

University of Southampton Research Repository ePrints Soton

Copyright © and Moral Rights for this thesis are retained by the author and/or other copyright owners. A copy can be downloaded for personal non-commercial research or study, without prior permission or charge. This thesis cannot be reproduced or quoted extensively from without first obtaining permission in writing from the copyright holder/s. The content must not be changed in any way or sold commercially in any format or medium without the formal permission of the copyright holders.

When referring to this work, full bibliographic details including the author, title, awarding institution and date of the thesis must be given e.g.

AUTHOR (year of submission) "Full thesis title", University of Southampton, name of the University School or Department, PhD Thesis, pagination

University of Southampton
Faculty of Engineering, Science and Mathematics
School of Electronics and Computer Science

**An investigation into Chinese cybercrime and the
underground economy in comparison with the West**

By

Michael Yip

24th September 2010

A dissertation submitted in partial fulfilment of the degree of
MSc Web Science
by examination and dissertation

Supervised by
Dr. Craig Webber

Abstract

With 420 million Internet users, China has become the world's largest Internet population. In terms of Internet security, this implies that the security of the Internet in China has become globally significant. In this investigation, cybercrimes in China are studied from both sociological as well as technical perspectives. The paper begins with a study into the state of the Internet development as well as the state of Internet security in China. An introduction is also given on the rise of Chinese hacktivists, the politically motivated hackers in China. This is followed by a detailed account of a recent case of Chinese hacktivism against Japan which has brought to light some valuable insights into the true state of hacktivism in China and the level of tolerance of the Chinese government towards politically motivated hacking. A top-down approach was then used to study and compare frameworks of cybercrime in the West and in China. It was found that not only do organised cybercrimes exist in China but also an underground economy as sophisticated as that in the West is flourishing at a rapid pace. Furthermore, estimates from Chinese security experts suggest that the size of the Chinese underground economy may well be much larger than that in the West. Lastly, the Chinese underground economy was studied in details by looking at the common ways in which Chinese cybercriminals trade as well as the pricing of the commonly traded goods, which are compared against the West. It was found that in general, while carding merchandises are similarly priced in China and in the West, malware and technical support services are not.

Acknowledgement

I would like to sincerely thank Dr. Craig Webber, my project supervisor for his valuable feedbacks and guidance which helped me to make systematic progress.

I would also like to express my gratitude to the Serious Organised Crime Agency (SOCA) for kindly granting me access to invaluable information and providing me with continuous support throughout the project. This has allowed me to gain unique insights into the true nature of cybercrime.

Lastly, special thanks to Mr. Scott Henderson for his willingness to respond to my questions and consolidating my understanding about Chinese hackers and cybercrimes.

Table of Contents

Abstract	1
Acknowledgement.....	2
Chapter 1 Introduction	5
1.1 Project aim	6
1.2 Objectives.....	6
1.3 Organisation of thesis.....	6
Chapter 2 China and the Internet	7
2.1 Internet trends in China	7
2.2 Internet security in China	9
2.3 The rise of the Chinese cybercriminals	9
2.3.1 The Chinese hacktivists.....	10
2.3.2 The Chinese government and the hacktivists	12
2.3.3 A recent case study of Chinese hacktivism	14
2.3.4 Size of the hacking community in China	18
2.3.5 Emergence of cybercriminals.....	19
2.4 Cyber-regulations and law enforcements in China	20
Chapter 3 Framework of Cybercrime	21
3.1 Understanding cybercrime	21
3.1.1 Definition of cybercrime	21
3.1.2 Characteristics of cybercrime and the Internet.....	21
3.1.3 Typology of cybercrime	22
3.2 Comparison of organised cybercrime in China and the West	23
3.2.1 Case studies in China	23
3.2.2 Case studies in the West.....	25
3.2.3 Compare and contrast between China and the West	28
3.3 Organised cybercrime and the underground economy	29
3.3.1 Labour specialisation, deskilling and reskilling	29
3.3.2 The actors in the underground economy	29
3.4 Chains of need shapes the underground economy	36
Chapter 4 Understanding and Comparing the Underground Economy	37
4.1 Communication and advertising platforms	37
4.1.1 Baidu Tieba	38
4.1.2 QQ and QQ Group (群).....	41
4.1.3 Online forums (BBS)	44
4.1.4 Taobao.....	45

4.2	Advertised Goods and Services.....	45
4.2.1	Financial goods and services.....	46
4.2.2	Malware.....	47
4.2.3	Technical Support Services.....	48
Chapter 5	Conclusion.....	49
References	51
Appendix A	- Useful Chinese terms	54
Appendix B	– Carding merchandises.....	57

Chapter 1 Introduction

According to the Internet World Stats¹, the current total Internet population stands at around 1.9 billion. For those living in the developed countries, the Internet has become so embedded in our daily lives that it is difficult to live without it, or at the very least, the absence of it would be of a great disadvantage. For those with good intent, the Internet is an indispensable tool because it gives them an unprecedented level and speed of access to information. Unfortunately, the Internet has also become an indispensable tool for those with criminal intent. Not only has it given them the potential access to millions of Internet users spanning hundreds of countries, it has also removed traditional boundaries of crime, such as geographical and jurisdictional boundaries (Home Office 2010). This in effect generates new opportunities for crime. Indeed, the consumers are well aware of the threat of Internet crime, or *cybercrime*. 71% of consumers surveyed by CyberSource indicated their concern of the risk of online fraud and 50% still do not buy online (CyberSource 2010). Therefore, the advance in Internet security is critical to the growth of ecommerce.

Prior to the availability of the Internet, cybercrimes have been primitive in nature and low in volume. However, the Internet has created new opportunities for crime and the reach of the criminals have been vastly extended. As societies become more reliant on the Internet, the amount of personal data that resides on the network increases dramatically. The financially motivated cybercriminals recognise this opportunity and have subsequently shifted to stealthier attacks with the aim of stealing personal data. Traditional organised crime gangs who are always on the lookout for new profitable opportunities have also been attracted. As a result, a sophisticated underground economy of cybercriminals trading goods and services has emerged.

With 420 million Internet users, China has become the single largest Internet population in the world according to Internet World Stats. Astonishingly, the Internet penetration rate in China is only 31.6%, which means that the Chinese Internet population has the potential to triple in size in the foreseeable future. Just to give a clearer picture of the scale of the potential threat from China: the U.K. Internet population is just over 51 million but its Internet penetration rate is already at 82.5%. When China eventually achieves the same level of penetration, the present U.K. Internet population would be equivalent to just around 5% of the Chinese Internet population. One potential threat is the emergence of huge botnets² in China, ones that could be too great in size for some nations to handle. The tendency for Chinese botherders³ to launch DDoS⁴ attacks against the West, including the U.K., has already been documented in the works of Zhuge *et al.* (Zhuge 2007).

Perhaps due to the language barrier, while cybercrime in the West has been subject to intense study and research by the software vendors, security firms, law enforcement agencies and the academia, little attention has been paid towards cybercrime activities in China. As China is now the world's largest Internet population and the fact that cybercrimes have no bounds, the security of the Internet in China has profound implications on the global Internet. Therefore, it is the author's belief that in the interest for those responsible for cybersecurity, such as the Serious Organised Crime Agency (SOCA) the study of Chinese cybercrime and its underground economy is of both a critical and timely subject.

¹ Internet World Stats (06/09/2010) - <http://internetworldstats.com/stats.htm>

² **Botnet**: a botnet is a network of compromised machines (also known as zombies). Botnets are considered as the "Swiss Army knife of the underground economy" (Wilson 2008).

³ **Botherders**: they are people who manage one or more botnets.

⁴ **DDoS**: DDoS is an abbreviation for Distributed Denial of Service attacks, which are network attacks aimed at starving Web servers' resources and preventing them from operating normally.

1.1 Project aim

The aim of this project is to carry out an in-depth investigation into cybercrimes and the underground economy in China. The results are compared with the findings of the similar activities in the West. The thesis should serve as a valuable intelligence report for the cybersecurity industry.

1.2 Objectives

In general, the project seeks to answer the following questions:

1. What are cybercrimes?
2. What are the models of cybercrimes in the West? E.g. their core characteristics
3. Are there any cybercrimes in China? Are they individuals or well organised organisations?
4. What are the similarities and differences between the cybercrimes and the underground economy in China and others?

More precisely, the following questions should be answered upon the completion of the project:

1. What are the statistics of cybercrime incidents?
2. What is the state of the economy?
3. What are the motivations behind cybercriminals?
4. How do cybercriminals communicate? E.g. IRC channels, forums, QQ. Any popular/common venues for Chinese hackers?
5. Are there any particular “slangs” or specially crafted terms in the language the criminals use to communicate? They should be used in finding out relevant forums and identifying potential cybercriminals.
6. How do cybercriminals build trust?
7. What are the common distribution channels of stolen assets for hackers?
8. What are the common traded assets in the underground economy?
9. What are the characteristics of the underground economy in the different places?

1.3 Organisation of thesis

The remainder of the thesis is as follows. Chapter 2 documents the study of the current state of the Internet in China, the rise of the Chinese hackers as well as the Internet regulations. Chapter 3 provides a study of the nature of cybercrime and to compare and contrast frameworks of cybercrime documented in Chinese and Western literatures, including materials from SOCA. Chapter 4 documents a detailed study into the underground economy in China and compared with the Western underground economy. The thesis is concluded in chapter 5.

Chapter 2 China and the Internet

With a population of 1.3 billion people, China's economy has become the world's centre of attention. In the last ten years or so, it has made tremendous growth at a frightening pace. Similarly, although the Internet was only made publically available during the mid 1990s, China has now become the world's largest Internet population with 420 million Internet users and the penetration rate is only 32%. With such a large Internet population, the security of the Internet in China is now significant to the rest of the world.

In this chapter, an introduction is given about the state of the Internet in China including the characteristics of the Chinese Web and its state of security. An introduction is also given to the rise of the Chinese cybercriminals and their characteristics are compared with those in the West. Finally, an introduction is given to the Internet regulations in China and compared with those in the West.

2.1 Internet trends in China

Below are some of the highlights from the latest Internet development report (Dec. 2009 – June 2010) compiled by the China Internet Network Information Centre (CNNIC):

98.1% of Internet users in China accessed the Internet via a broadband connection. However, the connection speed may still be a problem, because according to Akamai, the average connection speed in China is only 695kbps. This is far lower than other large economies like the U.S. (4.6Mbps) U.K. (3.8Mbps) South Korea (12Mbps) and Japan (7.8Mbps) (Akamai 2010).

