00.htm>



Friendly Download Site: click red square to obtain the 2005 version of Gray

Other experts were also skeptical that the IP addresses alone proved the attacks were coming from China. However, on 23 October 2005, *Hackbase* posted a story about the attacks on the British government and the speculation that the attacks were coming from the Far East. The article was apparently taken from the foreign press and translated into Chinese. The comments in response to the article from members of *Hackbase*, while not conclusive, are very suggestive:

*41444: Awesome, I am very moved!! My thanks to the elder hackers, I hope you all can attack the US!*¹¹²

Real Cow x: I want to express my sincere sympathy to the English government!!! Many thanks to the elder hackers

*Well done!!: The English government has become the target of a Trojan e-mail attack!!!*¹¹³

¹¹² There appears to be a typo in the Chinese for “you all” where the poster wrote 你们 rather than 你们. The two characters have the exact same sound but different tones. The character 们 is a plural marker for pronouns while the poster wrote 们 that normally means a door, gateway, or opening.

¹¹³ Comments taken from the web site *Hackbase* as downloaded on 25 Jan 06 from <http://hackbase.com/News/hacker/2005102314588.html>



Comments Posted on Hackbase Web Site

By applying the hacker profile to this case, the evidence points very strongly to Chinese fingerprints present at the crime scene. The attack perpetrated against the UK government had: IP addresses that originated from China; used a backdoor to gain entrance to the computers, one of the preferred methods of the Red Hacker Alliance; and used both Gray Pigeon and Nethief, two of their favorite tools. In addition, members within the organization, when reading about the attack, expressed their admiration for the “elder hackers” who they seem to credit for the attack’s success.

New Hacker Alliance

Another site using a Shanghai server, <http://www.hacker-cn.com/> (English name *New Hacker Alliance of China*) maintains a “trophy room” of web site defacements. The practice of maintaining a special location for posting defaced web sites is a common one seen across the alliance. The trophy defacement pictured below was actually hacked by another group in the alliance called the *Novice Hacker Alliance* at www.birdhacker.com.



Defacement of Taiwanese web site *Mediatek* over perceived moves toward independence posted 12 June 2005

NOTE: As some may have noticed, the English for the URL is *birdhacker* and not *Novice Hacker Alliance*. The reason for the change in translation is that the name of the group 菜黑联盟 (found just under the flags below) begins with the character 菜 that actually means vegetable. This character 菜 is often seen in combination with another character 鸟 that does translate to bird but when combined together 菜鸟 means novice or beginner. It would seem from the clue in the English URL (*birdhacker*) that 鸟 (bird) does go with this character and that the full name of the group would probably be 菜鸟黑联盟 or *Novice Hacker Alliance*.

Translation:

www.mediatek.com.tw (address of attacked web site)

“3.20 Referendum on the Taiwanese Independence Movement”

Graphics

Depicted on the Left hand side is the China National flag – the Right hand side is Taiwan’s National flag crossed out with the caption written over it “There is only one China!!”

--- Novice Hacker Alliance ---

We are resolutely opposed to the “Referendum” on Taiwanese Independence. Taiwan is an inseparable part of China, any attempt to separate Taiwan from China, or any vain attempt to block Cross-Strait unification will meet with failure! There is only one China!!!

Hack by oNe's wAr (550669)

As a side note to the story of the defacement, the hacker oNe's wAr, attended a Black Hat conference in Canada four months earlier in February of 2005 and sent back the following message to the organization:

A security report from the Black Hat hacker conference in Canada

“Hello everyone: This is oNes wAr, the reason I am translating this article is not to have you all invade (exploit another system), it is to let you understand the steps to a hacker invasion. Only in this way can we better understand how to defend against hacking... Okay, let's get started ~”¹¹⁴

¹¹⁴Download on 7 Feb 06 from the cache file at ww.lzbiz.com/w,180,1,dllhttp://64.233.179.104/search?q=cache:6lzo95aDdv8J:www.lzbiz.com/w,180,1,dll+%22oNes+wAr%22+%E9%BB%91%E5%AE%A2+&hl=en

The rest of the narrative provided by oNe's wAr is a very lengthy report giving detailed steps on the process for breaking into a system.

Beijing

Student Hacker Union

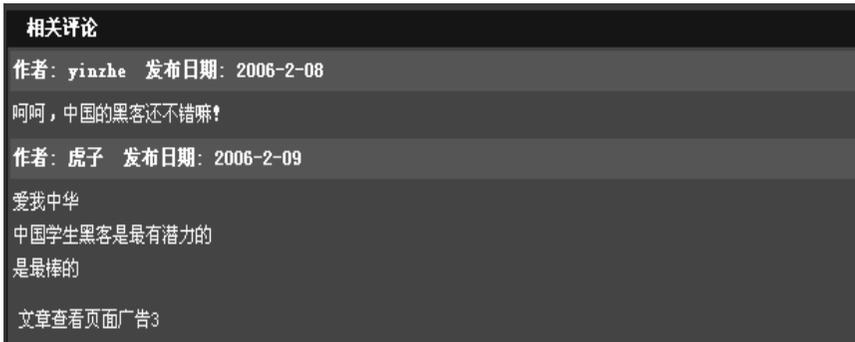
Beijing, with the second largest concentration of Red Alliance cells, maintains a site called *Student Hacker Union*. On 10 February 2006, the *Student Hacker Union* claimed to have 10,298 members and 41 people were online when the site was visited at 2:30 am. The site has 4162 main topics and 14,064 postings underneath these talking points.



Under the heading “Hot Topics,” a story was posted about Chinese hackers breaking into a South Korean bank. According to the article, the bank announced that they had already removed the Luoyi (TROJ_QAZ.A) Trojan/Worm from their system.¹¹⁵ Various reports from computer security companies state that the Luoyi worm sends an e-mail message back to an address (202.106.185.107) in Guangdong, China. The e-mail message that the program sends out contains the IP address of the infected machine. The program uses the sender name nongmin_cn (Translation: Farmer) and is said

¹¹⁵ Sunny Day Boar (online name), “Chinese Hackers Attack Korean Bank,” *Student Hacker Union*, 6 Feb 06, as downloaded on 10 Feb 06 from <http://www.stuhack.com/viewarticle.php?id=4536>

to have originated in China in July of 2000.¹¹⁶ Members of *Student Hacker Union* left the following comments in response to the article:



Yinzhe: Ha Ha, Chinese hackers are good!

*Tiger: Love our China
China's student hackers have the most potential
(They are) the most capable*

Yaqu163

Yaqu163, a web site that originally resided on a Beijing server seems to have switched server location to Wuhan as of 15 February 2006 and reformatted its appearance. When initially discovered in the middle of 2005, *Yaqu163* claimed to have 3966 members and was upgrading to a near-time server. A message on the site bulletin board stated that they were in the process of reorganizing, recruiting new staff, and adding newer internal animation. They were also involved in educational training for the 8th Group

¹¹⁶ Virus alert from Pandasoft as downloaded of 10 Feb 06 from http://www.pandasoftware.com/virus_info/encyclopedia/overview.aspx?lst=det&idvirus=35796

Virus alert from Symantec as downloaded on 10 Feb 06 from <http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.qaz.a.html>

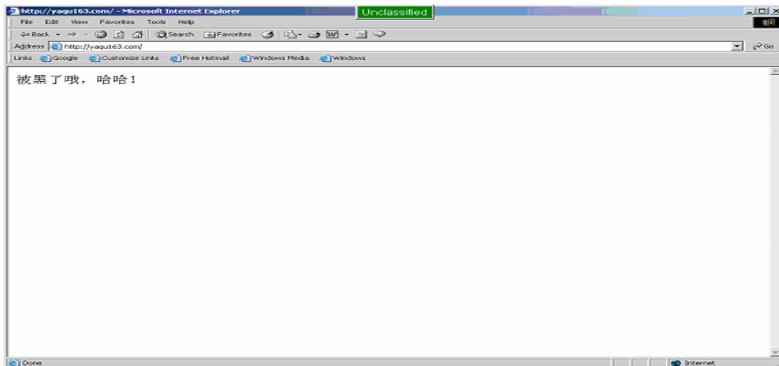
Virus alert from Virus List as downloaded on 10 Feb 06 from <http://viruslist.com/en/viruses/encyclopedia?virusid=23818>

Army, which is another cell in the Red Hacker Alliance and not a military organization.¹¹⁷



Yaqu163 as it originally looked in the middle of 2005

Revisiting the site on 27 July 2005 proved that even the hackers get hacked. The site's portal had been defaced and the following message was left:



Translation: "Hacked, HAHA!"

¹¹⁷ Bulletin board message taken from www.yaqu163.com

Worth noting is that the message is written in Chinese characters. This could mean that Chinese speakers outside of China carried out the attack. Or, given the lack of any political message, perhaps another member of the Red Hacker Alliance could have done it. This could be an internal prank or perhaps even a method of checking on each other's security procedures. Below is the new *Yaqu163* design on 15 February 2006.¹¹⁸



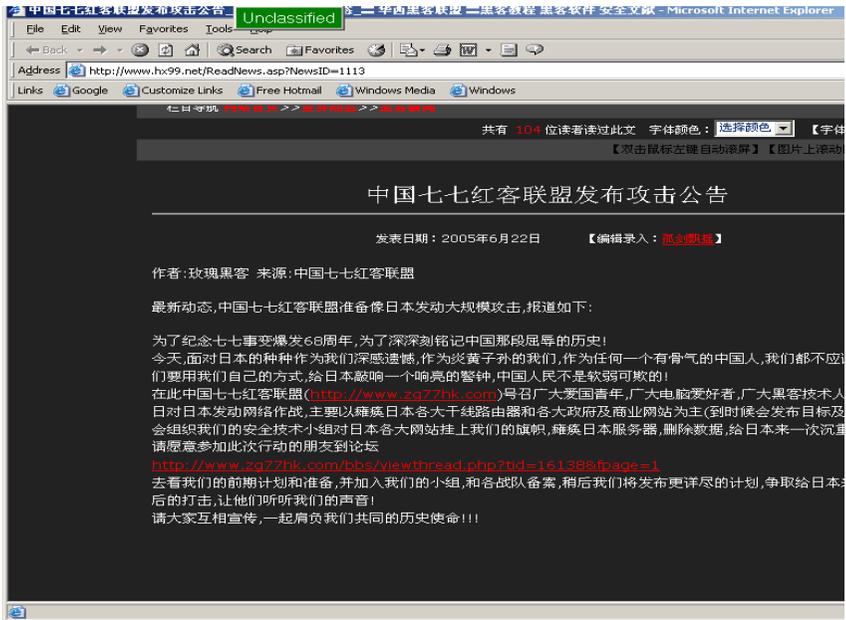
Sichuan

Hx99

One question that is sure to be raised is, “can this type of research produce information that is actionable?” From the history of Chinese hacking we can see that monitoring the postings of Chinese hackers at that time would have given us advance warning that attacks were coming and possibly in what form. Does that still hold true today? Are they still bold enough to announce their intent to launch attacks on the US or other nations? The answer is yes.

While monitoring hacker web sites on 22 June 2005, the site *Hx99* located in Sichuan posted the following message:

¹¹⁸ Web site frontpage found at <http://yaqu.315safe.com/> on 15 Feb 06



It was passing along a request from the hacker web site *Zg77Hk* to recruit people to attack Japan on 7 July 2005. The attack was to mark the anniversary of the Marco Polo Bridge incident (7 July 1937) that started the Sino-Japanese War. The attack would be aimed at main trunk lines, routers, government, and commercial web sites. The Chinese hackers planned on hanging Chinese flags on all of the Japanese web sites, paralyzing Japanese servers, and deleting data. *Zg77Hk* further claimed to have 7,667 members and were putting out the call for all other hacker groups to join them.¹¹⁹

The Chinese translation for the site *Zg77Hk* (中国七七红客网路安全中心)¹²⁰ is *Chinese 77 Red Hacker Internet Security Center*. When the Chinese post dates for important events they will often refer to them by the month and day. As an example, China marks the founding of the People's Liberation Army on August the 1st 1927 and refers to it as 八一 or 81 for

¹¹⁹ Message posted on *Hx99* <http://www.hx99.net/ReadNews.asp?NewsID=1113>

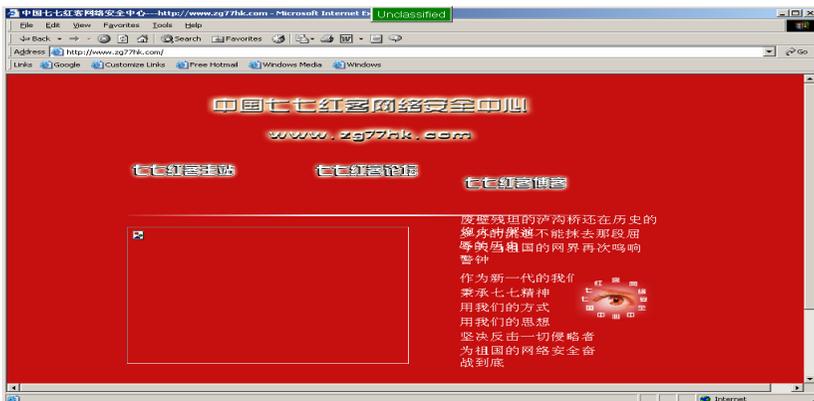
¹²⁰ Taken from the *Chinese 77 Red Hacker Internet Security Center* homepage at <http://www.zg77hk.com/>

August 1st. The People's Liberation Army banner and cap emblems even carry the two characters 8 and 1 to commemorate this historic date.



People's Liberation Army Banner showing the characters for 8 and 1 to the right of the star (August 1st)

This brings us back to the translation for the site that originated the call to attack Japan. Once again it is the *Chinese 77 Red Hacker Internet Security Center*. The 77 (七七) in their title more than likely stands for July 7th and represents the Marco Polo bridge incident that occurred on July 7th 1937.



Chinese 77 Red Hacker Internet Security Center

Clearly this information could have been used to provide advanced warning to the appropriate personnel of an impending computer attack.

Chapter Three Exploits and Money

攻击和钱

The phenomenon of Chinese hacking is made up of four-parts: one part nationalism; one part tech interest; one part financial; and one part fame. When political strife and interest begin to wane, it is money and fame that holds the organizations together. Many Chinese hackers are capitalistic entrepreneurs who not only finance their activities through illegal methods; they also generate income by marketing pop culture. Newspapers are clamoring to interview them, books are being written about them, hacker magazines are being distributed, and movie deals are in the offing. The capability of the Red Hacker Alliance to identify new methods for generating income is seemingly endless. This chapter will endeavor to ascertain the unique Chinese characteristics associated with malicious computer activities and organizational funding.

The Wooden Horse

Since the introduction of Trojan programs into the Chinese hacker community in 1998, they have remained a sentimental favorite for illegally penetrating and controlling other systems. The construction of indigenously produced programs such as Glacier, Grey Pigeon, and Myfip has further ingrained this as the weapon of choice for many Chinese hackers. Several large sites within the Red Hacker Alliance offer hundreds of Trojan programs for sale such as the following two advertisements:

The advertisement is presented in a window-like format. On the left, there is a text block with the following content:
软件名称:最新传奇木马(传染版)
详细说明:
截取得账号信息包括区域,服务器,账号,密码,新增加截取人物名称和等级和装备信息的功能!如果是新建的帐号还能截取到密码保护信息
能自行关闭多种杀毒软件及防火墙。
收信速度极快.特别推荐

On the right side of the advertisement, there is a graphic with the large red Chinese characters '热血' (Hot Blood) and a red seal. Below the graphic, the price is listed as '价格:150元' and there is a blue button labeled '我要购买' (I want to buy).

The Legendary Trojan Horse

软件名称：最新英雄年代木马

详细说明：
 截取得账号信息包括区域，服务器，账号，密码，新增加截取人物名称和等级 和装备信息的功能！如果是新建的帐号还能截取得密码保护信息
 收信速度极快。特别推荐
 能自行关闭多种杀毒软件及防火墙。

最新英雄年代木马



价格：150元

我要购买

The Heroic Era Trojan Horse

These advertisements offer the newest versions of the Legendary Trojan Horse and its cousin the Heroic Era Trojan. Both programs sell for approximately US \$18 and claim to have similar capabilities of retrieving account numbers, server and regional information, passwords, and equipment information and functions. They are also able to shutdown various types of virus protection software and firewalls.¹²¹

The Trojan program presents us with another side of Chinese hacking that we must consider: the ability to apply social engineering skills.¹²² The majority of these programs arrive via e-mail and require the victim to click on an attachment in order to activate and download the executable portion of the program. To do that, the perpetrator must have some knowledge of their target’s habits in order to motivate them into opening the attachment. This is getting more difficult as stories of various scams spread across the Internet and cause the average user to be very cautious when opening anything they do not recognize or request.

Social engineering: a collection of techniques used to manipulate people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery for information gathering or computer system access and in most (but not all) cases the attacker never comes face-to-face with the victim.

¹²¹ Both programs were for sale on the web site <http://www.wghack.com/>

¹²² Definition provided by Wikipedia
[http://en.wikipedia.org/wiki/Social_engineering_\(computer_security\)](http://en.wikipedia.org/wiki/Social_engineering_(computer_security))

Some hackers send out generic e-mails in a shotgun pattern designed to find the largest number of people, while others use a more precise approach to hit specific targets. Whether going after the UK government, as Gray Pigeon and Nethief did in 2005, or specific companies like Boeing using Myfip, the attackers first have to research their target.¹²³ While caution in opening e-mails has increased, our concern over operational and communications security has decreased. Go to most government or business web sites and you can find organizational charts, individual e-mail addresses, upcoming events, department projects and a laundry list of details that a hacker can use to manipulate the recipient. Fake the name of a boss to a subordinate and doctor the e-mail header to look like it came from the company account and someone will open it without a thought – it appears to be trusted correspondence. The following is an example of a faked e-mail that has the Myfip virus attached:

```
From: "hr@boeing.com" <hr@boeing.com>
Subject: Urgent: boeing company date
To: xxx@xxx

boeing company date: plane big \ plane table \.....

please you download boeingdate.txt

Attachment: boeing date.txt.exe
```

Myfip Trojan used to entice Boeing employees to open attachment.

Just as the Trojan programs will certainly be modified to cope with new security software, the methods for researching and deceiving an individual will also become more sophisticated.

¹²³ “Myfip Intellectual Property Theft Worm Analysis,” *lurhq.com*, as downloaded on 11 Oct 06 from <http://www.lurhq.com/myfip.html>. E-mail example also provided by *lurhq.com*.

Korean Game Theft

Capitalizing on the growing trend of selling virtual gaming property for real-time profits, Chinese hackers have taken aim at the online gaming community. From mid 2005 to the early part of 2006, South Korean officials reported that Chinese hackers stole virtual items and entire character accounts from approximately 4,000 South Koreans playing the online game Lineage.¹²⁴ Chinese hackers were accused of creating software with the sole intention of stealing virtual items from the South Korean players.



Screen shot from <http://www.lineage.co.kr/>

Mao Jieming, whose equities firm invested in a Chinese online game site that sells virtual items, had this to say:

"Hacking for virtual items used in online games is quite popular in China as China does not have explicit laws and regulations to protect online virtual assets. A large number of what are termed 'Chinese online game substitute playing companies' usually employ a lot of professional gamers to play for virtual items on foreign

¹²⁴ "Chinese hackers accused of mass theft relating to online game Lineage in South Korea," *InterFax*, 24 Feb 06, as downloaded on 8 May 06 from <http://www.interfax.cn/showfeature.asp?aid=10191&slug=INTERNET-ONLINE%20GAME-NCSOFT-LINEAGE-GEOT>
"Hackers Stole 1 Million IDs for Online Game," *Chosun*, 13 Mar 06, as downloaded on 8 May 06 from <http://english.chosun.com/w21data/html/news/200603/200603130026.html>

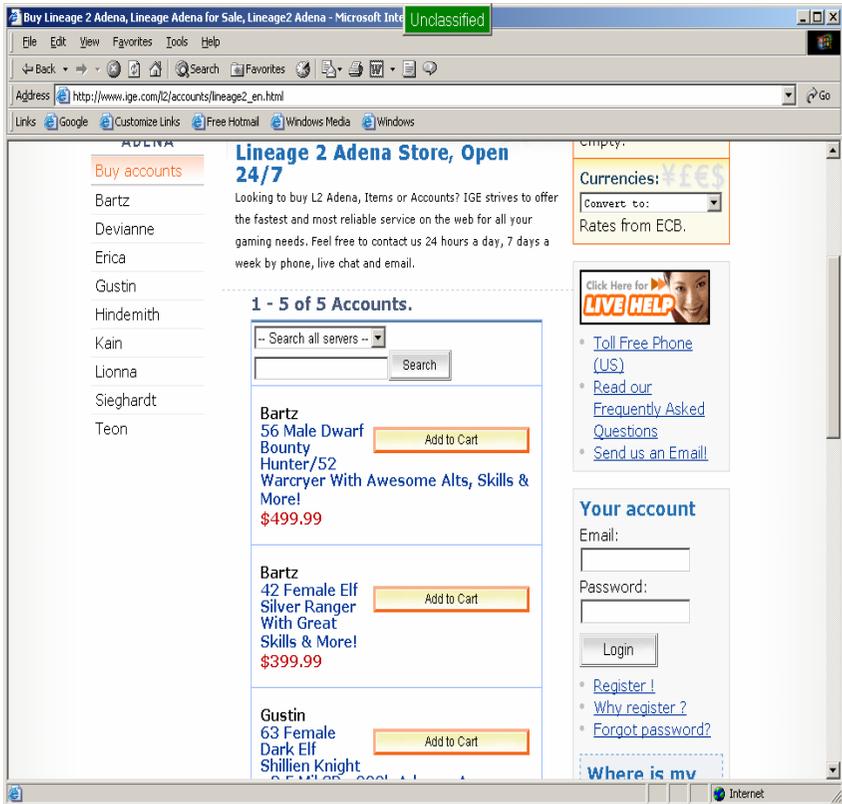
game servers, but it is more efficient and profitable for them to get these virtual items through hacking.”¹²⁵

Mao’s reference to “substitute professional gamers playing for virtual items” is a euphemism for farming; a side industry that has sprung up around the marketing of virtual merchandise. Farming is the online “sweatshop” practice of warehousing large numbers of people to play online games for hours and hours to collect gold that will be sold on *eBay* and other specialty sites.

To understand why someone would pay real money for a virtual object, one needs to understand the nature of online gaming. While there are many different scenarios, most online games involve a fantasy world in which users are given a character that is initially very weak and must be developed in order to survive in the world’s hostile environment. Fighting other opponents, learning magic, acquiring skills, and completing quests will gradually strengthen the character, but this takes time – lots of time. Some online players take years to build up their characters. These online identities require virtual money to buy items such as armor, weapons, and food to enhance their chances for survival. The better the weapon or armor the more expensive it is and, just as in real life, players must save up virtual money in order to afford them. In some cases, it can take months to save enough to purchase rare articles.

For those unwilling to devote the time and effort needed to mature their characters, there are web sites that market ready-made characters, equipment, and virtual money for sale. The web site *ige.com*, one of the largest online retailers of virtual gaming goods, lists the following characters for sale from the game *Lineage II*:

¹²⁵ “Chinese hackers accused of mass theft relating to online game *Lineage* in South Korea,” *InterFax*, 24 Feb 06, as downloaded on 8 May 06, <http://www.interfax.cn/showfeature.asp?aid=10191&slug=INTERNET-ONLINE%20GAME-NCSOFT-LINEAGE-GEOT>



Virtual Characters for sale on ige.com

Visible from this screenshot are two of the five characters for sale, a male dwarf who is a level 52 hunter and a level 42 female elf ranger selling for US \$499.99 and US \$399.99 respectively. The same principle applies for those who don't want to do the tasks required to earn money, *Itemgarden.com* sales "Adena," the virtual currency used in Lineage.¹²⁶

¹²⁶ Adena pricelist obtained from <http://www.itemgarden.com/g/pricelist.jsp>

Type	Price	Add to Cart
Adena 20M	\$24.79	Add to cart
Adena 30M	\$35.29	Add to cart
Adena 40M	\$45.89	Add to cart
Adena 50M	\$55.89	Add to cart
Adena 60M	\$64.79	Add to cart
Adena 80M	\$84.69	Add to cart
Adena 100M	\$102.99	Add to cart
Adena 150M	\$151.49	Add to cart
Adena 200M	\$199.99	Add to cart

Adena Pricelist

As can be seen from the two pricelists, the time and emotional investment in these characters produces real world value. Working online for several months to obtain a particularly expensive weapon, only to find it missing from your character’s arsenal the next day can seem like real world theft.

The Seoul Metropolitan Police certainly treated such a theft as a real crime and attached monetary value to the stolen articles. On 8 July 2006, Seoul’s cyber investigation unit apprehended several men suspected of collaborating with Chinese hackers to launder over US \$150,000 in stolen virtual items and gold. Chinese hackers were able to take advantage of a flaw

in Windows OS to install a keystroke logger¹²⁷ to lift usernames and passwords. According to reports, one member of the cyber gang, Mr. Lee, hired Chinese and ethnic Korean Chinese hackers from Shenyang, China.¹²⁸

eBay Hijacked

The schemes do not always have to be elaborate or even involve a high-degree of technical skill; sometimes it just takes imagination and good reconnaissance. This was demonstrated in 2005, when Chinese hackers began hijacking eBay accounts in Germany. The hackers first looked for accounts that met two specific criteria. First, the account had to have been inactive for an extended period of time in order to minimize the chances that the true owner would notice new activity. Second, the account had to have a satisfaction rating of 100% from other eBay customers who had purchased from them. This rating implies that the person buying or selling an item has always fulfilled their part of the bargain and is an honest broker. Once a suitable account was identified, the Chinese hackers then used a dictionary attack to obtain the password of the authentic account holder.¹²⁹ Next, they simply changed the account information along with the e-mail address so that all inquiries would be sent directly to them. Expensive items were posted at a

¹²⁷ Writing software applications for key logging is trivial, and like any computer program can be distributed as a Trojan horse or as part of a virus or worm. What is not trivial however, is installing a keystroke logger without getting caught and downloading data that has been logged without being traced. An attacker that manually connects to a host machine to download logged keystrokes risks being traced. A Trojan that sends key logged data to a fixed e-mail address or IP address risks exposing the attacker. Definition supplied by Wikipedia
<http://en.wikipedia.org/wiki/Keylogger>

¹²⁸ “Man Hires Chinese to Hack Into Korean Computers,” *Seoul Dong-A Ilbo*, 9 Jul 05, FBIS reference number KPP20050708000217

¹²⁹ Dictionary Attack: In cryptanalysis and computer security, a dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by searching a large number of possibilities. In contrast with a brute force attack, where all possibilities are searched through exhaustively, a dictionary attack only tries possibilities which are most likely to succeed, typically derived from a list of words in a dictionary. Generally, dictionary attacks succeed because most people have a tendency to choose passwords which are easy to remember, and typically choose words taken from their native language. Definition taken from *Wikipedia*, http://en.wikipedia.org/wiki/Dictionary_attack

fraction of the normal rate and the hacker waited for potential victims. The seller/hacker wrote that they would only accept payments made to the Bank of China or Western Union international money orders. The hacker even gave an address:

Zhang Yanguang
No 7 Building 19, Floor11
Beijing Chaoyang District, Huawei Xili
100021

The unsuspecting victims would then pay for merchandise that would never be delivered. The attacks were not limited to Germany alone. It was reported that over 200 accounts in the US had been taken over in a one-week period.¹³⁰