CNNIC reported that 277 million people accessed the Internet via a handheld device and the growth rate for mobile Internet exceeds that of those who access the Internet using desktop stations.

Characteristics of the Internet users

54.8% of the Internet users were male and 45.2% female. The age distribution is as shown in figure 1 below:

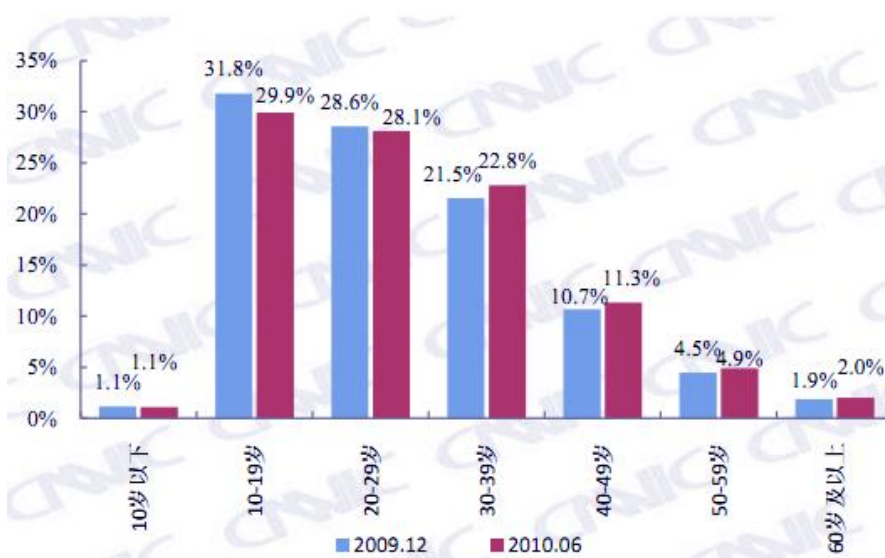


Figure 1 - age distribution of Chinese internet users 2010 (CNNIC 2010)

As shown in figure 1, 29.9% of the Internet users were aged 10 to 19 and 80.8% of Chinese Internet users were aged 10 to 39. Furthermore, the average age of Chinese Internet users is increasing and this can be seen by the fall in the percentage of Internet users aged 10 to 19 and 20 to 29 while there have

been increases in those aged 30 to 39, 30 to 39 and 50 to 59. This trend is echoed by both the U.K.⁵ and the U.S.⁶.

Students continue to dominate the Internet population in China with an increase from 28.8% to 30.7%. There is also a significant increase in the number of self-employed users, a rise of 3.7% in six months. This could be due to the booming economy and increasing opportunities for business start-ups. This is supported by over 50% fall in the number unemployed users.

The average monthly income distribution among the Internet users in China is as shown in figure 2 below:

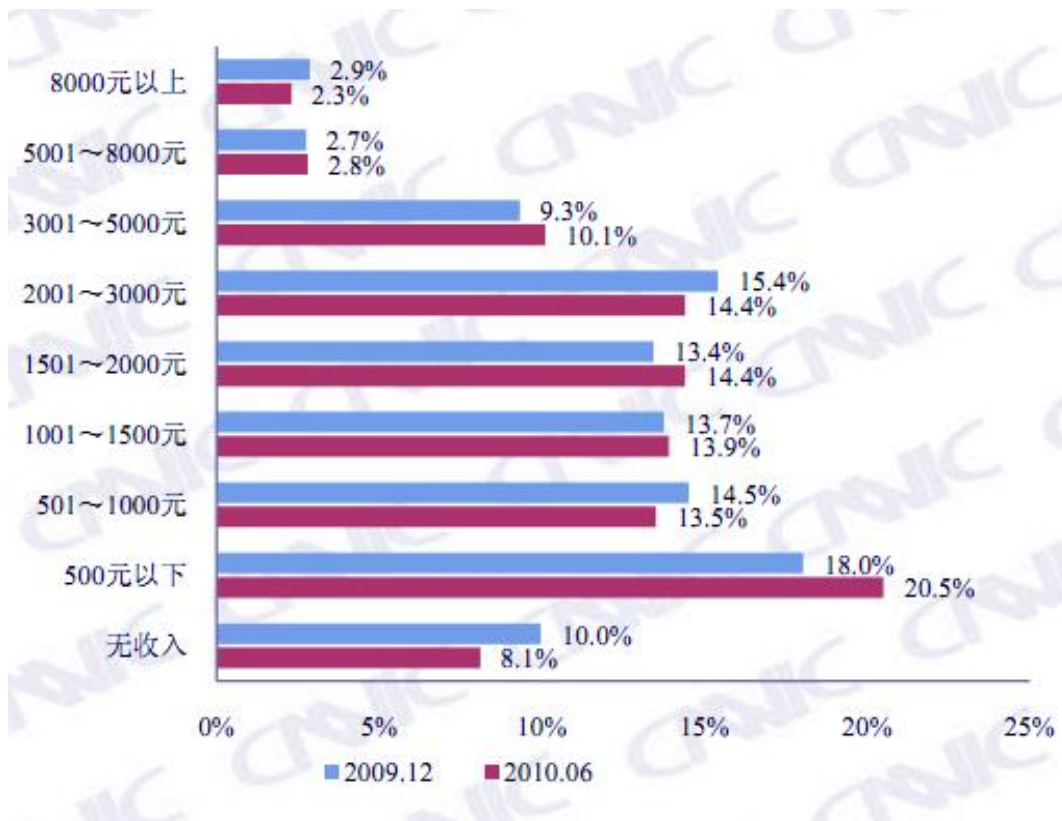


Figure 2 - average monthly income of the Internet users in China

Figure 2 shows that the most significant increase within this period lies in the number of Internet users with a monthly income of less than 500 RMB, an increase from 18% to 20.5%. 8.1% of the Internet users are still without income. This means that 28.6% of the users are with a monthly income of 500 RMB or less. Also, figure 2 show that 94.9% of the users have a monthly income of 5000 RMB (£479) or less. This is very low compared with developed countries like the U.K. where the average weekly income for full time employees is £489⁷.

Internet usage patterns

During this period, China saw significant growth in Internet commerce. There is a 36.2% increase in Internet payments, 29.9% increase in Internet banking, 31.4% increase in Internet shopping and

⁵ The ageing UK internet population - http://www.nielsen-online.com/pr/pr_071218_UK.pdf

⁶ Home Broadband Adoption 2009: Trends within demographic groups - <http://www.pewinternet.org/Reports/2009/10-Home-Broadband-Adoption-2009/2-Trends-in-broadband-adoption/2-Trends-within-demographic-groups.aspx>

⁷ Earnings: 2009 Annual Survey of Hours and Earnings - <http://www.statistics.gov.uk/cc/nugget.asp?id=285>

19.4% increase in travel bookings. 31.5% of users use bulletin board systems (BBS)⁸, an increase by 13.1% and 70.5% of users play online games, an increase of 11.9%.

2.2 Internet security in China

According to the 2009 China Netizen⁹ Information Security State Investigation Report (CNCERT/CC 2010) jointly compiled by CNCERT/CC and CNNIC, the state of Internet security in China is as follows:

In 2009, 95.6% of Internet users had security softwares installed but 4.4% were without. In other words, 18.5 million machines in China were left totally exposed to malware infections. This is of great concern as the machines could be infected to form botnets which could then be used to attack machines in other parts of the world.

Malicious websites remain to be the primary source of infection with 77.6% of victims reported malware infection during web browsing. The second most popular infection channel is through removable drives at 26.9%.

Interestingly, only 32.3% of infections resulted in the loss of QQ or email account logins, and 18.5% resulted in the loss of online game account logins. Only 2.5% resulted in the loss of online banking logins. One of the explanations for this is that approximately 46.6% of Internet users own some sort of virtual assets such as “QQ coins¹⁰” and online game accessories. This suggests that the theft of virtual assets is more prominent in Chinese cybercrime than financial related crimes.

According to 2009 Internet Security report¹¹ by Kingsoft Security¹², there were approximately 76 million machines infected in 2009, an increase of 13.8% from 2008. 2009 saw a 49% increase in the number of new virus and Trojans detected. Symantec also reported a sharp rise in the number of new types of malware detected in 2009, an approximately 71% increase over 2008 (Symantec 2010).

Lastly, Kingsoft reports that large scale high profile infection attacks are decreasing and attackers are choosing to use stealthier attacks. Again, this is echoed by the findings of Symantec (Symantec 2010). Attackers have gradually changed to stealthier infection tactics such as placing fraudulent download links, malicious redirections and browser hijacking.

2.3 The rise of the Chinese cybercriminals

Chinese hackers are frequently speculated in the West as being the masterminds behind cyber-attacks against foreign targets, the most recent high profile case being the attacks against Google CN. They are often portrayed as mystical and invisible, generating fear among Western nations. In this section, a short introduction is given on the rise of the Chinese hackers and how the Chinese hacking community evolved from a few highly skilled hacktivists¹³ to a generation of cybercriminals.

⁸ **Bulletin board systems (BBS):** they are equivalent to online forums

⁹ Netizen is a popular label used to refer to the Internet users in China

¹⁰ QQ is China’s most popular instant messenger service and “QQ coin” is their virtual currency.

¹¹ 2009 China Computer Virus Infection State and Internet Security Report -

<http://www.cnetnews.com.cn/2010/0128/1615976.shtml>

¹² Kingsoft Security is one of China’s most popular Internet security software vendors. See:

<http://www.duba.net/>

¹³ **Hacktivists:** politically motivated hackers

2.3.1 The Chinese hacktivists

“Many young people are first enticed into cybercriminality by intrigue, by the challenge and by the promise of getting something for nothing” (McAfee 2006). The Chinese hackers are no different.

According to Scott Henderson¹⁴, the origin of Chinese hacking began in the mid-90s, as soon as the Internet was made available to the public (Henderson 2007). 1997 saw the emergence of two prominent hacker groups:

- **Green Army**: formed by a hacker from Shanghai called Goodwill. It is reported to have had around 3000 members. The Green Army is said to have hacked an uncountable foreign websites and many of China’s best hackers were members of this group. This group disbanded in 2000 (Henderson 2007). However, during this study, a popular hacker forum Isbase uses the exact same Chinese name which has 66,437 members (as of 14/09/2010).
- **China Eagle Union**: founded by a person named Wan Tao, this group began in 1997 under the name Chinawill. Wan Tao then officially founded the China Eagle Union in 2000.

These hackers groups were comprised mainly of males in their 20’s and with the Internet, they were the few armed with the ability to voice their opinion and protest against national humiliations. This sense of nationalism stems from a century of national humiliation, as described by Callahan:

“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. Chinese books on the topic generally tell the tale of China going from being at the centre of the world to being the Sick Man of Asia after the Opium War (1840) only to rise again with the Communist Revolution (1949)...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’.” (Callahan 2004).

The Chinese hacktivists, also known as “honkers”, finally got the chance to show the world their abilities when anti-Chinese riots were held in Indonesia in 1998. Outraged by the events, the hacker groups were united under a common goal and they jointly formed the “Chinese Hacker Emergency Conference Center”. They sent email bombs to the Indonesian government websites and mailboxes as well as carrying out DDoS attacks against Indonesian domestic websites. Their actions gain the attention of the chief-editor of *China Byte*¹⁵ and the news began to viral amongst the subscribers and eventually made it to newspapers headline. This event is one of the most significant events in China’s history of hacking as it has shown the hackers that their attacks really did make an impact and they were not forced to swallow indignation (Henderson 2007). This marks the beginning of a hacking alliance with a sacred duty to protect the country’s interests as well as dignity in the face of humiliation.

Another significant event was the cyber conflict with Taiwan in 1999. It was launched in response to Taiwan’s “Two states theory”. It is in this event which saw the first Chinese-made malicious software, called the “Glacier” Trojan. It is claimed that Glacier is the inspiration behind other malware such as the infamous *Huigezi* Trojan. Chinese hackers no longer had to rely on foreign hacking tools.

¹⁴ Scott Henderson is a retired language expert in the U.S. Army and is now working in open source intelligence.

¹⁵ China Byte – one of China’s leading IT media and wireless service providers. See: <http://www.chinabyte.com>

The year 2000 saw a major change in the hacktivist community. The Green Army broke up in the heat of commercialisation. Due to the naming convention, it is believed that the offsprings of the Green Army went on to form the security firm *NSFocus*¹⁶. Furthermore, several large hacker groups emerged:

- **Honker Union of China (HUC)**: founded by a hacker operating under the online name Lion (his real name is Lin Yong). At the height of popularity, it is reported that there were as many as 80,000 members in this group. However, this group was disbanded by Lion in late 2004 as he believed the group no longer hold the same passion as in the beginning (Henderson 2007). During this study, it was found that some suggests Lion disbanded HUC because it was being monitored by the government. Perhaps due to the significance of its name, there are two forums using this name, as shown in figures 3 and 4 below:



Figure 3 – the forum of *cnhonkerarmy* (<http://www.cnhonkerarmy.com>)



Figure 4 – the BBS of the Honker Union of China (<http://www.honker.net>)

- **Javaphile**: this group was founded by a hacker named Coolswallow and all members were said to be students of Jiaotong University in Shanghai. Javaphile is behind the defacement of Lite-on and Fox T.V.. This is the same university accused of being involved in the attacks

¹⁶ NSFocus - <http://www.nsfocus.com/>

against Google CN back in January 2010¹⁷. Allegedly, Coolswallow is now an information security consultant for China's Public Security Bureau¹⁸.

It is important to distinguish the Chinese honkers from hackers because honkers have a strict code of conduct on not hacking within China. They see themselves as different from the hackers. Figure 5 below shows a recent post on honker.net announcing the banning of a member for hacking within China:



Figure 5 - banning a honker for hacking within China

2.3.2 The Chinese government and the hacktivists

There have been many speculations by the Western media about a direct link between the Chinese government and the hacking community. To date, there is no conclusive evidence which shows that the Chinese government is the mastermind behind the reported attacks.

Recently, the Information Warfare Monitor carried out network forensic examinations on the infected Tibetan computer systems and found that some command and control servers used in the attack were located in China (Information Warfare Monitor 2009) and (Information Warfare Monitor 2010). Furthermore, there is little doubt that China is the biggest strategic beneficiary to the stolen documents from the targeted machines. Interestingly, an email address used to register a domain name (lookbytheway.net) utilised by the command and control servers was traced by Henderson as having also been used to register accounts on hacker forums such as *Xfocus*¹⁹ and *Isbase*²⁰. The individual is

¹⁷ Chinese schools deny link to Google attack - <http://www.reuters.com/article/idUSTRE61I0OS20100221>

¹⁸ Javaphile, Buddhism, and...The Public Security Bureau? -

<http://www.thedarkvisitor.com/2007/12/javaphile-buddhism-andthe-public-security-bureau/>

¹⁹ XFocus - <https://www.xfocus.net/bbs/index.php?lang=cn>

²⁰ Isbase - <http://bbs.isbase.net/>

born on July 24, 1982, lives in Chengdu, Sichuan and attended the University of Electronic Science and Technology of China. Interestingly, Chengdu is also the location of one of the People's Liberation Army (PLA)'s technical reconnaissance bureaus tasked with signals intelligence collection (Information Warfare Monitor 2010). While the findings do not link the Chinese government with the foreign hacking incidents, they nonetheless show an obvious link to the Chinese hacking community.

However, according to a report for the U.S.-China Economic and Security Review Commission, there are several reasons why hacker groups would not be part of formal PLA plans as part of a computer network operation (CNO) campaign in wartime:

- **Command and Control:** the lack of an easily implemented command and control structure from the PLA to the hacker community makes guiding or directed attacks extremely difficult.
- **Precision targeting:** hacktivist target selection is generally based on political or nationalist symbolism and not on an alignment with real or perceived PLA campaign objectives and may actually hinder PLA operations or intelligence gathering.
- **Indications and warning:** surprise and deception are central to successful attacks but the hacker groups are mostly public (Krekel 2009).

Even though it is unlikely that the hacking community would be a formal part of the PLA's plan, their presence and actions such as the attacks on the Tibetans are nonetheless beneficial for the government. This suggests that the Chinese government would continue to hold such informal relationship with the hacking community. Henderson suggests that the Chinese government tends not to prosecute hackers unless they attack within China²¹. This is evident in a recent case of hacktivism against Japan which is documented in the following section.

Lastly, there is evidence which shows that the Chinese government are becoming increasingly active in closing down hacker forums, especially those disseminating hacking tools. This is in line with China's announcement of tough tackling on cybercrime (IOSC 2010).

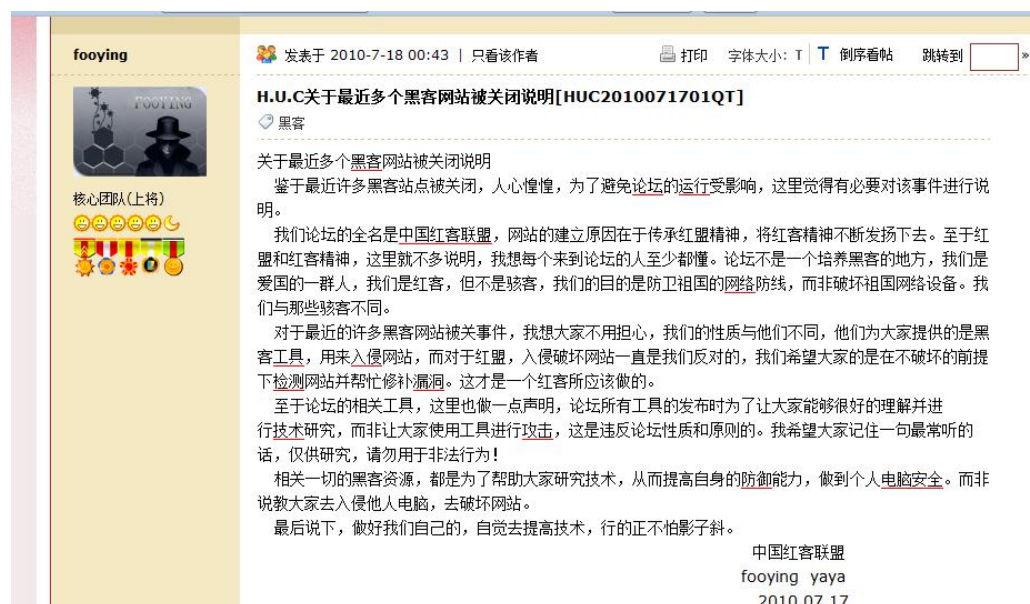


Figure 6 - reassurance with regards to recent crack down on hacker forums

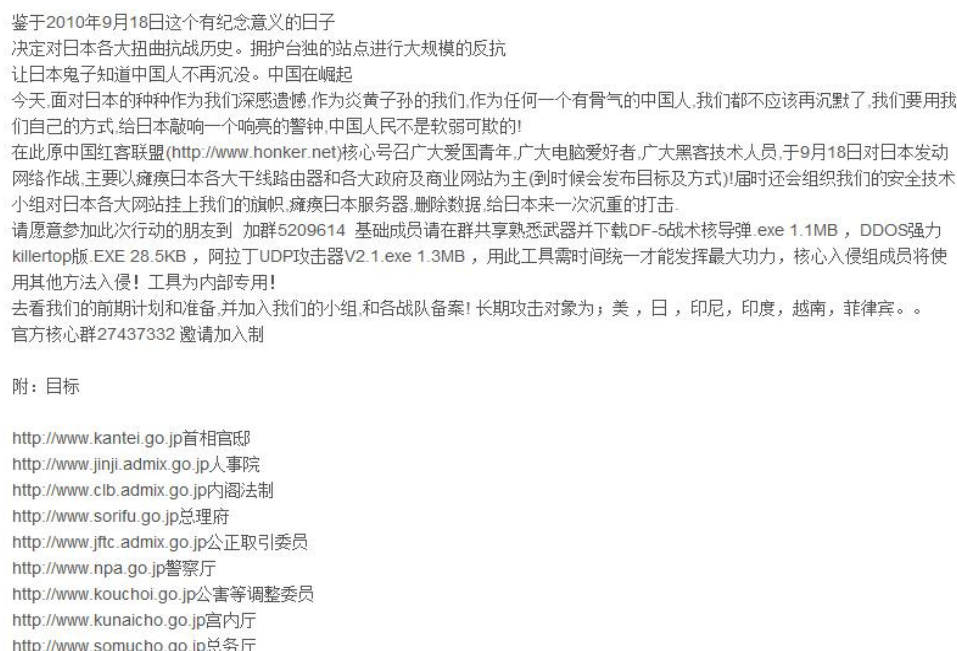
²¹ Chinese Hacker "Community" exposed - <http://www.darkgovernment.com/news/chinese-hacker-community/>

Back in February 2010, the Chinese government closed one of the most popular hacker forums called “Black Eagle”. The reason was that the forum had been offering training to some 12,000 hackers and had received more than 7 million RMB (US\$1 million) from training provision²². However, it was found that the “Black Eagle” forum is now back online. In July, a large number of hacker forums were also closed down. It was so significant that a prominent member of the Honker Union of China made an announcement (figure 6) to the members to reassure them that they should have nothing to worry about because they are different from the other hackers and the forum has always discouraged people from malicious hacking.