Bank Fraud

In June of 2004, mainland Chinese hackers were involved in a scheme to steal money from Taiwanese bank accounts. According to Taiwan police, a Taiwanese citizen surnamed Chen was arrested and found to have 45 million e-mail addresses and the passwords to 200,000 bank accounts in his possession. Investigators said that Chen had attained the 45 million e-mail addresses from contacts with mainland Chinese hackers. Chen then used the e-mail addresses he had obtained from the mainland hackers to send out a Microsoft patch message containing a Trojan horse designed to lift the customers' banking account passwords. Taiwanese officials were first made aware of the crime after five Taiwanese banks reported millions of dollars worth of unauthorized ATM withdrawals from several cities across mainland China. The report also stated that Chen had received a shelled version of the Trojan from a mainland government "information officer" to keep it from being detected.¹³¹

¹³⁰ *Janko Tietz*, "Hackers Hijack Ebay Accounts," *Spiegel*, 19 Dec 05, as translated from German by *Christopher Sultan*, downloaded on 11 May 06 from <http://service.spiegel.de/cache/international/spiegel/0,1518,391774,00.html>

¹³¹ Staff of the Taiwan" page, "Police Nab Hacker for Bank Account Thefts," *The China Post*, 10 Jun 04, transcribed by FBIS reference number *CPP20040610000220*

Blackmail

Not all of the exploits are so well thought out or executed. A Chinese hacker from Jilin Province was sentenced to two years imprisonment for attempting to blackmail a Mr. Gao with photographs he stole from Mr. Gao's e-mail account and then doctored to make them appear pornographic. The hacker threatened to post Mr. Gao's "pornographic images" on the Internet if Mr. Gao did not pay him 30,000 RMB (approximately US \$3,600). However, according to the Chinese court, the photos were not those of Mr. Gao, they were actually photos of his friend.¹³²

In a grander but no more successful attempt, a Chinese hacker tried to extort 20 million RMB (approximately US \$2.4 million) from the Beijing Science and Technology Vocational College by stealing the university's enrollment information. The 22-year-old suspect confessed that he had stolen over 57,000 bits of data about the applicants by exploiting a weakness in the college's Telnet-system. Holding the information hostage, he placed a phone call to the college administrators and told them he would release it in exchange for payment of US \$2.4 million dollars. Besides the difficulties in continuing the registration process, had the data been lost it would have cost the college between US \$3.5 -18 million dollars.¹³³ No information was given on the length of the court sentence.

Extortion of schools continued when a hacker named Zhang broke into the Yu De You Teaching web site and downloaded "information" and the school's teaching materials. Holding the site hostage, he defaced the main page and demanded 7,000 RMB (approximately US \$870). Zhang was arrested in June of 2003 and sentenced to two years.¹³⁴

Public Security Bureau and Cultural Inspectors from the Lanzhou Region successfully broke up a ring of 14 Chinese hackers attempting to blackmail the Golden Line Internet Bar. The group left messages on a number of computers stating that if the owner did not give in to their demands,

¹³² "Hacker Jailed for On-Line Blackmail in China," *Beijing Xinhua in English*, 24 Mar 03, FBIS reference number CPP20030324000096

¹³³ Mu Zi, "Admissions Hacker Collared in Time," *Beijing China Daily*, 5 Jul 04, as translated by FBIS reference number CPP20040705000010

¹³⁴ "Crime, Punishment in PRC 21 Feb-15 Mar 2004," *Jinan Da Zhong Daily*, 26 Feb 04, p 10, as transcribed by FBIS reference number CPP20040329000219

all of the computers belonging to the Internet bar would be brought down. The owner refused, and true to their word, the hackers attacked all of the computers. Four of the arrested suspects confessed to damaging the computer system.¹³⁵

At 9:45 pm on 20 July 2002, computers at the Internet bar in Mawei District of Fuzhou suddenly went blank. The technician at the bar, Mr. Chen, checked the host computer and was dumbfounded as to what was happening with his system. Unable to determine what had occurred, Mr. Chen performed a restart of the system. At 10:50 pm, customers again complained that their computers were shutting down. Much to Mr. Chen's surprise the server also shutdown for no apparent reason. It was at this point that he began to suspect that it might be someone hacking into his system.

Once again at 9:45 pm the next evening, cursor control was lost on the host computer and those of the patrons. The cursors began to move erratically over the computer screens and nothing could be done to restore control. As suddenly as the incident started, the system inexplicably returned to normal. Taking no chances, Chen installed several firewalls to prevent the hacker from returning. However at 10:50 pm, the hacker re-entered the site and made changes to the member database. This pattern of attacks at 9:45 and 10:50 pm would be repeated continuously over the next few days.

At 9:45 on the evening of July 28, the hacker going by the name of Black Network made his intentions known. A document titled "Internet Cafe Surveillance" suddenly appeared on the screen of the host computer containing the following:

*"You now know how serious I am. That's right, I am that person who can shut down your computer whenever I want to and manipulate your data whenever I want to. Don't make a futile attempt to shake off my control, because I can clearly see every move you make. If you don't believe me, then try.
- Black Network."*¹³⁶

¹³⁵ "Highlights: Crime and Punishment in PRC 18 Nov-8 Dec 2002," *Beijing Renmin Gongan Bao*, 23 Nov 02, p 3, as translated by FBIS reference number CPP20021211000212

¹³⁶ Zhu Zhi, Mengmeng Baobao, "Small Hacker Attacks Internet Cafés for Extortion," *Mengmeng Baobao of Wozhai.com*, 20 Feb 05. According to the report,

Mr. Chen attempted once again to reboot the system and reinstalled the firewalls. As soon as he brought the system online again the following message appeared:

“Don't doubt my capabilities. Maybe you haven't heard about the internet cafes that have already closed. They didn't listen to me, so I was left with no choice but to shut them down permanently. You don't want to follow the same path as them, do you? When the time is right, I will of course let you know. I'll leave you alone for tonight...”

- *Black Network*¹³⁷

While the game of cat and mouse continued for several days, the hacker finally made his demands that the café owner give him 200 phone cards with a face value of 100 RMB (approximately US \$12). However, Black Network eventually ended up settling for two phone cards. Police from the Public Security Bureau were able to solve the case and arrested Wang Jian, a high school student, who confessed to the crime and said that he only wanted the phone cards so he could cover online phone charges for his computer. Wang considered the whole thing a game and said he did not know it was illegal.¹³⁸

Hacking and Music

In November of 2004, users in China were alerted to a virus named after Taiwanese pop star Stephanie Sun. It was reported that the virus was up and running shortly after the release of Ms. Sun's debut album “Stephanie.” The article further noted or insinuated, with little elaboration, that the virus was created due to the high number of searches that were being generated by Stephanie's name. The popularity of the album ensured the rapid spread of the virus from downloads of her music.¹³⁹

the original article was taken from the Taiwanese publication *Strait News* (Haixia Dushi Bao). The author was unable to locate the source document.

¹³⁷ Ibid.

¹³⁸ Ibid.

¹³⁹ “Stefanie Sun, a computer virus?” *China View*, 30 Nov 04, as downloaded on 16 May 06 from http://news.xinhuanet.com/english/2004-11/30/content_2276190.htm



Stephanie Sun
Photo: dayoo.com

Similarly, in November of 2005, hackers infected Taiwanese singer Jay Chow's music with the Gray Pigeon Trojan shortly after its release. The Trojan was discovered on an MP3 download of a song from his "November Chopin" album. At least three web sites were found to have the infected version of the song.¹⁴⁰



Jay Chow
Photo: China Radio International

¹⁴⁰ "Virus hits Chow's new MP3 song," *China View*, 7 Nov 05, as downloaded on 16 May 06 from http://news.xinhuanet.com/english/2005-11/07/content_3743192.htm

While the act of loading a virus or Trojan onto a music file is not terribly sophisticated, the timing and preparations behind the attack appear well organized. The hackers combined net reconnaissance and social engineering to produce the most effective spread of their malicious programs.

Web sites similar to Google's Adwords or Technorati were probably used to carry out the net reconnaissance. These sites allow users to view the most popular keywords and topics being searched on Google and blogs. Tools of this nature would assist the hackers in attaching their programs to the most popular vehicles in order to reach the largest number of people. While the author is not aware of their Chinese equivalent, the reference to the high number of searches generated by Stephanie Sun, strongly suggests that something similar was used.

The targeting of Taiwanese pop stars may have been a deliberate attempt to gain access to island systems and individual computers. If the hackers were simply going for the widest possible dissemination, they surely could have located more popular international stars. The timed release of the attacks in conjunction with the debut of the albums further guaranteed that unsuspecting fans would download the programs.

Hacking for Fame and Fortune

In a survey conducted by the Shanghai Academy of Social Sciences, 43% of the 5,000 primary school students they interviewed said they "adored" hackers and 33% said they dreamed of becoming one someday. Hacking in China is more than surface appeal; it is a way of life, a sub-culture, and a dream. It offers an independent path to a future of one's own choosing and not a life dictated or controlled by the state. One student named Fan Yi had this to say:

"Hackers are very cool. Hackers leave people an impression of high intelligence and are able to do whatever they like and get whatever secrets they want. That is what I lack but dream of."¹⁴¹

¹⁴¹ Yan Zhen, "Morals lost in cyberspace," *Beijing Time*, 12 Dec 05, as downloaded on 31 Aug 06 from www.shanghaidaily.com/art/2005/12/12/226181/Morals_lost_in_cyberspace.htm

To advance toward this dream and attain the lifestyle of a hacker requires cash. However, the money generated is not always done illegally. Members of the Red Hacker Alliance have found many legal methods for producing income and continue to improve and expand on them.

Publish or Perish

Given the popularity of hacking in China, there is a large market for magazines and books about the subject. Who better to provide these products than the hackers themselves? *HackerXfiles*¹⁴² produces a hacker magazine with a CD that retails for nine RMB or US \$1.10. *Hacker.com* sells their magazine, *Hacker Defense Online*¹⁴³ for 19.80 RMB or US \$2.45.



Magazine published By
HackerXfiles



Hacker Defense Online
published by *Hacker.com*

Book to Movie

On 23 August 2005, Chinese Educational Television reporter, Wang Zhonglang, interviewed *RedHacker* stationmaster Sharp Winner about his new book The Turbulent Times of the Red Hackers. During the course of the discussion, Sharp Winner made some interesting comments on the reasoning

¹⁴² “Hacker Xfiles” published by HackerXfiles
<http://www.hackerxfiles.net/viewthread.php?tid=19394> the sales figures were converted to US using the exchange rate of 8.08 Yuan to the dollar on 17 Oct 2005

¹⁴³ “Hacker Defense Online” published by <http://www.hacker.com.cn/>

and commerciality of the enterprise. He stated that the original plan was to have the book published on their web site. However, after further consideration, he wanted to make it available to everyone so they could better understand the hacker culture.

The theme of the book revolves around the Red Hacker Alliance defending the country against a large-scale computer attack, to include an overseas spy ring. When asked about the book becoming a movie, Sharp Winner admitted that he was involved in negotiations with investors and if it could be settled, he would ask Zhang Yimou, one of China's most famous directors, to shoot the film.¹⁴⁴ He also detailed his plan to market numerous Red Hacker souvenirs, to include hats, T-shirts, sunglasses and even the props used in the movie.

Asked about what was going on with the group, Sharp Winner replied that the group had established a club¹⁴⁵ and future projects included promoting Red Hacker training and more books.¹⁴⁶ Pictured below is the *RedHacker* club logo:



It Pays to Advertise

China's online advertising market is predicted to reach approximately US \$550 million in 2006 and skyrocket well beyond that in 2008 when

¹⁴⁴ Zhang Yimou's resume includes the films *Hero*, *House of Flying Daggers*, and *Raise the Red Lantern*. Profile of Zhang Yimou at <http://www.imdb.com/name/nm0955443/>

¹⁴⁵ *RedHacker* Club picture downloaded from <http://www.redhacker.cn/index.html> on 18 Oct 2005

¹⁴⁶ Gao Shaohua, Interview with Sharp Winner, 26 Aug 05, <http://news.chinabyte.com/115/2089115.shtml>

Beijing hosts the international Olympic games.¹⁴⁷ As network dollars continue to flood in, members within the Red Hacker Alliance are marketing their site members' demographics to lure advertisers and capture a share of the booming Internet sector of the economy.

As discussed earlier, the site *CyCyCy* posted membership demographics to attract advertisers. Along with this information was a detailed argument for why software firms should advertise their products on the site. The argument was: (1) the site is dedicated to people who are in search of software; (2) *CyCyCy* is a large web site that receives over 10,000 hits per day and still growing; (3) the site is devoted to amateur computer enthusiasts who are very interested in software and hardware information; (4) the site has a very stable group of online users that translates into a long-term market; and (5) *CyCyCy* members have strong purchasing power. Further, the users are between the ages of 20 and 45; mostly high school graduates; located in major cities; and have above medium income level.¹⁴⁸ It is unknown how the revenue is divided up among the members but certainly some of it is used to pay site managers, technicians, cover equipment costs, and domain fees.

HackVip provides some fairly typical examples of the types of companies that advertise on the hacker's web sites such as Love 9 Network¹⁴⁹ (an IT service company) and an online movie download site.¹⁵⁰

¹⁴⁷ Analysys International Forecast, "Analysys International says China's Online Advertising Market Will Reach RMB 4.39 Billion in 2006," 28 Aug 06, <http://english.analysys.com.cn/3class/detail.php?id=241&name=report&FocusAreaTitleGB=&daohang=Internet&title=Analysys%20International%20says%20China's%20Online%20Advertising%20Market%20Will%20Reach...>

¹⁴⁸ Demographics promotion from <http://www.cycycy.net/ads.html> downloaded 5 Oct 2005

¹⁴⁹ Taken from sponsor site of Love 9 Network <http://www.99i.cn/about.asp> 18 Oct 2005

¹⁵⁰ <http://movie.jdide.com/>



Love 9 Network



Online Movie Download Site

The web site *Chinesehack* even provided potential customers with a breakdown of the advertising costs on their site:

Ad type	Position on Page	Cost Per Month (RMB)
150 by 30	Homepage	200 (approx US \$25)
120 by 60	Homepage	200 (approx US \$25)
468 by 60	Top of the Homepage	450 (approx US \$56)
468 by 60	Bottom of the Homepage	400 (approx US \$50)
Text Ads	All internal pages	200 (approx US \$25)
100 by 100 Hovering Ads	Homepage	300 (approx US \$37)
400 by 300 Pop-Up Ads	Homepage	600 (approx US \$75)

Training the next generation of hackers may also generate income. While many of the sites have sections on their bulletin boards for novice hackers to ask questions and exchange information, some sites are turning to a for-fee comprehensive training course to educate their members. It is rumored that brick and mortar schools also exist with onsite instructors.