2.3.3 A recent case study of Chinese hacktivism

On the 8th September 2010, the captain of a Chinese fishing trawler was held by the Japanese after a collision with two Japanese patrol vessels, near the highly sensitive Diaoyu Island in the East China Sea²³. Predictably, this incident has drawn the attentions of some Chinese hacktivists.

Since the incident, there have been several rumours about launching cyberattacks against Japan. Interestingly, an advert²⁴ (figure 7) was found to have been widely disseminated across Chinese forums rallying Chinese hacktivists into participating in a coordinated attack on 18th September 2010.



鉴于2010年9月18日这个有纪念意义的日子
决定对日本各大扭曲抗战历史。拥护台独的站点进行大规模的反抗
让日本鬼子知道中国人不再沉没。中国在崛起
今天 面对日本的种种作为我们深感遗憾,作为炎黄子孙的我们,作为任何一个有骨气的中国人,我们都不应该再沉默了,我们要用我们自己的方式,给日本敲响一个响亮的警钟,中国人民不是软弱可欺的!
在此原中国红客联盟(<http://www.honker.net>)核心号召广大爱国青年,广大电脑爱好者,广大黑客技术人员,于9月18日对日本发动网络作战,主要以瘫痪日本各大干线路由器和各大政府及商业网站为主(到时候会发布目标及方式)!届时还会组织我们的安全技术小组对日本各大网站挂上我们的旗帜,瘫痪日本服务器,删除数据,给日本来一次沉重的打击。
请愿意参加此次行动的朋友到 加群5209614 基础成员请在群共享熟悉武器并下载DF-5战术核导弹.exe 1.1MB, DDOS强力killertop版.EXE 28.5KB, 阿拉丁UDP攻击器V2.1.exe 1.3MB, 用此工具需时间统一才能发挥最大功力,核心入侵组成员将使用其他方法入侵! 工具为内部专用!
去看我们的前期计划和准备,并加入我们的小组,和各战队备案! 长期攻击对象为:美,日,印尼,印度,越南,菲律宾。。
官方核心群27437332 邀请加入制

附: 目标

<http://www.kantei.go.jp>首相官邸
<http://www.jinji.admix.go.jp>人事院
<http://www.clb.admix.go.jp>内閣法制
<http://www.sorifu.go.jp>总理府
<http://www.jftc.admix.go.jp>公正取引委员
<http://www.npa.go.jp>警察厅
<http://www.kouchou.go.jp>公害等调整委员
<http://www.kunaicho.go.jp>宫内厅
<http://www.somuchou.go.jp>总务厅

Figure 7 – advert rallying hacktivists to participate in a coordinated attack against Japan on cfdd.org.cn

It is claimed on the advert that the rally comes from the founding members of the Honker Union of China (<http://www.honker.net>) and the aim of the attack is to “hang the flag of the nation” on various large Japanese websites, to disrupt their servers and to destroy databases, thereby punishing the Japanese for their actions. The advert in figure 7 is believed to be the original post and it was found on a forum dedicated for protecting Diaoyu Island.

²² Hubei cyberpolice successfully closed down China’s largest hacker training website - <http://news.qq.com/a/20100206/001649.htm>

²³ Japan arrests Chinese skipper intense maritime row - http://news.yahoo.com/s/afp/20100908/wl_asia_afp/chinajapanmaritimeincidentdiplomacy_20100908041734

²⁴ Founding members of Honker Union of China: 9.12 – 9.18 coordinated attack announcement - <http://www.cfdd.org.cn/bbs/thread-71680-1-1.html>

Three interesting details are also specified:

1. QQ groups (#5209614, #5210969 and core group #27437332) are setup to coordinate the attacks. A channel on a team voice tool called YY²⁵ is also setup.
2. Novices are also invited to participate in the attack by using ready-made tools which are claimed to be available in the QQ groups specified above.
3. A long list of targeted Japanese websites is published. The list includes many official websites such as the Japanese Ministry of Justice, the Prime Minister and His Cabinet as well as the Fire and Disaster Management Agency. Large corporate websites are also in the list.

The author of the thesis has attempted to join the QQ groups but two groups (each with a maximum of 100 members) were already full and membership in the core group is by invitation only.

Interestingly, as shown in figure 7 below, the administrator of the forum Honker Union of China (<http://www.honker.net>) denies making such rally call and discourage people from participating because real attacks are carried out silently, not publicised as shown. He believes that defacing websites is of very little benefit to China. Rather, stealthier attacks such as infiltration and spying have a much greater value. Finally, he believes that such attacks would only give other governments the excuse to increase funding for cyber-defence, such as the U.S.. Subsequently, the author of the thesis went on to try and verify the source of the advert in figure 7. By browsing through the “Red hacker” bar²⁶ on Baidu Tieba, it seems clear that the advert is the work of an individual or a minority of hackers.



Figure 8 – denial of rally call by Honker Union of China

However, this is not the only initiative on attacking Japanese websites. There is another Chinese hacktivist forum (<http://www.cnhonkerarmy.com>), which although they does not use the name Honker Union of China, their logo does bear the initials HUC. On the 13th Sept 2010, this group claim to have already attacked and defaced several Japanese websites and they have even displayed their work like a trophy:

²⁵ YY team voice tool - <http://yy.duowan.com/>

²⁶ “Red hacker” bar, Baidu Tieba - <http://tieba.baidu.com/f?kw=%BA%EC%BF%CD>



Figure 9 - showcasing the defacement of a Japanese website on cnhonkerarmy

The hackers of *cnhonkerarmy* defaced websites by changing the homepage to a page as shown above. The page clearly indicates that the website has been hacked by *cnhonkerarmy*. The page also demands an official apology from the Japanese government and at the bottom of the page reads a line “The war was left unfinished 5 years ago, we will continue the fighting. This is just a little warning, Japan please self-respect”.



Figure 10 - *cnhonkerarmy* forum under DDoS attack from Japan

From various sources on the Chinese web, it was found that the *cnhonkerarmy* forum was only launched a few months ago. However, it appears that they are actually the same group of hackers who launched a cyber-attack against the Japanese back in July 2005²⁷. The group disbanded some time after the attack in 2005 but has now regrouped.

²⁷Honker Union of China announcing war on Japan - <http://paper.wenweipo.com/2005/07/29/CH0507290047.htm>

On 14th Sept. 2010, the administrator of *cnhonkerarmy* claimed that the forum has been under a heavy DDoS attack and the origin of attack has been traced back to Japan as shown in figure 10 above. While the author of the thesis was attempting to access a page on the forum on the same day, an “out of memory” error was given, as shown in figure 11 below. This suggests that the load on the server was being strained, possibly by a DDoS attack.



Figure 11 - "out of memory" error given while accessing *cnhonkerarmy*

On 15th Sept. 2010, a member of the HUC technical team made an announcement claiming that their attack which began on the 12th Sept., was a tremendous success. This is shown in figure 12 below.



Figure 12 - *cnhonkerarmy* claiming their cyberattack on Japan as a tremendous success

They also claimed that despite suffering some losses of their own, their goal was achieved nonetheless. Most importantly, they claimed that the Chinese government has intervened under increasing pressure from foreign countries and media. Subsequently, the groups have decided to temporarily pause all attacks on Japan to avoid giving foreign countries the excuse to attack China.

On 22nd Sept. 2010, it was found that both *honker.net* and *cnhonkerarmy.com* have been taken down. Although the exact reasons are unknown, it is reasonable to assume that they have been taken down by the Chinese government due to the increasing pressure from foreign media.

There are several implications from the above findings:

- Hacktivism in China is active and hacktivists are easily rallied by public announcements
- QQ groups and the YY team voice tool are popular tools to be used for coordination
- There has not been any clear evidence of a widespread collaboration between the hacker groups to attack Japan. One possible reason is the increased level of monitoring by the Chinese government agencies.

- This is evidence demonstrating the Chinese government willingness to intervene with cyberattacks from hackers. However, the group has not made any claim that any participant has been arrested as a result of the attack which shows government leniency.

Finally, findings from the observations above share some similarities with the Russian hacktivists:

- When attacks are arranged, the necessary attack tools are disseminated in order to allow novice hackers to participate
- Novices are encouraged into participation by being exposed to patriotic materials
- List of targeted websites is published
- Coordination and discussion prior to attack including the selection of tools (Project Grey Goose 2008)

2.3.4 Size of the hacking community in China

To get an idea of the size of the hacker community in China, Henderson carried an investigation in 2006 and subsequently concluded with an estimation of approximately 380,000 active hackers in China with a lower limit of around 24,000 and an upper limit of 1.2 million (Henderson 2007).