安盟商城		[安全光盘]	[安全书籍]	[CS作弊器]	
					
黑客防线2006第6期	编程学习	动画教程大全	黑客工具	破解工具大全2006	
市场价：¥35	市场价：¥60	市场价：¥60	市场价：¥60	市场价：¥60	
商城价：¥35	商城价：¥58	商城价：¥58	商城价：¥58	商城价：¥58	
会员价：¥32	会员价：¥55	会员价：¥55	会员价：¥55	会员价：¥50	
精品黑客安全动画		[入侵动画]	[破解动画]	[安全动画]	[综合动画]
		[菜鸟必看]	[QQ攻防]	[木马相关]	[漏洞攻击]

Four disc training course including preloaded hacking tools from *hnhacker.com*

Pornography

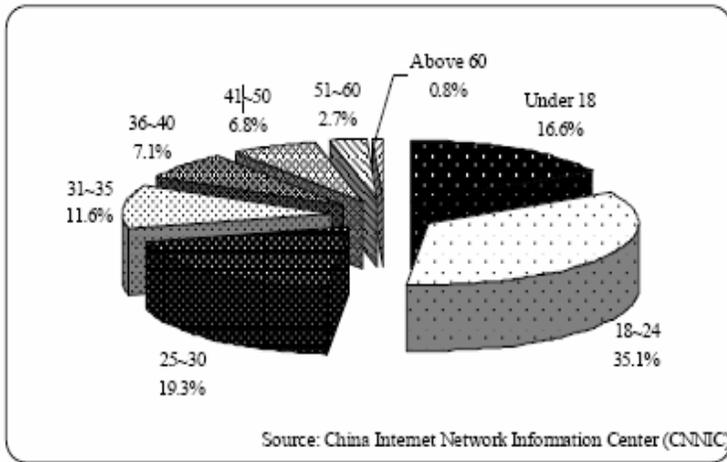
The pairing of demographics and culture in the Chinese hacker community has produced another mechanism for making money in the form of pornography. According to information contained in the 17th Statistical Survey Report on Internet Development in China (published in January 2006), conducted by the China Internet Network Information Center (CNNIC):

58.7% of Chinese online users were male

41.3% of Chinese online users were female

51.7% of Chinese online users were under the age of 24¹⁵¹

¹⁵¹ “17th Statistical Survey Report on Internet Development in China (Jan. 2006),” CNNIC, as downloaded on 15 Jul 06 from <http://www.cnnic.net.cn/en/index/00/index.htm>



Breakdown of Internet users by age group

China’s *Xinhua News Agency* reported 46% of online minors “often” visited web sites containing pornographic material. The overall lack of sex education in China is also noted as a reason for the explosion of pornography. A college student from Jiaotong University in Shanghai made the following observation:

*"Porn web sites are rooted in young people who were thirsty for the facts of life, on which education is so deficient in the nation."*¹⁵²

According to *Xinhua*, this sentiment was “echoed” by numerous university students throughout the country. Cultural norms have resulted in the reluctance of Chinese parents to discuss these types of topics with their children. A study conducted by China Social Survey, found that 92.5% of students had questions or difficulties with sex and only 2.6% had received answers from their parents.¹⁵³ The age demographic and void in sexual education has caused some to search the Internet to satisfy their curiosity.¹⁵⁴

¹⁵² “China's Fight Against Internet Porn Continues,” *Beijing Xinhua in English*, 31 Jul 05, FBIS reference number CPP20040801000010

¹⁵³ Ibid.

¹⁵⁴ Ibid.

A minority in the Red Hacker Alliance have seized on this combination of age and curiosity to increase membership and produce income. It should be emphasized that this is a small minority and that there are conversations within the community that speak out quite vocally against it. That said, it is still important to remember this activity is a source of funding and reaches back to servers in the United States.



From the web site <http://www.hack77.com/>. The last two photos were completely downloaded when the screenshot was taken. This was probably to prevent showing lewd pictures on the main page. This is an example of free internal soft-porn presented on hacker web site.



Same type of photography contained on the web site <http://www.sollit.com/>

The two methods that seem to be employed are posting soft-core pictures on the hacker site itself or providing a pay link to a proxy server outside of China. The sites that post pictures on their individual web sites exclusively use pictures of young Asian females. This is most likely to attract and retain young male members who make up a majority of the hacking community.

For example, a link from the hacker web site *Hackol* contains a link to a pornographic web site that is hosted on a proxy server in California. The *Hackol* link is probably to generate cash revenue and at the same time thwart Chinese censors who are cracking down on online pornography. The hacker site *21safe* has a similar link, however it resolves to a link in Henan Province inside of China. Once again, this is more than likely to generate income.



Pay site from <http://www.hackol.com/index.html> linking back to a proxy server located in California.



Pay site from <http://www.21safe.com/index.htm> linking back to Henan

In May of 2005 a Chinese hacker from Hubei Province was brought up on charges of “disseminating lewd advertisements for profit.” According to the report, he illegally gained access to the welfare information system operated by the Bureau of Civil Affairs of Tianjin. He then set up a

homepage called *Sexual Paradise* and in only two months attracted 66,000 club members.¹⁵⁵

¹⁵⁵ “China's Fight Against Internet Porn Continues,” *Beijing Xinhua in English*, 31 Jul 05, FBIS reference number CPP20040801000010

Chapter Four Government Affiliation

政府

Black and White Do Not Exist

In the opening of this book, government affiliation of the Red Hacker Alliance was identified as a key question and one essential to answer. Are they or are they not an officially sanctioned apparatus of the state? When this question was initially raised, it referred to tasking, oversight, and control of the organization. The simple answer is no, they are not a branch of the government or the military. Based on the extensive research and analysis conducted here in order to understand Chinese hackers, this author concludes that the alliance is exactly who and what they claim to be: an independent confederation of patriotic youth dedicated to defending China against what it perceives as threats to national pride. No evidence whatsoever has been uncovered showing direct government control of the alliance and all indicators point to it being a civilian led organization. However, it is also the author's contention that the question of direct government affiliation is itself flawed and the simple answer of "no" highly misleading.

The central problem with our initial inquiry and the thinking behind it is that we are viewing the situation from a US paradigm and applying cultural bias. In Chinese society, independence from government direction and control does not carry with it the idea of separation from the state. The PRC government views its citizenry as an integral part of Comprehensive National Power and a vital component to national security.

Comprehensive National Power: "The combined overall conditions and strengths of a country in numerous areas. During the Cold War and the US-Soviet confrontation, a nation's power was largely determined by military force, but in the current transition period, as the world moves toward multipolarity, military might is no longer the main defining factor of strength. Instead, elements such as economics and science and technology have become increasingly important in the competition for power and influence in the world. An evaluation of current and future strength requires the inclusion of a variety of factors, such as territory, natural resources, military force,

economic power, social conditions, domestic government, foreign policy, and international influence.”¹⁵⁶

The masses figure heavily into China’s strategic calculations and will be actively used in times of conflict and peace. So, while applying the label of a nongovernmental entity to the alliance is true, it is also deceiving. Affixing this tag implies that the Red Hacker Alliance is not associated with the official intelligence structure in any capacity. This is also incorrect. The inability to derive a “yes” or “no” answer to this problem is rooted in our tendency to apply mirror imaging of societal norms where they do not exist.

From a Western perspective, the idea of active espionage against another nation requires government initiative, involvement, and direction. It is hard for us to conceive of links being formed between state authorities and quasi-freelance intelligence operations, simply because it does not fit our preconceived notion of the proper relationship. When in fact, there is a very good chance this is exactly the type of association that is taking place between the central government and the Red Hacker Alliance. Western nations assign virtually no intelligence-gathering role of any kind to its nongovernmental citizens in peacetime; even during periods of active conflict Western citizens are probably best defined as heightened citizen watch groups. China, on the other hand, does not make a distinction between these two responsibilities; citizens are expected to take part in both arenas. The People’s Liberation Army emphasizes the integration of military and civilian roles in their strategic doctrine of future wars:

“In the high-tech local war which we will face in the future, the role of the masses as the main body of the war is embodied by the country. The great power of the people’s war is released through comprehensive national power, the combination of peace time and war time, the combinations of the military and the civilian, and the combination of war actions and non-war actions. Besides the direct participation and cooperation with the army’s operations in the region where war happens, the masses will support the war

¹⁵⁶ Michael Pillsbury, *CHINA DEBATES the FUTURE SECURITY ENVIRONMENT*, Jan 00, Chapter 5,

mainly by political, economic, technical, cultural and moral means.”¹⁵⁷

The Chinese believe in the idea of a people’s war in which the entire population is mobilized to struggle on behalf of the nation. The Red Hacker Alliance will gladly assume its role as protector and seek out targets of opportunity to attack. Being a civilian organization will in no way limit their participation in striking out at the enemies of China. If history is any indication, as the numerous examples in Chapter One demonstrate, they will take the lead in launching preemptive or retaliatory assaults.

So, what would this quasi-official relationship look like and what characteristics would it take on? An interview with a Chinese hacker from Beijing provides an excellent example of this “nontraditional” relationship:

*“One Beijing hacker says two Chinese officials approached him a couple of years ago requesting ‘help in obtaining classified information’ from foreign governments. He says he refused the ‘assignment,’ but admits he perused a top US general’s personal documents once while scanning for weaknesses in Pentagon information systems ‘for fun.’ The hacker, who requested anonymity to avoid detection, acknowledges that Chinese companies now hire people like him to conduct industrial espionage. ‘It used to be that hackers wouldn’t do that because we all had a sense of social responsibility,’ says the well-groomed thirty something, ‘but now people do anything for money.’”*¹⁵⁸

This technique used with the Beijing hacker typifies the same soft-control the government exercises on human intelligence collectors in the US and other countries. China relies on a broad informal network of students, tourists, teachers, and foreign workers inside of host nations to collect small bits of information to form a composite picture of the environment. Rather than set a targeted goal for collection, they instead rely on sheer weight of

¹⁵⁷ Peng Guangqian, Yao Youzhi, *The Science of Military Strategy*, Military Publishing House, Academy of Military Science of the Chinese People’s Liberation Army, 2005, p. 455

¹⁵⁸ Melinda Liu, “High-Tech Hunger,” *Newsweek International Edition*, 16 Jan 06, as downloaded on 23 Feb 06 from <http://www.msnbc.msn.com/id/10756796/site/newsweek/>

information to form a clear understanding of the situation.¹⁵⁹ This work hopes to demonstrate that this is the type of informal association the government and certain members of the Red Hacker Alliance share. However, the government has recognized the value of Red Hacker Alliance members and has made tentative contacts that will be discussed later in this chapter under recruitment and communications. The reasons behind the contacts are that alliance members make ideal candidates for flexible operations; they have proven themselves to be creative, patriotic, capable, and motivated. To clarify, this is not to suggest that every member or even a majority of alliance members have connections with the government. In fact, there are probably only a select few who have any dealings whatsoever with officials.

Additionally, there are intricacies and complexities of this dynamic that move it far beyond the headline grabbing probes for international secrets. Political, economic, and social issues account for a majority of the contacts between the two and require a delicate balance of constraints and freedoms. We can even surmise that there are times when an uneasy truce exists between the two parties. This unease would stem from the alliance's concerns over a possible crackdown on the organization and the government's fear of a hacker instigated rebellion among its youthful members. A better understanding of the points where mutual interests converge will aid us in unraveling what mechanisms bind them together and how they possibly interact.

Intelligence and Economics

From the Party's viewpoint, the Red Hacker Alliance must have benefits that outweigh their liabilities. If political activism and attempts to penetrate foreign systems brought about only international condemnation and created points of contention between China and other nations, the organization's activities would be halted. Beijing is well aware of the possible downside this group represents and the inherent dangers present in their involvement during times of crisis. An international dilemma on the verge of resolution might be exasperated by cyber attacks on infrastructure or governmental institutions and could possibly result in unforeseen and unmanageable consequences. On the other hand, if the returns are greater

¹⁵⁹Jay Solomon, "FBI sees big threat from Chinese spies," *Wall Street Journal*, 10 Aug 05, downloaded on 23 Feb 06 from <http://www.post-gazette.com/pg/05222/551701.stm>

than the costs and the benefits outweigh the risks, then the Red Hacker Alliance will be seen as an asset and allowed to continue. At the moment, there are no indicators that the authorities in Beijing are making any attempts to rein in or shutdown the alliance, a telling sign that the cost-benefit analysis is still in the alliance's favor. So, if this is not a government-sponsored agency, what are the factors that make it more profitable to protect the organization and risk a possible escalation of international tensions, than to be rid of them?

The most obvious reason for Beijing's apparent tolerance of the group is that it likely receives valuable information from the alliance. Thousands of hackers, working around the clock, could surely fill in some of the blanks of a composite intelligence picture. As a civilian organization, the Red Hacker Alliance also provides the government with plausible deniability. Even if alliance members are caught red-handed breaking into a system, it is easily disavowed as the actions of overzealous youth and certainly not that of the government. In December of 2005, as accusations of China's involvement in government-sponsored hacking heated up, People's Republic of China Foreign Ministry spokesman Qin Gang flatly denied charges that the government was involved and asked the US to produce any information it had proving these allegations.¹⁶⁰ The foreign minister offered nothing further and simply dismissed the idea in its entirety, holding fast to the argument that China had regulations prohibiting attacks on the Internet and that should be proof enough to show they were not involved. This denial of involvement and demand for proof is highly effective at deterring further inquiry. It requires specific incidents be revealed and the techniques that led to those conclusions be explained, thereby revealing US operational capabilities in intrusion detection, backtracking, and identifying attacking points of origin.