To get an updated view, the author of this thesis examined some 19 forums by following the affiliated links on the forums. The findings were as below:

URL	Registered?	No. of registered members	Highest no. of online users
http://hackbase.com	n	1,111,335	11000
http://bbs.77169.com	n	956,715	12739
http://bbs.hmwz.net/	y	432,922	N/A
http://bbs.mmbest.com/index.php	y	254,969	5500
http://www.eviloctal.com	y	204,496	10875
http://bbs.neteasy.cn	y	134,109	2213
http://bbs.honker.net	y	80,543	5500
http://www.patching.net/bbs/	n	78,718	N/A
http://bbs.isbase.net/	n	66,437	5500
http://www.hx99.net/bbs/	y	52,940	714
https://www.xfocus.net/bbs/	y	51,249	5433
http://yeshack.com	y	45,265	3061
http://bbs.7747.net	y	35,649	4463
http://www.hack95.com/	n	29,874	3463
http://www.3800-hk.cn/	y	23,409	1226
http://www.hackersa.org/	y	16,760	9122
http://bbs.hackvip.com	y	14,019	815
http://bbs.myhack58.com/	n	13,364	15220
http://www.cnhonkerarmy.com/index.php	y	9,460	592
	Total	3,612,233	97436

Table 1 – membership in hacking forums in China

As shown in table 1, there are around 3.6million registered users amongst the 19 forums studied. While this is by no means an accurate reflection of the true size of the hacker community due to the possibility of duplicate memberships held by an individual as well as the inactive users, it nonetheless

does reflect the popularity of hacking in China. The number of online users at any one time also suggests that there are potentially a high number of active hackers in China. Lastly, the popularity of *Hackbase* and the fact that it has stopped taking in new members suggests that the demand for membership affiliation with a reputable hacking group is so high it is almost cult-like in China. This further highlights the popularity of hacking in China.

2.3.5 Emergence of cybercriminals

One can begin to see why Chinese cybercriminals have emerged by comparing the average income between countries. As stated in section 2.1, 94.9% of the Internet users in China have an average monthly income of less than 5,000 RMB (£479), equivalent to the average weekly salary in the U.K.²⁸. This is comparable to Russia where the average monthly wage in Moscow is officially only around 17,000 rubles (£360) per month (Jellenc 2007).

Also, just like their Russian counterparts, the Chinese I.T. employees are generally better off than most in the economy. According to CNET²⁹, the average monthly income for a programmer with 2-3 years of experience is 3,000 to 6,000 RMB (£286 to £573). This varies between provinces and industry. Those in game development could earn as much as 8,000 to 10,000 RMB per month (£764 to £955). A programmer working in larger corporations with 5 years experience typically earns between 12,000 to 15,000 RMB per month (£1,146 to £1433). Assuming £1,433 is an above average salary in the Chinese I.T. industry then an above average annual salary for a Chinese I.T. employee is £17,196. This is almost twice as low as their counterparts in the U.K., who on average earns £35,000 per year.

Obviously, one may suspect if there is such a big difference in the average income between the countries, perhaps the price of the goods sold would also differ by similar margins. This is not always the case. E.g. the price for a 13" Macbook Pro 2.4 GHz³⁰ costs 9,498 RMB (£908) in China and the exact same model costs £999³¹ in the U.K..

Furthermore, it has been widely reported that some Chinese cybercriminals, normally in their late teens to early 20's, are making as much as 50,000 RMB (£4,778) per month and a zero-day exploit³² can be sold for as much as a million³³.

Lastly, the education system in China is similar to that in Russia where strong emphasis has been placed on computer related subjects like Mathematics and Science, perhaps stemming from their common Communist root. According to Li *et al.*, the Chinese students also appear to be more confident with computers than their U.K. counterparts although the sample size in the study may have been too small to be conclusive (Li 2005). The Chinese dominance in top three finishing of the International Olympiad in Informatics in 2007 and 2008 also reflects their proficiency with informatics.

Therefore, with an average salary much lower than that of their Western counterparts, who some may perceive as intellectually inferior, and coupled with factors such as distance from victim and falling

²⁸ Earnings: 2009 Annual Survey of Hours and Earnings - <http://www.statistics.gov.uk/cci/nugget.asp?id=285>

²⁹ Which level are you at? An investigation on the state of survival for the IT people - <http://www.cnetnews.com.cn/2010/0311/1659908.shtml>

³⁰ MacBook Pro (CN) - <http://www.apple.com.cn/store/macbookpro/>

³¹ MacBook Pro (UK) http://store.apple.com/uk/browse/home/shop_mac/family/macbook_pro

³² Zero-day exploit: a zero-day exploit refers to a vulnerability in an application not yet noticed by the developers

³³ Uncovering the Internet Gang's Chinese Landscape: an 18 year old hacker's lavish lifestyle - <http://tech.163.com/09/0608/00/5B8D91KT000915BF.html>

skills required in committing cybercrime (Wall 2008), it really is no surprise that to see the emergence of cybercriminals and a flourishing underground economy in China.

2.4 Cyber-regulations and law enforcements in China

According to Qi *et al.*, the first piece of Chinese legislation on cybercrimes was enacted in 1997 and it is the Criminal Law of the People Republic of China which provides the basis of conviction and punishment. The cybercrime-related articles in the Law are 285, 286 and 287.

Other relevant regulations include:

- “Regulations on protecting the safety of computer information”, 1997
- “Regulations on State Secrets Administration for International Networking of Computer Information Systems”, 2000
- “Decision of by the State Committee of the National People’s Congress Concerning Maintaining Internet Security”, 2000

According to Qi *et al.*, there are several notable shortcomings with the laws and regulations documented above. Firstly, the punishment laid out by the Criminal Law fails to correlate proportionately with the tremendous social harm as the result of the cybercrimes. Secondly, the law offers little protection for rights of the individual users or networks. They concluded that cybercrime legislation in China is still in the very early stages of development and more specific laws targeting cybercrimes should be considered.

According to Yong, Article 286 in the Criminal Law fails to take into account data that is stored outside of the computer information system, such as on removable drives. Therefore even if the consequences are serious, this conduct cannot be punished in accordance to the Article (Yong n/a).

Another problem with Article 286 is its definition of “destructive programmes” which fails to take into non destructive programmes such as Trojans which do not necessarily affect the normal operation of the computer system. This may contribute to the reason why data stealing is becoming more prominent than high profile virus infections.

However, China is not the only nation with an insufficient legal framework against cybercrime. Due to the evolving natures of cybercrime, legal frameworks are needed to be constantly updated to be sufficient (Peiravi 2010).

With regards to law enforcement, Lu *et al.* made an interesting comparison of cybercrimes and governmental law enforcement in China and the United states. “China has historically been a communitarian society where individual rights typically yield to the interests of the community and society, which is a direct contrast with the more individualistic ideology in the U.S.” (Lu 2010). Moreover, they found that due to China’s communitarian orientation, Chinese authority is much more receptive to informal social control than the U.S. where formal social control is preferred. Lastly, in China, the suppression of crime and protection of public safety are regarded more highly than individual rights. In contrast, the fundamental goal of the legal system in the U.S. is to protect individual rights, including defendants’ rights (Lu 2010).

Chapter 3 Framework of Cybercrime

As documented in the last chapter, China has seen the rapid emergence of cybercrime since Internet has been made publicly available. In this chapter, a top-down approach is used to study and compare frameworks of cybercrime. The chapter begins by defining the nature of cybercrime and to study why it has become such a plague for the Internet users today. This is then followed by a comparison of the frameworks of cybercrime which have been documented in Chinese and Western literatures, leading to a generalised framework.

3.1 Understanding cybercrime

To study cybercrime, it is important to first understand what cybercrime is. The term “cybercrime” is in fact, largely an invention of the media, just like the term “cyberspace”, which originates from the novel *Neuromancer* (Jewkes 2010). While “cyberspace” is now casually used to refer to the imaginary “space” on the Internet, “cybercrime” is used to refer to the crimes committed over this “space”.

3.1.1 Definition of cybercrime

Symantec has defined cybercrime as “any crime that is committed using a computer, network, or hardware device” (Fossi 2008). Wall has a somewhat different explanation: “cybercrimes are understood here to be criminal or harmful activities that involve the acquisition or manipulation of information for gain” (Wall 2008). While the first two definitions highlight the importance of the involvement of technologies in cybercrimes, Wall’s unique definition has added that cybercrime is about intangible information rather than tangible assets such as physical goods. This is indeed true because the Internet is essentially a global network of users sharing information with one another. The Internet is all about informational transfer and it is the speed of this informational transfer which has led to its rapid growth. Barlow supports this view by describing the cyberspace as “a virtual environment in which economic value is attached to ideas and their virtual expression rather than physical property” (Wall 2008).

From the above definitions, it can be generalised that cybercrime refers to any crime that involves:

1. The acquisition or manipulation of information, rather than physical assets, for personal gain
2. The use of new technologies such as computers, networks and hardware devices.

3.1.2 Characteristics of cybercrime and the Internet

In order to identify the distinctive characteristics of cybercrime, Wall used what he called a “transformation test”, a heuristic which highlights the significant transformations that have made cybercrimes distinctive from traditional crimes (Wall 2008). The transformations he observed are summarised as below:

1. **Networking and the convergence of technologies:** technologies are becoming increasingly interoperable.
2. **Informational transfer and value:** on the Internet, value is attached mainly to intangible ideas and information rather than tangible assets. The focus of cybercrime is to acquire information in order to extract its values.
3. **Globalization:** the collapse of traditional geographies of distance. This has created informational crime opportunities across cultures and jurisdictions by extending the reach of criminals globally.

Sandywell also recognised the need for such characterisation and his observations extend Wall’s list. He identified the following:

1. **Instantaneous** information transmission enabled by the Internet.
2. The **anonymity** or “facelessness” of cyberspace.
3. Material **incorruptibility** of materials that can be reproduced without degradation in quality.
4. **Manipulability** of digitally coded electronic information as integrity can easily be compromised (Sandywell 2010).

The Internet has also torn down the traditional boundaries of crime such as geographical and jurisdictional boundaries. This makes cybercrime especially difficult to control because any prosecution would require the collaboration from law enforcement agencies over the globe. Also, the Internet has given the cybercriminals the option of harbouring in countries with a poor legal framework such as the developing countries. Such countries act as safe havens for cybercriminals.

The most important feature is anonymity, which refers to the ability to hide one’s true identity from another. Anonymity is implicitly facilitated by the architecture of the Internet and it is perhaps one of the most influential factors that motivate people into committing crimes over the Internet. However, one must remember that anonymity can also be preserved by using the telephone to carry out criminal activities. However, using a telephone, a criminal is required to interact with the victim personally. On the other hand, communication over the Internet is fully mechanised. Over the Internet, one only has to interact with the computational device that is used to access the Internet. It is this sense of distance from the victims that has motivated criminals into committing cybercrimes. This is noted by Wall when he asked convicted internet fraud offender whether he would have gotten into crime had the internet not been involved. The offender replied: “for me the internet made it, it was anonymous; you just tapped your details into the web page.” (Wall 2008). The importance of the sense of distance from the victim is further highlighted when Wall asked the offender if he could have rung a vendor and ordered the same goods over the phone, the offender replied: “no way, if it was face to face...then no way. It was a specific opportunity that arose”.

3.1.3 Typology of cybercrime

As described in the above section, the identification of the unique characteristics of cybercrime would help the reasoning behind the decisions made by the cybercriminals as well as the emergent frameworks of cybercrime. In this section, the general types of cybercrime are discussed.

The three main types of cybercrime as identified by both Grabosky (Grabosky 2007) and Wall (Wall 2008) are as follows:

1. Computer integrity crimes
2. Computer assisted (or related) crimes
3. Computer content crimes

Computer integrity crimes are crimes with the aim of disrupting the integrity of computer systems. Thus, computer integrity crimes are crimes where the computers are the target of criminal activities. The cybercrimes falling into this category include hacking, cracking, spying, vandalising, denial/disruption of service, digital piracy and the infection of malicious software (malware). These are crimes which seek to exploit the manipulability as well as the incorruptibility of digital data, as described in the previous section.

Computer assisted (or related) crimes refer to the traditional crimes committed with the use of computers, or in other words, computers as instruments of crime. This category of crime usually involve the acquisition of sensitive information, such as personal information, through techniques such as spamming, phishing and social engineering, and the ultimate goal is to utilise the acquired information for personal gain.

Lastly, computer content crimes are crimes where the involvement of computers is insignificant, or in another word, incidental to the actual crime committed. Crimes falling into this category are more sensitive to regional laws than the other two categories but generally, the distribution of child pornographic materials as well as the promotion of hate and extremist ideas fall into this category.

The three categories of cybercrimes above have subsequently led to the emergence of three distinctive groups of criminals involved in cybercrimes (Choo 2008a):

1. Traditional organised criminal groups
2. Organised cybercriminal groups
3. Ideologically and politically motivated cybercrime groups

Traditional organised criminal groups refer to those which have existed long before the prevalence of cybercrime and are actively engaged in real world offences such as drug trafficking and human trafficking. This group of criminals are mainly driven by financial gain and are always actively seeking new opportunities in order to increase their wealth. These criminals have recognised value of technologies in facilitating the commission of crime as well as the identification of new opportunities and circumventing law enforcement restrictions. According to Paget, online extortions and digital piracy are already being exploited out by China's longest running triad, the *Sanhehui* (McAfee 2009). Information from SOCA has also revealed that traditional organised criminal groups are also "increasingly using false and stolen identities to commit non-fiscal frauds" (Choo 2008a).

Organised cybercriminal gangs are those that operate exclusively over the Internet. Choo suggests that such organisations are more loosely structured flexible, transnational and tend to have smaller membership sizes. Furthermore, they are more temporal and would go their separate ways after successfully accomplishing the tasks at hand.

Lastly, the ideologically and politically motivated cybercrime groups are those who use the Internet to disseminate their ideas as well as to facilitate their extremist activities. There are emerging trends that extremists and traditional organised crime groups have converged and that both have used the Internet to finance their offline activities, such as through online credit card frauds.

3.2 Comparison of organised cybercrime in China and the West

It is now rare to see cybercrimes being committed by lonely individuals. At present, most cybercrimes are committed by organisations of cybercriminals who are motivated by financial gain. This trend applies to both China and the Western countries such as the U.S., U.K. and Eastern European countries like Russia and Romania. In this chapter, several high profile case studies from China and Western countries are introduced.

3.2.1 Case studies in China

The two most high profile cases regarding cybercrimes in China are documented below, both of which demonstrates the existence of organised cybercrime in China.

The first and perhaps the most famous case³⁴ with regards to cybercrime in China occurred in 2006 when Li Jun, the author of the Panda worm (a.k.a. “Panda Burning Joss Stick”) met online with Wang Lei, a Web Master and Zhang Sun, an Envelopes Stealer. Li Jun and Wang Lei set up several websites which infected visitors with the Panda virus. Furthermore, they sold traffic to Zhang Sun by allowing him to link his Web-based Trojans to the websites. Subsequently, the visitors to the websites were infected by several Trojans and virtual goods, mainly online game and QQ logins were stolen. Millions of machines were believed to have been infected across China and the losses due to this incident were estimated to be up to 100 million RMB (US \$14 million). Li Jun made an estimated profit of around 150,000 RMB (US\$ 22,156) (Zhuge 2008). In February 2007, Li Jun and his accomplices were caught by uncover police pretending to be a potential buyer for his malware³⁵. This case is widely believed to be the first case which brought to light the underground virus production chain in China. The virus author Li Jun, as shown in figure 13, was aged 25 in 2007. He claimed that he only began using computers in 1999 in Internet cafes and he quickly began writing viruses as a hobbyist. However, after he was asked to sell his Trojan, he believed he could make money from it and subsequently continued his actions.



Figure 13 - Li Jun, the author of the Panda worm

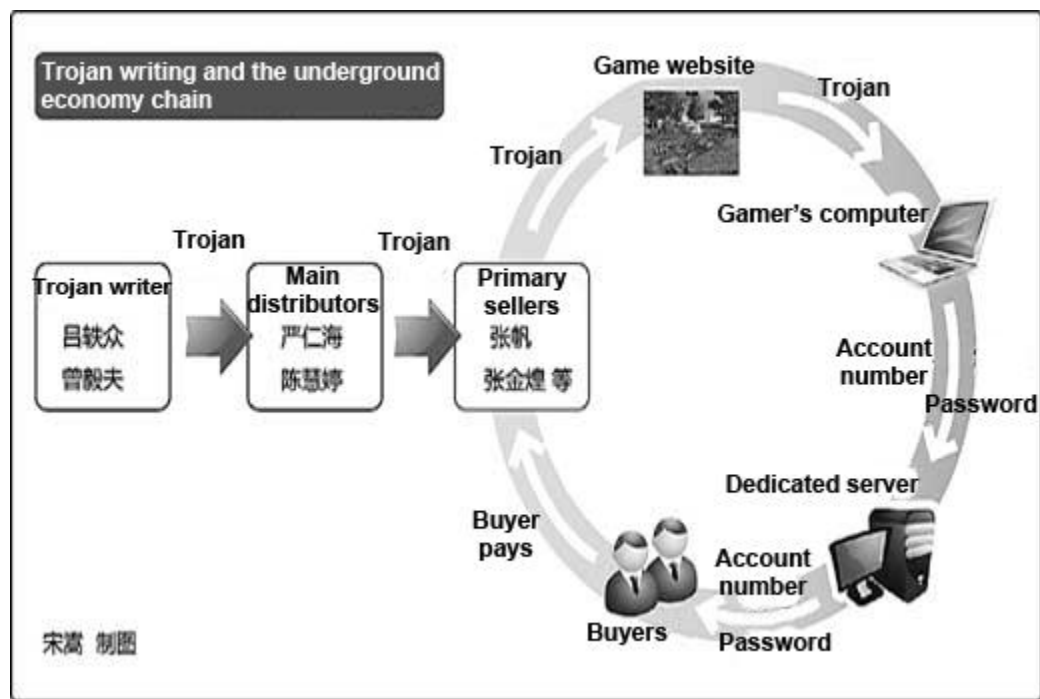


Figure 14 – the underground economy chain in China exposed

³⁴ Revealing the Internet virus production chain behind “Panda Burning Joss Stick” - http://news.china.com/zh_cn/news100/11038989/20070217/13946944.html

³⁵ Shanghai Youth Newspaper: The true story behind the “Panda burning joss stick” case - <http://it.sohu.com/20070214/n248244529.shtml>

The second case occurred in 2007 to 2008 when a cybercriminal group illegally produced and traded more than 40 variants of a Trojan known as “Gentle” which targeted stealing online game accounts and passwords. The investigation into the group’s activities has exposed a flourishing underground economy and malware production chain in China.

The criminal gang began when Trojan authors Lu and Zhang wrote more than 40 variants of a Trojan targeting online games. Zhang then asked his friend Zheng to distribute the series of Trojans and Zheng accepted the request and traded using his girlfriend Chen’s online name “Gentle”. Lu also allowed Zhang Fan and Zhang Jin Wang to act as primary sellers to sell the Trojans. Within one year, they have managed to steal over 5.3million online gaming accounts and passwords. The Trojan authors Lu and Zhang made a profit of around 645,000 RMB, which is equivalent to approximately 94,534 U.S. dollars.

This case involved 16 provinces with more than a hundred people involved with the investigation and concerns as much as 30 million RMB (US\$4 million). A translation of the depiction of the virus production chain concerning the “Gentle” Trojan is as shown in figure 14 above. Eleven people were prosecuted³⁶ for the involvement in the dissemination of malware. Of these eleven men, eight had received university level education and ten were born after 1980 with the youngest being 22 years old.

From the two above cases, it can be seen that there is little doubt that organised cybercrime exists in China but further proof was needed to prove whether an underground economy exists in China. The author of this thesis subsequently went on to search for more information on the “underground economy” and it turns out that the existence of it has already been widely reported by Chinese security firms and the media. The level of attention from the Chinese media indicates that this is of a great concern for the Chinese Internet population. Figure 15 is a translated version of a widely distributed depiction of the underground economy chain in China.

3.2.2 Case studies in the West

One noticeable difference between the underground economy in China and the West is that markets most often exist in the form of forums and IRC³⁷ channels (Thomas 2006) in the West but these are rarely mentioned in cybercrime cases in China. Western online black markets have been known to exist in as early as 2002.

The first major organised cybercrime case in the West which brought to the light existence of an elaborate underground economy concerned an online forum called ShadowCrew which was dedicated to carding activities.

ShadowCrew began operation in 2002 and it was a safe haven for carders and hackers to trade goods and services with free membership. It offered contents in both English and Russian in order to increase geographical dispersion of its members so that the availability of cash-out and drop³⁸ locations would increase. Shadowcrew was shut down by the U.S. and international law enforcement agencies in Operation Firewall in 2004 (Fossi 2008).

³⁶ “Gentle Trojan” exposes underground information market, concerning nearly RMB 30million - <http://society.people.com.cn/GB/10618004.html>

³⁷ Internet Relay Chat (IRC): an Internet Communications protocol using a client-server model which offered real-time group communications, requires little bandwidth and the client applications required to access the service are freely available.

³⁸ Drop – an intermediary location at which carders could use as delivery address for physical goods bought with fraudulent cards. They are also used to refer to intermediary bank accounts used in money laundering.