We should also be careful in assuming that the relationship between the government and the alliance is a one-way street, with the authorities requesting information and Red Hacker Alliance members providing it. It is quite possible there are times when the alliance, of its own volition, initiates collections against certain targets and then supplies that sensitive data to the government. Owing to the increased entrepreneurial nature of the

¹⁶⁰ "Internet hack accusation groundless," *China Daily*, 12 Dec 05, as downloaded on 22 Feb 06 from http://www.chinadaily.com.cn/english/doc/2005-12/13/content_503098.htm

organization, financial compensation for these efforts cannot be ruled out and may act as a possible motivator for them to break into foreign systems. Going even further with this speculation, it is not certain that the Chinese government is the only client or requestor for the information. This knowledge would be highly valuable to other governments or even private companies around the world.

Corporate espionage is another arena where we must put aside our cultural bias and make judgments based on the Chinese system rather than Western practices. If a US citizen were asked, “Who would be the most likely suspect in a crime involving the theft of corporate secrets for financial gain?” The answer given would probably be another company. That the government would condone or even encourage industrial spying and data theft for fiscal gain is a very remote idea for us. However, the Chinese government does not divorce itself from domestic industry and all assets located inside of China are viewed as assets of the state. Financial institutions are deemed a vital component for the health and stability of the nation and are at least on par with, if not on a higher priority than the development of its military capabilities. Hacker efforts to assist in the advancement of state enterprises, whether that assistance is offered in return for monetary compensation or not, would be viewed as advantageous and likely overlooked by officials.

It is claimed that Taipei’s M-etal Multimedia Company experienced this idiosyncrasy of the relationship between the Chinese government, a “private” mainland corporation, and a hacker (albeit from Taiwan) first-hand when it lost millions of dollars to the ChuangYu corporation through software piracy. It is alleged that a Taiwanese student named Huang was hired by the ChuangYu Internet Company to break into M-etal’s system and make copies of their online games. Huang reportedly then posted the stolen online games on ChuangYu’s system where mainland Chinese users could download them for a mere fraction of the price charged by M-etal. Following this incident, Taiwanese police issued a warning to remain alert, reminding corporations that there are “some 300,000-plus hackers in China who break into high-tech companies around the world and steal confidential information and programs, with the tacit consent of the Chinese government.”¹⁶¹

¹⁶¹ “Taiwan: Hacker Working for PRC Firm Arrested,” *Taipei Times*, 26 Jun 02, as downloaded from FBIS reference number CPP20020626000139

In a wave of industrial spying that began in August of 2004 and lasted through at least the first quarter of 2005, hacker/hackers from China unleashed the Myfip Trojan on corporate computers. Myfip is designed to search for files related to high-tech research and development and send them back to an individual named Si Wen in Tianjin, China. Joseph Stewart, a senior security researcher and the man responsible for reverse engineering Myfip, noted that Tianjin is “China’s third-largest city and the second-biggest hub for manufacturing, particularly electronics.” It was further pointed out that the attacks were so brazen, the hacker/hackers didn’t bother to obscure their location, a norm for most experienced hackers.¹⁶² Weighing in on the issue, Chief of Defense John Watters said:

“Nothing suggests that Chinese authorities are vigilantly prosecuting those who are attacking foreign interests. They turn a blind eye to it as long as it doesn't oppose national interests.”¹⁶³

Sectors where the financial interest of the alliance and the security interests of the state coincide could present even greater difficulties for outside industries to protect their trade secrets and keep them confidential. Take for example China’s rising energy needs and its worldwide search for energy resources. There are tremendous pressures exerted on the state to sustain the country’s economic momentum moving forward and to do that they must ensure a consistent and steady supply of fuel. The competition to secure finite resources such as oil and natural gas can be quite competitive and the methods to attain them could move far beyond those of traditional market mechanisms. Chinese hackers, working for personal gain, could find a lucrative market in the sale of information related to the petroleum industry and the state may be more inclined to turn a blind eye to the practice if it facilitated expansion of Chinese industrial interests.

Political

In addition to intelligence gathering and economic interests, politics is also a driving force that binds the alliance and government together. The political front can be divided into two distinct categories, domestic and

¹⁶² Nathan Vardi, “Chinese Takeout,” *Forbes*, 25 Jul 05, as downloaded on 8 May 06 from http://www.forbes.com/forbes/2005/0725/054_print.html

¹⁶³ *Ibid.*

international. Internal or domestically motivated political hacking is aimed at dissident elements and separatist movements found inside the country and extended to supporters of those same movements outside the country. The recipients of these attacks are typically causes that threaten national sovereignty and challenge the legitimacy of the ruling party, such as the Falun Gong, the Free Tibet movement, and Hong Kong activists.¹⁶⁴

In 2002, dissident groups outside of China complained that attempts were made by Chinese hackers to shut down their operations through virus and Trojan attacks focused on the e-mail addresses of the Falun Gong,² banned news sites, freenet-china.org, and Xinjiang independence activists.¹⁶⁵ It was noted that the attacks began at roughly the same time that the Minister of Public Security called for more aggressive measures in going after “foreign

¹⁶⁴ Falun Gong has been the focus of international controversy since the government of the People's Republic of China began a nationwide suppression of Falun Gong on July 20, 1999. Concerns were triggered especially when 10,000 practitioners assembled in peaceful protest at the Central Appeal Office at Foyou street, outside Zhongnanhai. The assembly was prompted by reports of violence and harassment inflicted upon practitioners by Chinese police in the city of Tianjin, as well as a ban on publishing Falun Dafa materials. Falun Gong; literally "Practice of the Wheel of Law" is also known as Falun Dafa, a system of qigong introduced by Li Hongzhi in 1992. *Falun* is also sometimes translated as dharma wheel or chakra. Central to Falun Gong is five sets of meditation exercises (four standing, and one sitting). A few years after its public introduction in 1992, Falun Gong quickly grew to become one of the most popular forms of qigong in Chinese history, and has been growing in popularity around the world. Background and definition provided by *Wikipedia* http://en.wikipedia.org/wiki/Falun_Gong; for Hong Kong causes, see Liu Yong, “Hong Kong activist says Chinese hackers read his e-mails,” Radio Free Asia, 6 Jul 05, http://chinadigitaltimes.net/2005/07/hong_kong_activ_1.php; for dissident causes, see

Doug Nairne, “State hackers spying on us, say dissidents,” *South China Morning Post*, 18 Sep 02, http://www.tibet.ca/en/wtnarchive/2002/9/18_5.html
Dorothy E. Denning, “Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy,” *Rand Corporation*, Chapter 8, p. 38, 10 Dec 99, http://72.14.203.104/search?q=cache:Cebk04cEdLYJ:www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch8.pdf+%22chinese+hackers%22+falun+gong&hl=en&gl=us&ct=clnk&cd=75

¹⁶⁵ Doug Nairne, “State hackers spying on us, say dissidents,” *South China Morning Post*, 18 Sep 02, http://www.tibet.ca/en/wtnarchive/2002/9/18_5.html, http://www.fofg.org/news/news_story.php?doc_id=44

forces subverting China via the Internet.”¹⁶⁶ Chong Yiu-kwong, a human rights activist who organized democracy marches in Hong Kong, discovered that his e-mail was being monitored.

*"I didn't know that my computer had been monitored ever since, until I found that all my e-mails from the account registered to the University of Hong Kong disappeared all of a sudden. I approached the computer center of Hong Kong University. They told me that my account had been monitored by three different IP addresses from China and that information from the account had been downloaded every few minutes."*¹⁶⁷

A Chinese Internet security official described separatist activities as one of the major trends in cyber crime for 2002. According to the official, Falun Gong practitioners had used the Internet to spread their philosophy and “organize illegal activities.” “Splittist” and anti-Chinese elements had evoked disunity and made attacks on the government and Party leadership.¹⁶⁸ This statement likely stemmed from a 2002 speech made by Luo Gan, a member of the Political Bureau and secretary of the Central Commission on Politics and Law, at the National Conference on Judicial, Procuratorial, and Public Security Work referencing law enforcement reforms. At the conference, Luo Gan identified cyber crimes as one of the three most important problems facing the country and singled out the Falun Gong as an example:

*"Hostile forces at home and abroad as well as the Falun gong cult are doing everything in their power to spread rumors and launch attacks on the Internet. They are sending reactionary e-mail messages in large quantities to stir up trouble. Hostile forces and some people with ulterior motives may disrupt our Internet system through such means as computer virus attacks and hacker attacks. Other illegal and criminal acts, such as online financial fraud, are also growing. Hidden security hazards are becoming more acute."*¹⁶⁹

¹⁶⁶ Ibid.

¹⁶⁷ Liu Yong, “Hong Kong activist says Chinese hackers read his e-mails,” Radio Free Asia, 6 Jul 05, http://chinadigitaltimes.net/2005/07/hong_kong_activ_1.php

¹⁶⁸ Li Heng, “New Faces of Cybercrimes,” *People's Daily Online*, 11 Apr 02, as transcribed by FBIS reference number CPP20020411000097

¹⁶⁹ Yu Bin, “National Conference on Judicial, Procuratorial, and Public Security Work Unveils New Measures for Safeguarding Stability in Order To Provide Strong

Toward the middle of 2004, a Hong Kong pro-democracy web site called Anti-Tung, named after the unpopular Chief Executive who was viewed as a Beijing puppet, was hacked. Reports claimed that Anti-Tung was instrumental in using the Internet to mobilize public demonstrations against the central government. Mr. Wai, a spokesman for the movement, commented on the attacks:

*"We are worried that we are just the first victim. There might be more attempts to disrupt this powerful medium in the run-up to September's polls and the protest this July. This is definitely a calculated attack. It may be politically motivated. I don't know what the police could do. If the hacker is not in Hong Kong, the police can't do much about it."*¹⁷⁰

In international disputes, Beijing has been able to count on the Red Hackers as a surrogate political hammer and a rallying force for mainland solidarity. The historical account of the alliance, from its inception to present day, demonstrates an organization that aggressively backs governmental policy through a flexing of cyber muscle. As documented in Chapter One, these international cases include the attacks against the United States, the United Kingdom, Japan, and Indonesia. Other favorite targets of these attacks are elections and referendums that touch on Taiwanese independence. During the June 2005 Asian-Pacific Economic Cooperation forum held in Seoul, an officer of the Taiwanese Criminal Investigation Bureau approached delegates from the People's Republic of China and requested their assistance in a joint crackdown on hacker attacks. Chinese delegates "cold-shouldered" the officer's request.¹⁷¹

Favorable public sentiment for the alliance's nationalistic stances also provides some degree of guaranteed protection and support from the government. Ordinary citizens see them as a voice for the people, stretching across great distances to right the wrongs done to China by her enemies. In

Legal Guarantees for Building a Well-Off Society in an All-Around Manner," *Beijing Liaowang*, 23 Dec 02, No 51, pp 11-13, as translated by FBIS reference number CPP20030102000030

¹⁷⁰ Jimmy Cheung, "Anti-Tung group suffers cyber attack," *Hong Kong South China Morning Post*, 1 May 04, as transcribed by FBIS reference number CPP20040501000012

¹⁷¹ Flor Wang, "China 'Rejected' Taiwan Proposal On Joint Crackdown On Hackers," *Taipei Central News Agency*, 23 Jul 05, FBIS reference number CPP20050723000115

some circles, individuals such as Lion and Wan Tao are looked on as Hollywood stars and not criminals. During the Sino-Japanese hacker attacks of 2000, Japanese officials requested that the web sites of known hackers in the Guangxi, China area be shutdown for attacking Japanese web sites. Police responded that they had no intentions of doing so because it was a “patriotic” web site.¹⁷² Few media outlets in China show the darker side of Chinese hackers. Their reputations as crusaders for the motherland are meticulously maintained.

Recruiting

“The smallest detail, taken from an actual incident in war, is more instructive for me, a soldier, than all the Theirs, and Jominis in the world. They speak, no doubt, for the heads of states and armies but they never show me what I wish to know – a battalion, a company, a squad, in action.”

-Col. Charles Ardant du Picq¹⁷³

China, which is still in the early stages of informationizing the nation and its military, recognizes the disparity in technical knowledge and experience between itself and other countries. To some extent and in certain circles, the government has also come to appreciate this same gap between the older and younger generations of its own citizenry. It is easy for us to lose sight of the fact that China has only recently gained access to the Internet and the migration process from social elites to the average citizen has taken some years. Familiarity and comfort levels with new programs and the Web in general are likely sharply divided between age groups. Chinese youth, like those in most nations, are more flexible and quickly adapt to new technologies while the older generation struggles to incorporate it. China’s elders are now reaching out to their children for help in understanding the uses of this new technology and the children are eager to assist.

Evidence taken from People’s Republic of China Internet forums and news broadcasts demonstrates that members of the Red Hacker Alliance

¹⁷² “Chinese 'Right-Wingers' Vow To Hack Japanese Web sites,” Hong Kong AFB, 14 Feb 00, translated by FBIS reference number CPP20000214000027

¹⁷³ Battle Studies: Ancient and Modern Battle from Russel A. Gugeler, Combat Actions in Korea, US Government Printing Office, 1970 revised edition, p. iii

would like to be a state-sponsored agency and are somewhat offended they are not. On 6 August 2005, Phoenix television news carried a report that Chinese hackers wanted to be recruited by the government to form network security units in order to protect the safety of domestic networks. Postings on the *Honker Union of China's* web site were in firm agreement.

"We need to move toward standardized honker unions. We can't wait until the nation has a crisis to act; we must be prepared to do something meaningful for the motherland. Why can't we become a government-approved network technology security unit?"¹⁷⁴

According to other postings, various members of the organization had learned of foreign countries establishing "hacker network security units" and felt China should do the same.

"It should have been this way earlier! The US, Westerners, Israel, and even the good guys [a san] have all formed hacker army groups! We can't lag behind!"¹⁷⁵

Similarly, portions of the government have expressed interest in recruiting or at least learning from members of the alliance. Following the Sino-US cyber conflict of 2001, ignited by the mid-air collision of a US reconnaissance aircraft and a PRC fighter aircraft, renowned Chinese military expert Professor Zhang Zhaozhong expounded on the vital significance of the 7-day network war. He suggested that these real-life experiences in network warfare should be officially researched for the benefit of the country. As the Director of the National Defense University's Military Science and Technology and Equipment Research Department, Professor Zhang pointed

¹⁷⁴ Highlights: PRC Military Forums 7-25 Aug 2005, compiled from *Jiefangjun Bao forums* <http://bbs.chinamil.com/cn/forums/> a Beijing bulletin board page for *Jiefangjun Bao* includes forums for enlisted soldiers and one on general defense issues; *Tiexue*, www.tiexue.com, PRC military enthusiast web site with Bulletin boards on general military topics; and *Warsky*, www.war-sky.com, PRC military enthusiast web site. The latter's bulletin boards include good coverage of Chinese navy developments. All translations by FBIS reference number CPP20050829000234

¹⁷⁵ Ibid.

out that during the course of the cyber conflict, Chinese hackers had developed many new tactics and gained much experience.¹⁷⁶

However, he also believed that neither the Chinese nor the US government could tacitly condone this type of behavior, as it was harmful to the relationship between the two nations and at odds with their national interests. Professor Zhang also expressed concern over the violation of treaties and laws. He felt that on the one hand the hackers should be commended for their well-intentioned spirit and motives for carrying out the attacks but on the other, they needed to be educated on the serious consequences of these attacks and how easily innocents can be harmed.¹⁷⁷

Returning to his argument for the study of this incident, Professor Zhang brought up President Clinton's invitation for expert hackers to attend a meeting at the White House to discuss network security. Perhaps such an invitation could be used as a precedent for China to explore the "special role" of hackers. According to Zhang, network warfare was one of the measures of the comprehensive national power of a nation. To underscore the importance of the study, he gave examples of the levels of difficulty in systems penetration.

"While it is relatively easy to tamper with a few web pages, it is much harder to attack the Department of Defense's network. Trying to penetrate the Pentagon, stealing nuclear secrets, or passing yourself off as a high ranking US military commander issuing orders to operational units is like reaching for the stars."¹⁷⁸

Even though this mutual attraction to form collaborative efforts could be seen as a positive trend in the relationship, it may, in the end produce the opposite effect and wind up being a source for potential tension between the hackers and the Chinese government. In early 2006, members of the Red Hacker Alliance were dissatisfied with the government's slow reaction in responding to what they considered a deterioration of the domestic network security environment and began taking matters in their own hands. Through

¹⁷⁶ "China Military Expert Praises Chinese Hackers for 'Innovative Tactics' during the Sino-US computer conflict," *Zaobao.com*, 12 May 01, http://www.zaobao.com/special/china/sino_us/pages2/hackers120501.html

¹⁷⁷ Ibid.

¹⁷⁸ Ibid.

monitoring of foreign hacker web sites, Chinese hackers had discovered numerous daily intrusions into Chinese government systems. The “foreign” hackers were making a game of counting the number of servers they could break into inside of China. When alliance members attempted to notify officials of these security vulnerabilities, they were rebuffed and told appropriate security firms were handling the situation. In some cases, it took days for the defaced web sites to be discovered and returned to normal. In growing frustration, Chinese hackers, in an effort to reinforce their warnings of the defective security measures, took to defacing their own government web sites.¹⁷⁹ One hacker felt it might even have ramifications on any future cyber warfare with Japan:

"If there really is a China-Japan Hacker War in the future, will this type of network technology do! Last week I spent an immense amount of energy to get into a petty Japanese trash web site. I uploaded the modified main page. Half an hour later I took a look and its main page was, to my surprise, restored. Looking at those web sites, those Chinese web sites, which are, moreover, the web sites of government departments, they were hacked over a week ago and still no one knows. Geez!"¹⁸⁰

The weakness of government servers may be another possible explanation for cyber espionage charges leveled at China. Civilian hackers inside the country and foreign hackers outside the country, hijacking these systems, could account for a large number of the attacks originating from Chinese government owned resources. It is doubtful, the People’s Liberation Army or any other affiliated group, would attempt intrusions from accounts so easily identified. However, independents could find them easily co-opted targets and excellent launching pads for attacks. In March of 2005, the Ministry of Public Security arrested a man from Hubei Province for forming a Botnet of 100,000 stolen computers.¹⁸¹ According to the bureau, of the

¹⁷⁹ “Foreign Hackers Target Chinese Government Web; Honkers Worried About Being in Inferior Position in Internet War,” *Hong Kong Feng Huang Wang*, 6 Feb 06, FBIS reference number CPP20060228398001

¹⁸⁰ Ibid.

¹⁸¹ “(roBOT NETwork) Also called a "zombie army," a botnet is a large number of compromised computers that are used to create denial of service attacks or send spam. The computer is compromised via a Trojan that often opens an IRC channel and waits for commands from the person in control of the botnet. There is even a botnet business with lists of compromised computers sold to hackers and spammers.”

100,000 infected, more than 60,000 were inside China, with a portion of those government computers.¹⁸² A year later, *Xinhua News Agency* reported that in the first quarter of 2006, hackers had “changed information” on the web pages of 2,027 official government web sites. The 2006 first quarter statistics almost matched the entire number of compromised for all of 2005.¹⁸³

An individual going by the alias of Chang Wei gave his personal account of PRC civilian hacker recruiting practices. During an interview in 2002, Chang stated that he worked for a secret department under the Ministry of Information Technology and Telecommunications Industries tasked with breaking computer codes of foreign companies and governments. He revealed that due to the large concentration of software talent, new members for his organization were mainly scouted from universities. However, the search was not limited to college campuses, people from all social strata were sought after if they were qualified. According to Chang, the workers were called “Internet Warriors” and received about US \$52 dollars a month while private sector programmers took home around US \$800 dollars. Training for new personnel began with monitoring Internet user’s online activities so that they could learn how to track their movements through the Internet. Depending on the talents displayed, some would move up to become computer hackers or software writers and those who demonstrated the most talent would become code breakers. Chang Wei stated:

*“If you know how much we can find out about you from the Internet, you probably will never again dare to surf the Internet in the Chinese mainland. We can break practically any codes and intrude into your bank account. We can read your e-mails as well as send an e-mail to your boss from your computer and can write in Chinese as well as English.”*¹⁸⁴

Definition supplied by *PC Magazine* as downloaded on 11 May 06 from http://www.pcmag.com/encyclopedia_term/0,2542,t=botnet&i=38866,00.asp

¹⁸² “Top Chinese Hacker Arrested for Manipulating 100,000 Computers,” *Beijing Xinhua*, 25 Mar 05, FBIS reference number CPP20050325000191

¹⁸³ “Attacks on Gov Web sites skyrocket,” *Shanghai Daily*, 31 Mar 06,

<http://www.shanghaidaily.com/press/2006/03/31/attacks-on-gov-web-sites-skyrocket/>

¹⁸⁴ Chu Chien-ling, “Communist China Organizes, Trains Internet Warriors as Information Warfare Requires,” *Taipei Chung-Kuo Shih-Pao*, 2 Sep 02, Description of Source: Taipei Chung-Kuo Shih-Pao (Internet Version-WWW) in Chinese -- Internet version of daily newspaper provides good coverage of political affairs,

A further blurring of the lines between civilian and government ties is the way the Chinese Communist Party will co-opt public use facilities and draft them into military service. Corporations in Western nations may contract to the government on issues of national defense but they are not drafted. In 2003, Dongshan District of Guangzhou China, one of the major science and technology centers in the Southern region, spent US \$54,000 to turn the provincial telecommunications company, data communications bureau, microwave communications bureau, and Southern Satellite Telecommunications Services Corporation into a militia information warfare battalion. While these public facilities were becoming an official unit in the militia battalion, others such as NetEase Guangdong and the China Unicom Paging Company in Guangzhou were being brought onboard even though they did not have an established mission.¹⁸⁵ The Guangdong area has been cited as one of the major areas for “government sponsored” hacking and the activities of groups such as these may be adding to the confusion of what is state organized and what is civilian.



Guangzhou

generally takes a pro-unification stance, translated by FBIS reference number *CPP20020913000193*

¹⁸⁵ Ye Youcai and Zhou Wenrui, “Building a High-quality Militia Information Technology Element,” *Beijing Guofang in Chinese*, 15 Sep 03, p 45, as translated by FBIS reference number *CPP20031002000138 Beijing Guofang in Chinese* -- monthly journal of the PLA Academy of Military Science, carrying in-depth articles on a wide range of military topics, often by significant authors. Map provided C.I.A *World Fact Book*, <http://www.cia.gov/cia/publications/factbook/geos/ch.html>

Communications

An interesting facet of the interaction between the government and the Red Hacker Alliance is the evolution in means of communications between the two. Without direct control over the daily workings of a group, how do you signal that they have crossed a line of departure and it is time to cease and desist certain activities? Turning once again to the cyber conflict of 2001 and also to the anti-Japanese protests of 2005, a picture begins to emerge of indirect communications through mass media, universities, text-messaging, and online postings. The ability to ensure compliance with these directives seems tenuous at best and may be aimed at keeping the situation under control rather than 100% observance.

When authorities in Beijing decided that the hacker war between China and the US had gone on long enough, they began issuing public statements and contacting leaders of the alliance telling them that it was time to stop. The opening government salvos came from a variety of sources aimed at getting their message across.

Official web site of the *People's Daily*:

*"The attacks by the Honker Union of China, or Red Guests, on US Web sites are unforgivable acts violating the law. It is Web terrorism."*¹⁸⁶

Liao Hong, the director of the *People's Daily Online* editorial office:

*"We understand the passion of these hackers but we do not endorse their way of expressing it. We do not want to offend patriotic Web surfers but it is important we alert the public to the risk of such acts and prevent further disasters."*¹⁸⁷

Officials from China's Internet security:

¹⁸⁶ Vivien Pik-kwan Chan, "HK: SCMP Report on PRC Officials Condemning Hacker Attacks," *Hong Kong South China Morning Post*, 8 May 01, FBIS reference number CPP20010508000067

¹⁸⁷ Ibid.

*"The war between Chinese and American hackers that led to the White House Web site being shut down was illegal."*¹⁸⁸

Spokeswoman for the Internet Safety Bureau, under the Public Security Ministry:

*"Such attacks are not legal. It is against the law to enter other people's systems."*¹⁸⁹

Su Zhiwu , Vice-president of the Beijing Broadcasting Institute:

*"Sino-US conflicts should be resolved through diplomatic channels, not hacking maneuvers."*¹⁹⁰

On 15 August 2001, Wan Tao, the leader of *China Eagle*, announced a temporary termination of attacks on foreign enemy web sites. According to *China Eagle*, this was based on instructions from government departments. In May of 2002, after negotiating an agreement with five other Chinese hacker web sites to include the *Honker Union of China*, a joint statement was issued calling for an end to anniversary attacks of the 2001 incident.¹⁹¹

From 2001 to 2005, the government gradually developed more sophisticated and expansive methods for communicating with its patriotic youth. Simple calls from recognized state newspapers and agencies were being supplemented with postings on web sites and text messaging. The Party had quickly grasped that traditional methods alone were inefficient at reaching a younger generation that felt more at home on the computer and who used cell phones to communicate with their peers.

Beginning on 9 April 2005, anti-Japanese demonstrations spread across China. Japan's bid for a seat on the United Nations Security Council and additional revisions to history textbooks that downplayed Japanese actions in WWII brought out large crowds of Chinese protestors. The demonstrations ranged across cities from Beijing to Shenzhen and were

¹⁸⁸ Ibid

¹⁸⁹ Ibid.

¹⁹⁰ Ibid.

¹⁹¹ Unknown, No Title, *China Eagle*, as downloaded on 9 Aug 2005 from <http://bbs.chinaeagle.org/archive/index.php/t-98075.html>

characterized by attacks on anything symbolic of Japan to include government buildings, cars, businesses, and restaurants. There were even reports of Japanese citizens being attacked during the protests.¹⁹²



Anti-Japanese Demonstrations in Beijing's Haidian District (see footnote 188)

Toward late April, the Ministry of Public Security was tasked with bringing the demonstrations to a halt. Utilizing Internet postings and text messages in combination with traditional print media, the ministry ordered protestors not to organize anti-Japanese demonstrations without police approval.¹⁹³ China's Minister of State Council Information summed up the Party's ability to control the populace:

"Most citizens obey no-demonstration orders. For example, a Beijing newspaper's warning against illegal demonstrations deterred all but a few hundred protesters from gathering for a second weekend of demonstrations in the capital last April. You need to understand that Chinese citizens still respect the

¹⁹² Ralph Jennings, "China Unlikely To Allow Repeat of Mass Anti-Japan Protests," *Tokyo Kyodo World Service*

4 Apr 06, FBIS reference number JPP20060404067014. Photo provided by Voice of America <http://www.voanews.com/english/archive/2005-04/2005-04-14voa17.cfm?CFID=44343444&CFTOKEN=36797897>

¹⁹³ Ibid.

*government. So if the government makes clear that this kind of demonstration is not OK, 90% of the people won't go.*¹⁹⁴

¹⁹⁴ Ibid.