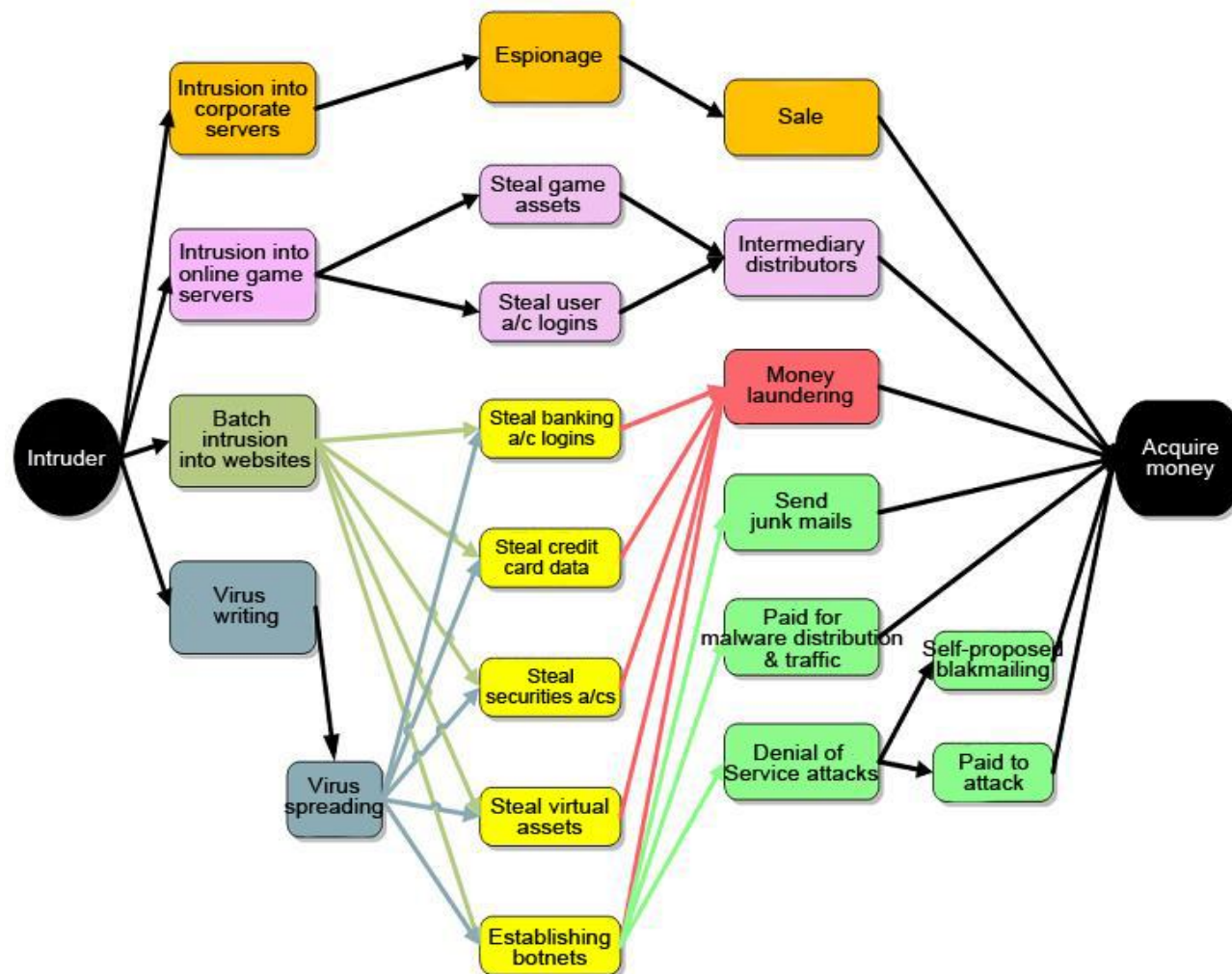


Figure 15 – a translated version of a mapping of the underground economy “production chain” in China³⁹ Case studies in the West

³⁹ Investigation into hacker production chain: the formation of an underground virus trading market. Available at: <http://news.qq.com/a/20090630/000190.htm>

SHADOWCREW FOR THOSE WHO WISH TO PLAY IN THE SHADOWS			
MAIN FAQ Search Memberlist Usergroups Register Profile Login to check your private messages Login			
The time now is Mon Oct 14, 2002 12:09 pm shadowcrew Forum Index			
Forum		Topics	Posts
Global Forum For all you speed-posters. The Global Forum contains all topics from all forums except trash and the archives.		2221	20766
		Mon Oct 14, 2002 12:08 pm Theallosingphantom	
Forum		Topics	Posts
Discussion Forums			
The Lounge Anything goes in this forum. Take your battles and personal matters into the lounge. Moderators midhack , macavver , golumfun		867	9129
		Mon Oct 14, 2002 12:08 pm Theallosingphantom	
Identification Technical discussion on Novelty Identification, 2nd ID, Passports, and the like. Moderator macavver		546	4404
		Mon Oct 14, 2002 11:07 am golumfun	
Cyberspace Discussion about online anonymity and tools to hide your online presence. Moderator macavver		155	821
		Mon Oct 14, 2002 10:27 am crowd	
Credit & Checks Discussion concerning credit cards, credit bureaus, credit reports, credit services, checks, bank accounts, and banking services. Moderator golumfun		436	4501
		Mon Oct 14, 2002 12:06 pm golumfun	
Qualification Discussion of Diplomas, Employment References, Job searches, Transcript, Etc Moderator golumfun		66	427
		Mon Oct 14, 2002 11:14 am andy	
Vendors and Reviews			
Vendors/Reviews Find out what vendors offer and who delivers. Moderator midhack		63	568
		Mon Oct 14, 2002 10:51 am Buck	
Scamming Bastards Tell everyone who ripped you off and maybe save the newbies a few dollars. Moderator midhack		20	175
		Sun Oct 13, 2002 6:12 pm newmessagein	
Archives			
Tutorials and How-To's Learn from those who came before you.		111	262
		Sun Oct 13, 2002 10:45 pm midhack	

Figure 16 – a screenshot of the Shadowcrew forum in 2002

Another noticeable online forum which was shut down by Operation Firewall was called the CarderPlanet, which was created by a man named Script. CarderPlanet operated in similar fashion to ShadowCrew and as its name suggests, it is another carding forum. Script's real name is Dmitry Golubov, now an Ukrainian cybercriminal turned politician. In 2001, Goulubov held a meeting at a restaurant in Odessa, Ukraine with 150 other interested people from Eastern Europe. Soon after the meeting, he decided to launch CarderPlanet in order to facilitate underground carding (Paget 2010). Script was reportedly earning up to \$100,000 U.S. dollars a day (Fossi 2008). In July 2004, Golubov closed CarderPlanet claiming it has attracted too much attention from law enforcements.

A more recent case with regards to online carding forums is the high profile closure of the forum named DarkMarket⁴⁰ in 2008. According to an interview with SOCA, Darkmarket was founded by Renukanth Subramaniam, who was also a member of Shadowcrew and Carderplanet using an online identity called JiLSi. Darkmarket operated as a closed membership forum but and had around 2500 members. JiLSi attracted the attention of the FBI and an undercover operation was launched. A FBI agent named Keith Mularski, known as Master Splynter, infiltrated Darkmarket as a reputable spammer who has featured on Spamhaus. He subsequently became the administrator of Darkmarket after securing Darkmarket from rivalry attacks. This gave the FBI great convenience in evidence gathering. Since November 2006, Mularski operated the site as an administrator. The operation ultimately led to around 60 arrests in a dozen countries including the U.K..

The last case study of Western organised cybercrime is the Russian Business Network (RBN) an organisation which offered a complete infrastructure to achieve malicious activities (Bizeul 2007). The RBN provided a safe haven for cybercriminals for hosting malware, malicious websites as well as

⁴⁰ Welcome to DarkMarket – global one-stop shop for cybercrime and banking fraud-
<http://www.guardian.co.uk/technology/2010/jan/14/darkmarket-online-fraud-trial-wembley>

illegal content such as child pornography by obfuscating essential domain name registration details as well as sheltering them from complaints and take down orders.

3.2.3 Compare and contrast between China and the West

According to the 2009 Internet Security report⁴¹ by Kingsoft Security⁴², the total revenue from the Chinese underground virus production chain is estimated to soon be reaching as much as 10 billion RMB (US\$1.48 billion). This is far larger than the figure reported in 2008 by Symantec who estimated the total amount of the advertised goods they observed was worth approximately US\$276 million⁴³. By solely looking at the figures, this suggests that the underground economy in China could be as much as five times larger than the Western economy. However, one has to bear in mind that the way both sets of data are gathered and the scope taken into account are different. Nonetheless, the estimation does reveal that the underground economy in China is flourishing.

Furthermore, it has been reported that an underground malware production chain for mobile devices also exist. According to a news report⁴⁴ from ChinaByte, the number of detected mobile malware in China has been doubling every year since 2006, reaching 1000 variants by the end of 2009. The direct damage caused by mobile malware in China is estimated to be worth 20 million RMB (US\$2.9 million). The annual revenue of the mobile malware production chain is conservatively estimated to be around 1 billion RMB (US\$148 million). In contrast, West security firms do not have such separate study and distinguishing for mobile related malware.

With regards to the case studies documented above, several notable differences are observed:

- Western cybercriminals has a high preference to use online forums to facilitate carding activities but there is no mention of such centralised means being used in China
- U.S. cybercriminals most often collaborate with Russian speaking counterparts but they also collaborate with people from other countries.
- Western forums also offer tutorials to exchange knowledge.
- Chinese cybercriminals are mostly prosecuted for producing and disseminating malware rather than for carding offences.
- Chinese cybercriminals mostly operate within China and collaborate with Chinese counterparts only.
- Despite only infecting Chinese users over a short period of time, the infection rate in China could be very rapid. E.g. the “Panda” worm which is reported to have infected millions of machines over a space of six weeks.
- Undercover police operation seems to be the preferred method used by both the Chinese and the Western law enforcement agencies.

A more detailed comparison between the Chinese and Western underground economy is given in chapter 4.