Appendix I

Hacker/Internet Terminology

<http://hackbase.com/hacker/safety/2005070812361.html>

2005-7-8 Source China Network Management Union

1) 攻击	Gongji	Attack
2) 黑名	Heiming	Blacklist
3) 冲击波	Chongjibo	Blaster (Worm)
3) 攻破	Gongpo	Breach
4) 可破密的	Kepomide	Breakable
5) 基于 CGI 攻击	Jiyu CGI Gongji	CGI-based attack
6) 闯入	Chuangru	Crack
7) 赛博朋克	Caibo Pengke	Cyber Punk
8) 数据驱动攻击	Shuju Qudong Gongji	Data-Driven Attack
9) 字典式攻击	Zidianshi Gongji	Dictionary Attack
10) 拒绝服务	Jujue Fuwu	Denial of Service
11) 分布式拒绝服务	Fenbushi Jujue Fuwu	Distributed Denial of Service
12) 域名服务器 电子欺骗	Yuming Fuwuqi Dianzi Qipian	DNS spoofing
13) 窃听	Qieting	Eavesdropping
14) 淹没	Yanmo	Flooding
15) 黑客	Heike	Hacker
16) 砍客	KanKe	Hacker
17) 劫持终端	Jiechi Zhongduan	High Jacking
18) 伪装攻击	Weizhuang Gongji	Impersonation Attack
19) 入侵者	Ruqinzhe	Intruder
20) IP 欺骗	Qipian	IP spoofing
21) 逻辑炸弹	Loji Zhadan	Logic Bomb
22) 黑客帝国	Heike Diguo	Matrix (movie title)
23) 带外攻击	Daiwai Gongji	Out-of-Band Attack
24) 指控制电话 系统的过程	Zhi Kongzhi Dianhua Xitong De Guocheng	Phreaking

25) 扫描	Saomiao	Scan
26) 安全漏洞	Anquan	Security Loophole
27) 嗅探器	Xiutanqi	Sniffer
28) 探听	Tanting	Snooping
29) 垃圾邮件	Laji Youjian	Spam
30) 电子欺骗	Dianzi Qipian	Spoofing
31) 时间炸弹	Shijian Zhadan	Time Bomb
32) 泰坦雨	Taitan Yu	Titan Rain (FBI probe into Chinese hacking)
33) 骤雨	ZouYu	Titan Rain
34) 特洛伊木马	Teluoyi Muma	Trojan Horse
35) 木马	MuMa	Trojan Horse
36) 攻击向量	Gongji Xiangliang	Vector of Attack
37) 病毒	Bingdu	Virus
38) 脆弱性	Cuiruoxing	Vulnerability
39) 弱口令	Ruo Kouling	Weak Password
40) 蠕虫	Ruchong	Worm
41) 菜鸟	Cainiao	Novice Hacker
42) 网络钓鱼	Wangluo Diaoyu	Phishing
43) 域欺骗	Yu Qipian	Pharming
44) 模糊	Mohu	Fuzzing
1) 访问控制列表 (ACL)	Fangwen Kongzhi	Access Control List
2) 访问令牌	Liebiao	
3) 帐号封锁	Fangwen Lingpai	Access Token
4) 记帐策略	Zhanghao Fengsuo	Account Lockout
5) 帐号	Jizhang Celue	Account Policies
6) 适配器	Zhanghao	Accounts
7) 地址解析协议	Shipeiqi	Adapter
	Dizhi Jiexi Xieyi	Address Resolution Protocol (ARP)

8) 管理员帐号	Guanliyuan Zhanghao	Administrator Account
9) 算法	Suanfa	Algorithm
10) 别名	Bieming	Alias
11) 应用层	Yingyongceng	Allocation Layer
12) 应用程序	Yingyong Chengxu	Applications
13) 阿帕网	Apawang	ARPANET
14) 异步传递模式	Yibu Chuandi Moshi	Asynchronous Transfer Mode
15) 认证	Renzheng	Authentication
16) 授权	Shouquan	Authorization
17) 后端	Houduan	Back-End
18) 公司的一种 软件包	Gongsi De Yi Zhong Ruanjianbao	Back Office Microsoft
19) 备份	Beifen	Backup
20) 基线	Jixian	Baseline
21) 备份域控制器	Beifenyu Kongzhiqi	BDC (Backup Domain Controller)
22) 引导网关协议	Yindao Wangguan Xieyi	BGP (Border Gateway Protocol)
23) 基本输入/输出 系统	Jiben Shuru/Shuchu Xitong	BIOS (Basic Input/Output System)
23) 引导协议	Yindao Xieyi	BOOTP (Bootstrap Protocol)
24) 瓶颈	Pingjing	Bottleneck
25) 网桥	Wangqiao	Bridge
26) 浏览器	Liulanqi	Browser
27) 浏览	Liulan	Browsing
28) 只读型光盘	Zhiduxing Guangpan	CD-ROM
29) 校验和	Jiaoyanhe	Checksum
30) 密码	Mima	Cipher
31) 密文	Miwen	Cipher Text

32) A 类域	A Leiyu	Class A Domain
33) B 类域	B Leiyu	Class B Domain
34) C 类域	C Leiyu	Class C Domain
35) 无类地址分配	Wulei Dizhi Fenpei	Classless Addressing
36) 客户服务器	Kehu Fuwuqi	Client Server
37) 代码	Daima	Code
38) 组件	Zujian	Component
39) COM 口	COM Kou	COM port
40) 计算机名	Jisuanji Ming	Computer Name
41) 密码分析	Mima Fenxi	Cryptanalysis
42) 数据链路	Shuju Lianlu	Data-link
43) 数据链路控制	Shuju Lianlu Kongzhi	Data-Link Control
44) 数据库	Shujuku	Database
45) 数据报	Shujubao	Datagram
46) 解密	Jiemi	Decryption
47) 缺省文档	Queshang Wendang	Default Document
48) 缺省路由	Quesheng Luyou	Default Route
49) 缺省共享	Quesheng Gongxiang	Default Share
50) 数字键控系统	Shuzi Jiankong Xitong	Digital Key System
51) 目录	Mulu	Directory
52) 目录复制	Mulu Fuzhi	Directory Replication
53) 磁盘镜像	Cipan Jingxiang	Disc Mirroring
54) 分布式文件 系统	Fenbushi Wenjian Xitong	Distributed File System
55) 域	Yu	Domain
56) 域名控制器	Yuming Kongzhiqi	Domain Controller
57) 域名	Yuming	Domain Name
58) 域名服务器	Yuming Fuwuqi	Domain Name Server
59) 动态数据交换	Dongtai Shuju Jiaohuan	Dynamic Data Exchange
60) 加密通道	Jiami Tongdao	Encrypted Tunnel

61) 加密	Jianmi	Encryption
62) 企业网	Zhiyewang	Enterprise Network
63) 环境变量	Huanjing Bianliang	Environment Variable
64) 以太网	Yitaiwang	Ethernet
65) 外部网关协议	Waibu Wangguan Xieyi	Exterior Gateway Protocol
66) 外部安全性	Waibu Anquanxing	External security
67) 传真猫	Chuanzhenmao	Fax Modem
68) 文件属性	Wenjian Shuxing	File Attribute
69) 文件系统	Wenjian Xitong	File System
70) 过滤器	Guoluqi	Filter
71) 防火墙	Fanghuoqiang	Firewall
72) 固件	Gujian	Firmware
73) 分段	Fenduan	Fragments
74) 帧中继	Zhen Zhongji	Frame Relay
75) 文件传送协议	Wenjian Zhuansong Xieyi	FTP (File Transfer Protocol)
76) 图形设备界面	Tuxing Shebei Jiemian	GDI (Graphical Device Interface)
77) 全局帐号	Quanju Zhanhao	Global Account
78) 全局组	Quanjuzu	Global Group
79) 组帐号	Zuzhangho	Group Account
80) 图形用户界面	Tuxing Yonghu	GUI (Graphical User Interface)
81) 散表	San Biao	Hash Table
82) 硬件兼容性表	Yingjian Jianrongxing Biao	HCL (Hardware Compatibility List)
83) 高性能文件 系统	Gaoxingneng Wenjian Xitong	HPFS (High Performance File System)
84) 主目录	Zhu Mulu	Home directory
85) 竹叶	Zhuye	Home Page
86) 主机	Zhuji	Host

87) 超文本标记语言	Chaowenben Biaoji Yuyan	HTML (Hypertext Markup Language)
88) 超文本传送协议	Chaowenben Zhuansong Xieyi	HTTP (Hypertext Transfer Protocol)
89) 超文本链接	Chaowenben Lianjie	Hyperlink
90) 内部安全性	Neibu Anquanxing	IGP (Interior Gateway Protocol)
91) 信息服务器	Xinxiang Fuquqi	IIS (Internet Information Server)
92) 索引服务器	Suoyin Fuwuqi	Index Server
93) 继承权限 过滤器	Jichengquan Xian Guoluqi	Inherited Rights Filter
94) 内部安全性	Neibu Anquanxing	Internal Security
95) 解释程序	Jieshi Chengshi	Interpreter
96) 内联网	Neilianwang	Intranet
97) IP 地址	Dizhi	IP Address
98) IP 伪装	Weizhuang	IP Masquerade
99) 互连网分组协议	Hulian Wangfenzu Xieyi	IPX (Internet Packet Exchange)
100) 网上交谈	Wangshang Jiaotan	IRC (Internet Relay Chat)
101) 工业标准结构	Gongye Biaozhun Jiegou	ISA (Industrial Standard Architecture Bus)
102) 综合业务 数字网	Zonghe Yewu Shuziwan	ISDN (Integrated Services Digital Network)
103) 网络服务 提供者	Wanglu Fuwu Tigongzhe	ISP (Internet Service Provider)
104) 内核	Neihe	Kernel
105) 按键记录器	Anjian Jiluqi	Keystroke Recorder
106) 局域网	Juyuwang	LAN (Local Area Network)
107) 记录	Jilu	Log
108) 菜单	Caidan	Menu
109) 消息	Xiaoxi	Message

110) 网络接口卡	Wangluo Jiekouka	NIC (Network Interface Card)
111) 网络操作系统	Wangluo Caozuo Xitong	Network Operating System
112) 网络新闻传送协议	Wanglu Xinwen Zhuansong	NNTP (Network News Transfer Protocol)
113) 节点 node	Jiedian	Node
114) 开放数据库连接	Kaifang Shujuku Lianjie	ODBC (Open Database Connectivity)
115) 开放图形语言	Kaifang Tuxing Yuyan	Open Graphic Language
116) 分组过滤器	Fenzu Guoluqi	Packet Filter
117) 口令	Kouling	Password
118) 路径	Lujing	Path
119) 专用交换机	Zhuanyong Jiaohuanji	PBX (Private Branch Exchange)
120) 外设连接接口	Waishe Lianjie Jiekou	PCI (Peripheral Component Interconnect)
121) 个人通信业务	Geren Tongxin Yewu	PCS (Personal Communications Service)
122) 主域控制器	Zhuyu Kongzhiqi	PDC (Primary Domain Controller)
123) 对等	Duideng	Peer
124) 权限	Quanxian	Permissions
125) 点到点协议	Dian Dao Dian Xieyi	PPP (Point to Point Protocol)
126) 点到点隧道协议	Dian Dao Dian Suidao Xieyi	PPTP (Point-to-Point Tunneling Protocol)
127) 端口	Duankou	Port
128) 优先权	Youxianquan	Priority
129) 代理服务器	Daili Fuwuqi	Proxy Server
130) 伪随机	Weisuiqi	Pseudorandom

131) 远程访问服务	Yuancheng Fangwen Fuwu	RAS (Remote Access Service)
132) 远程引导	Yuancheng Yindao	Remote Boot
133) 远程控制	Yuancheng Kongzhi	Remote Control
134) 路由选择信息 协议	Luyou Xuanze Xinxi Xieyi	RIP (Routing Information Protocol)
134) 远程过程调用	Yuancheng Guocheng Diaoyong	RPC (Remote Procedure Call)
135) 路由	Luyou	Route
136) 路由器	Luyouqi	Router
137) 路由选择	Luyou Xuanze	Routing
138) 脚本	Jiaoben	Script
139) 搜索引擎	Suosuo Yinqing	Search Engine
140) 服务提供者	Fuwu Tigongzhe	Service Provider
141) 共享	Gongxiang	Share、Sharing
142) 安全标识符	Anquan Biaoshifu	SID (Security Identifier)
143) 站点	Zhandian	Site
144) 简单邮件 传送协议	Jiandan Youjian Chuansong Xieyi	SMTP (Simple Mail Transfer Protocol)
145) 电子欺骗	Dianzi Qipian	Spoofing
146) 结构化查询 语言	Jiegouhua Chaxun Yuyan	SQL (Structured Query Language)
147) 安全套接层	Anquan Taojieceng	SSL (Secure Socket Layer)
148) 独立服务器	Duli Fuwuqi	Standalone Server
149) 流密码	Liu Mima	Stream Cipher
150) 强密码	Qiang Mima	Strong Cipher
151) 强口令	Qiang Kouling	Strong Password
152) 子目录	Zimulu	Subdirectory
153) 子网	Ziwang	Subnet
154) 子网掩码	Ziwang Yanma	Subnet Mask
155) 交换文件	Jiaohuan Wenjian	Swap File

156) 传输控制协议/ 网际协议	Chuanshu Kongzhi Xieyi/Wangji Xieyi	TCP/IP (Transmission Control Protocol)
157) 远程登陆	Yuancheng Denglu	Telnet
158) 时间炸弹	Shijian Zhadan	Time Bomb
159) 用户数据报 协议	Yonghu Shujubao Xieyi	UDP (User Datagram Protocol)
160) 统一资源 定位器	Tongyi Ziyuan Dingweiqi	URL (Uniform Resource Locator)
161) 用户交流网	Yonghu Jiaoliuwang	Usenet
162) 用户名	Yonghu Ming	USER name
163) 用户帐号	Yonghu Zhanghao	USER account
164) 攻击向量	Gongji Xiangliang	Vector of Attack
165) 虚拟服务器	Xuni Fuwuqi	Virtual Server
166) 脆弱性	Cuiruoxing	Vulnerability
167) 广域网	Guangyuwang	WAN (Wide-Area Network)
168) 网页	Wangye	Web page
169) 隐写术	Yinxieshu	Steganography

Appendix II

Hacker Web sites

Name	URL
yaqu.315safe	http://yaqu.315safe.com/
redfox.88448	http://redfox.88448.com/
bbs.m01	http://bbs.m01.cn/
3her	http://www.3her.net/
3hack	http://www.3hack.com/
hack3	http://www.hack3.com/
s8s8	http://www.s8s8.net/
lgz8	http://www.lgz8.net/index.php
8way.be	http://www.8way.be/
hack8	http://www.hack8.cn/
vip8	http://vip8.org/
jc8	http://www.jc8.cn/
soo8.70bb	http://soo8.70bb.com/index.php
13age	http://www.13age.com/
17aq	http://www.17aq.com/
21cnlong.com/free/	http://www.21cnlong.com/free/
21safe	http://www.21safe.com/index.htm
25hack	http://www.25hack.com/
027safe	http://027safe.com/
27a.cn	http://www.27a.cn/
hack28	http://www.hack28.com/
hack51	http://www.hack51.com/
hack58	http://www.hack58.com/
66go	http://www.66go.net/index.html
66hack	http://www.66hack.com/
hack77	http://www.hack77.com/
hacker81	http://www.hacker81.net/
hack86	http://www.hack86.com/
cn90	http://cn90.net/
91one	http://www.91one.net/index.asp
hack95	http://www.hack95.com/

98exe <http://www.98exe.com/>
hack98 <http://www.hack98.com/>
hack099 <http://www.hack099.com/>
hx99 <http://www.hx99.net/>
safe110 <http://www.safe110.net/safe/>
cn110 <http://www.cn110.net/Index.html>
huo119 <http://www.huo119.com/>
hacker120 <http://www.hacker120.com/>
hacker121 <http://www.hacker121.com/bbs/>
hacker123 <http://www.hacker123.com/>
hk163 <http://www.hk163.com/>
muma163 <http://www.muma163.com/Index.html>
hack169 <http://www.hack169.com/>
315safe <http://www.315safe.com/>
361hack <http://www.361hack.com/bbs/index.php>
hacker365 <http://www.hacker365.com/>
520hack <http://www.520hack.com/>
520long <http://www.520long.com/bbs/index.php>
521hack <http://www.521hack.com/bbs/>
wxj521 <http://www.wxj521.com/>
hacker911 <http://www.hacker911.net/>
byx1763 <http://www.byx1763.com/Index.html>
2800cn <http://www.2800cn.com/>
d3389 <http://www.d3389.com/>
3800hk <http://www.3800hk.com/>
05112 <http://www.05112.com/>
7747.net <http://www.7747.net/>
9874 <http://9874.org/>
21169 <http://www.21169.com/>
77169 <http://www.77169.com/>
anqn <http://www.anqn.com/>
aomg.net <http://www.aomg.net/>
bbs.shhack <http://bbs.shhack.com/>
bdbase <http://www.bdbase.com/>
binkbase <http://www.binkbase.com/>
bitscn <http://www.bitscn.com/>

caomeng	http://www.caomeng.com/
cbhu	http://www.cbhu.org/
cchonker	http://www.cchonker.com/
ChinaEagle	http://bbs.neteasy.cn/
chinahacker.com	http://www.chinahacker.com/
chinahacker.net	http://www.chinahacker.net/
chinahksm	http://www.chinahksm.com/Index.htm
chinansa	http://chinansa.com/index.html
chinasu	http://www.chinasu.net/
chinesehackers	http://www.chinesehackers.com/
ciker	http://www.ciker.net/ciker/
cnhacker	http://www.cnhacker.cn/
cnhonke	http://www.cnhonke.com/
cnhonker	http://www.cnhonker.cn/Index.html
cnkinghack	http://www.cnkinghack.com/
cnlanker	http://www.cnlanker.org/
cnnsc	http://www.cnnsc.org/
cnsafer	http://www.cnsafer.com/index.html
cnsapc	http://www.cnsapc.com/
cntale	http://www.cntale.net/
cnxhacker	http://www.cnxhacker.net/
coolersky	http://coolersky.com/
crackshow	http://www.crackshow.com/bbs
cycycy	http://www.cycycy.net/
db.isbase	http://db.isbase.net/bbs/index.php
enet.com.cn	http://www.enet.com.cn/security/
eviloctal	http://www.eviloctal.com/
fanghei	http://www.fanghei.com/
guangzhilin	http://www.guangzhilin.com/
hackarea	http://www.hackarea.com/
hackba	http://hackba.com/2007/index.html
hackbase	http://hackbase.com/
hackblan	http://hackblan.com/index.html
hackboot	http://www.hackboot.com/index.asp
hackcao	http://www.hackcao.com/
hackcat	http://www.hackcat.net/bbs/index.php

hackchina	http://www.hackchina.cn/Index.html
hacker.cn	http://www.hacker.cn/
hacker.com.cn	http://www.hacker.com.cn
hacker.hkby	http://hacker.hkby.com/hacker/index.html
hackerbbs	http://www.hackerbbs.net/
hackercc	http://www.hackercc.net/?pUDXP=cjgjQ1GfhoJ1
hacker-cn	http://www.hacker-cn.com/index.html
hackeroo	http://www.hackeroo.com/
hackerxfiles	http://www.hackerxfiles.net/
hackfield	http://www.hackfield.com/
hackfocus	http://www.hackfocus.net/index.php
hackftp	http://wt.hackftp.com/forum/
hackhero	http://www.hackhero.com/
hackhome	http://www.hackhome.com/
hackol	http://www.hackol.com/index.html
hacksafe	http://www.hacksafe.org/
hackvip	http://www.hackvip.com/
hackway	http://www.hackway.cn/
hackwu	http://www.hackwu.com/
haisens	http://www.haisens.net/
heibai	http://www.heibai.net/
hhack	http://www.hhack.com/
hkonbluesky	http://www.konbluesky.com/Index.html
hmeng	http://www.hmeng.cn/
hnhack	http://www.hnhack.com/
hnhacker	http://www.hnhacker.com/
honkerbase	http://www.honkerbase.com/main.php
honkercn	http://www.honkercn.net/
honkerunion	http://www.chinahongker.com/index.asp
hookbase	http://hookbase.com/
huigezi	http://www.huigezi.com.cn/
hunke	http://www.hunke.com.cn/
icehack	http://www.icehack.com/
iceskysl	http://www.iceskysl.net/
ithack	http://www.ithack.net/
janker	http://www.janker.org/

jnhack	http://www.jnhack.org/tom/Index.html
juntuan	http://juntuan.net/
jztop	http://www.jztop.com/
kingti	http://www.kingti.com/
kker	http://www.kker.cn/index.asp
leftworld	http://www.leftworld.net/
lrbl	http://www.lrbl.net/
mmbest	http://www.mmbest.com/
mmwai	http://www.mmwai.com/Index.html
mumayi	http://www.mumayi.net/index1.htm
ncph	http://www.ncph.net/
netkox	http://www.netkox.com/
new.shockhack	http://new.shockhack.net/Soft/
newying	http://www.newying.com/
nohack	http://www.nohack.cn/bbs/
nschina	http://bbs.nschina.com/
nsfocus	http://www.nsfocus.net/index.php
nshacker	http://www.nshacker.com/
ntsky	http://www.ntsky.cn/
pccode	http://www.pccode.net/
polay	http://www.polay.net/polay.html
qqmuma	http://www.qqmuma.com/qqmuma.html
redhacker	http://www.redhacker.cn/
rednetcn	http://www.rednetcn.com/
sgmw	http://sgmw.net/
sjhack	http://www.sjhack.com/index.html
skyhk	http://www.skyhk.cn/
sollit	http://www.sollit.com/
sqcn	http://www.sqcn.net/index2.asp
stuhack	http://www.stuhack.com/
sun-lion	http://www.sun-lion.com/index.htm
syue	http://www.syue.com
tcsafe	http://bbs.tcsafe.com/
tech.ccidnet	http://tech.ccidnet.com/col/204/204.html
thysea	http://www.thysea.com/
ttian	http://www.ttian.net/

ttshjz	http://ttshjz.vxv.cn/
wghack	http://www.wghack.com/
wolfexp	http://www.wolfexp.net/
wolfol	http://www.wolfol.net/
wolvez	http://www.wolvez.org/index.htm
wrsky	http://www.wrsky.com/
xahack	http://www.xahack.com/
xfocus	http://www.xfocus.net.html
xinfeng	http://www.xinfeng.net/Index.html
xker	http://www.xker.com/
xzws	http://www.xzws.cn/
ygnet	http://www.ygnet.com.cn/
ynhack	http://www.ynhack.cn/
zkbbs	http://zkbbs.vxv.cn/

2Isafe, 100, 131
8th Group Army, 75
 Azuma Shiro, 23
 Bank, viii, 73, 87
 Beijing Green Alliance, 27
 blackmail, 3, 88
 blhuang, 36
 Brother Peng, 13
 Bundi Rahardjo, 18
 Chen Shuibian, 25
China Black Hawk Union, 58, 62
China Byte, 17
China Eagle, 5, 6, 14, 15, 32, 33, 34, 50, 62, 119
China West Hackers Union, 51
CHINAWILL, 14
 Chinese Embassy, 16, 48
Chinese government, 10, 107, 115
 Chong Yiu-kwong, 110
 Chu Tianbi, 11, 24, 25, 48
 CIH Virus, 15
 Coldface, 20
 communications, 16, 49, 81, 105, 117, 118
 Comprehensive National Power, 102
 Coolswallow, 6, 36
 Cult of the Dead Cow, 15
 culture, 2, 32, 39, 79, 92, 94, 97
 CyCyCy, 95
 defacement, 17, 20, 36, 41, 69, 71
 demographics, 52, 62, 95, 97
 Diaoyu Islands, 6, 41
 Dspman, 13
eBay, 83, 86
 espionage, 10, 103, 104, 107, 115
 Falun Gong, 109, 110
 Fox T.V., 36
Friendly Download Site, 66
 Gao Chunhui, 12, 49
 Glacier, 21, 66, 79
 Godfather. *See* Wan Tao
 Goodwill, 13, 20, 27, 29, 49
 government affiliation, 8, 102
 Gray Pigeon, 22, 66, 67, 69, 81, 91
 Green Army, 6, 12, 16, 20, 26, 27, 29, 49
 Green Power, 66
Hackbase, 53, 54, 55, 64, 68
HackerXfiles, 93
Hackol, 100
HackVip, 95
Hierarchy, vii, 57
 Hong Kong, 5, 21, 22, 62, 65, 109, 110, 111, 112, 115, 118
Honker Union of China, vii, 3, 5, 6, 35, 40, 42, 43, 44, 45, 47, 48, 49, 57, 62, 113, 118, 119
 Huang Xin, 21
Hx99, 76, 77
ICEHACK, 59, 60
 IceWater, 13
ige.com, 83
 Indonesia, 6, 16, 18, 48, 111
 Information War, 21
Iron and Blood Union, 9

Japanese, 6, 10, 22, 23, 24, 38,
 40, 41, 42, 77, 112, 115, 118,
 119, 120
Javaphile, 6, 36, 50
 Jay Chow, 91
 Jiaotong University, 36, 98
 Joseph Stewart, 108
KKER, 10, 12, 15, 17, 22, 52
 Korean, viii, 38, 73, 82, 86
 Li Zi, 13, 20
 Liang Huang. *See* blhuang
 Lin Yong. *See* Lion
 Lion, 6, 35, 42, 45, 48, 50, 112
Lite-On, 6, 36
 Little Rong, 13
 LittleFish, 13
 Mao Jieming, 82
 Marco Polo Bridge, 77
 Mark Sunner, 67
 Myfip, 79, 81, 108
 Nanjing Massacre, vii, 6, 22, 23
 nationalism, vi, 2, 9, 10, 48, 49,
 79
 NetSpy, 22
New Hacker Alliance of China,
 69
 NSfocus, 29
 oNe's wAr, 71, 72
 Peng Quan, 13
 People's Liberation Army, 3,
 77, 103, 104, 115
 people's war, 103, 104
 pornography, 97, 98, 100
 Power of the Night, 33, 34
 Qin Gang, 106
 reconnaissance aircraft, 36, 113
 recruiting, 3, 74, 113, 116
 Red Hacker Alliance, v, 3, 5, 6,
 8, 9, 10, 14, 16, 17, 18, 22,
 23, 26, 36, 38, 40, 41, 43, 48,
 49, 51, 53, 58, 62, 63, 65, 66,
 67, 69, 75, 76, 79, 93, 94, 95,
 99, 102, 103, 104, 105, 106,
 112, 114, 118
 Rocky, 13
 ROOT, 23
 Shanghai Green Alliance, 20,
 26, 27
 Sharp Winner, 18, 19, 29, 32,
 35, 41, 48, 93, 94
 Shen Jiye, 20, 27, 29
 Sky Talk, 25
 social engineering, 3, 80, 92
 Solo, 13
 Stephanie Sun, 90, 92
Student Hacker Union, 72, 73,
 74
 Taiwan, 6, 15, 18, 20, 21, 24,
 33, 38, 61, 63, 66, 70, 71, 87,
 107, 111
 thomasyuan, 36
 Tian Xing, 13
 Tibet, 109
 Trojan, 15, 21, 66, 67, 68, 73,
 79, 80, 81, 86, 87, 91, 92,
 108, 109, 115, 123
 Two-States-Theory, vii, 6, 20
 UK government, 69, 81
 US Embassy, 16
Voice of the Dragon, 6, 14, 49
 Wan Tao, 5, 6, 14, 15, 32, 49,
 112, 119

Whampoa Military Academy,
12
White House, 114, 119
William Callahan, 9
Xie Zhaoxia, 13
Xinjiang, 109
XSan, 22

YAI, 22
Yaqu163, 74, 76
Yasukuni Shrine, 38, 40
Zg77Hk, 77
Zhang Zhaozhong, 113
Zhou Shuai. *See* Coldface



The
Dark Visitor

Inside the World of Chinese Hackers

Scott J. Henderson