⁴¹ 2009 China Computer Virus Infection State and Internet Security Report - <http://www.cnetnews.com.cn/2010/0128/1615976.shtml>

⁴² Kingsoft Security is one of China’s most popular Internet security software vendors. See: <http://www.duba.net/>

⁴³ New Symantec Report Reveals Booming Underground Economy - http://www.symantec.com/about/news/release/article.jsp?prid=20081123_01

⁴⁴ Virus hidden in mobile texts, black production chain worth 1 billion - <http://sec.chinabyte.com/424/11532924.shtml>

3.3 Organised cybercrime and the underground economy

As described earlier, there are three main types of cybercrime groups involved in cybercrimes. While these groups can be theoretically distinctive, recent cases as shown in section 3.2 suggests that the distinction in their involvement in cybercrime are not as clear in reality. Criminal networks have emerged where cybercriminals trade with each other and each take on a specialised role (Moore 2009).

Figure 17 on the next page shows a mapping of the underground economy, which is a generalisation of the frameworks of cybercrime in both China and Western countries as discussed in section 3.2. In this section, the underground economy will be examined and the role of the major actors in this economy will be discussed.

3.3.1 Labour specialisation, deskilling and reskilling

In his book *Security Engineering*, Anderson introduced the economic theories which are often applied in computer security. One of the concepts he introduced was Adam Smith's theory on how self-interest in a free market economy leads to economic wellbeing: "specialisation leads to productivity gains at all levels from a small factory to international trade, and the self-interested striving of many individuals and firms drives progress, as people must produce something others value to survive in a competitive market" (Anderson 2008). Cybercriminals have come to realise that profits can be maximised by collaborating and trading with other like minded people with different skill sets.

Wall observes that cybercriminals often deskill and reskill just like those in the labour market. An example of deskilling is where the introduction of scripts has led to the automation of hacking which was used to be carried out manually (Wall 2008). However, at the same time, the introduction of technologies at a rapid pace means that the cybercriminals must reskill themselves in order to be familiar with vulnerable technologies and to exploit them to their advantage. An example of this is the increasing exploitation of social networks.

3.3.2 The actors in the underground economy

As described in the previous section, the underground economy is comprised of many different actors offering different products and services, each facilitating the commission of one or more cybercrime. In this section, some of the major actors, categorised by the type of products and services they offer to the underground economy, are introduced and discussed.

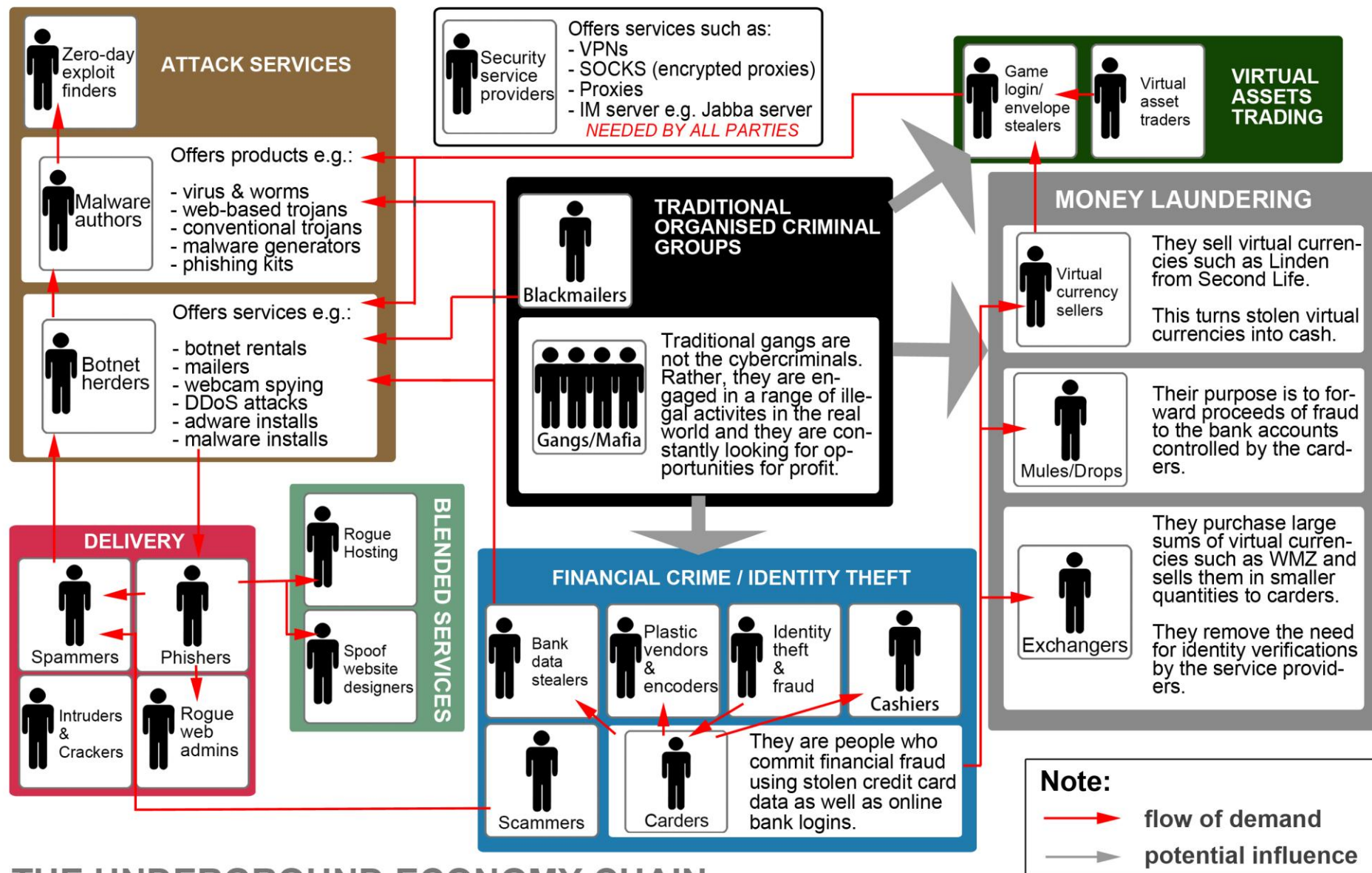
Referring to figure 17, there are eight major types of products and services offered in the underground economy:

1. Traditional organised criminal groups

As described by Choo, the traditional organised criminal groups are those that engage in real world crimes such as drug trafficking as well as cybercrimes. These criminals are motivated by profit and they are actively seeking money making opportunities in order to expand their wealth. It is this motivation which lured them into the online underground economy as cybercrimes become increasingly lucrative due to identity theft and fraud.

2. Financial crime/identity theft

Identity-related crime is not a new phenomenon nor is it an Internet specific crime. However, there is little doubt that the Internet and other communication technologies have greatly facilitated this type of crime due to a rapid increase in the amount of personal information available. More specifically,



THE UNDERGROUND ECONOMY CHAIN

Figure 17 – generalised mapping of the underground economy

identity-related crime is “a compound concept used to refer to a range of methods used to commit specific forms of deception and fraud” (Smith 2010). One example of such activities is carding, which refers to “the unauthorized use of credit and debit card account information to fraudulently purchase goods and services” (Peretti 2008).

Referring to figure 17, there are several notable actors in the underground economy who commit crimes belonging to this category:

Bank data stealers: they are the individuals who steal bank data from unsuspecting computer users, as described in section 3.3.1. The types of bank data most frequently traded can be found in Appendix B. An interesting study by Holz *et al.* gives an unique insight into how exactly malware such as keyloggers are used to steal data (Holz 2008).

Carders: they are the individuals who are engaged in criminal carding activities using the data listed above.

Plastic vendors and encoders: these are the individuals who sell blank credit cards. They often offer packaged services such as encoding and printing fraudulent credit cards for the client. This is a preferred method for new carders because this is less costly than having to purchase equipments such as an encoder and blank cards. China is a popular source for both types of equipment.

Cashiers: these are the individuals who perform cash withdrawal from the fraudulently obtained bank accounts in person, usually at ATM machines in quiet areas. They are also known as “runners”.

Scammers: these are the individuals who fabricate a fraudulent story and trick the victims into making financial losses. The Nigerian “419 Advance fee” scam is one of the most well known scams in recent years.

3. Attack services

The products and services offered in this category are all aimed at attacking the integrity of computers. As previously described, the list of crimes belonging to this category includes hacking and cracking, vandalising, spying, denial of service, digital piracy and the infection of malware. The major actors in this category are:

Zero-day exploit finders: zero-day refers to the number of days since a software vulnerability has been discovered and zero-day exploits refer to the fresh vulnerabilities unknown to anyone. Zero-day exploit finders are the individuals whose job is to find previously unknown vulnerabilities in targeted applications and would sell such exploits to malware authors. These exploits are the most expensive items sold on the underground economy as they would allow infections which would in turn bring about a revenue stream. In 2006, one such finder offered to sell a Windows Vista zero-day exploit for \$50,000 U.S. dollars⁴⁵. It has also been suggested that some sells for as much as \$120,000 (Muttill 2008).

Malware authors: malware, an abbreviation for malicious software are applications designed to exploit the vulnerabilities in software applications. There are several types of malware including web-

⁴⁵ A Windows Vista exploit costs \$50,000. Available at: <http://news.softpedia.com/news/A-Windows-Vista-Zero-Day-Exploit-Costs-50-000-42667.shtml>

based Trojans⁴⁶, conventional Trojans⁴⁷, virus and worms⁴⁸. Competition between malware authors also exists. Malware authors do reverse-engineer their rivals' malware in order to gain a bigger market share on the underground economy (Elser 2009).

Botnet herders: a botnet is a network of machines compromised bots and a bot is a malware acts upon commands received from a command server.

4. Delivery services

The services offered in this category are those which aim to disseminate malware as quickly as possible. The major actors in the category are:

Phishers: these are the people who specialise in creating legitimate looking messages with the aim of luring the unsuspecting victim into clicking on a link to visit an infected website or downloading an infected attachment. Most often social engineering skills are used to increase the legitimacy of the messages. Recently, there is an increasing threat of *spear phishing* whereby the phisher target specific individuals in an organisation.

Spammers: spammers specialise in mass mailing. Most often, spammers are also botnet herders and they utilise their botnet to send out huge volumes of email. A study on the financial reward from spam marketing conversion rate of the Storm botnet was carried out by Kanich *et al.* (Kanich 2008). In their study, they found that the conversion rate for pharmaceutical spams was well under 0.00001%. Using this same rate, the Storm-generated spam would produce roughly 3.5 million U.S. dollars worth of revenue in a year.

Rogue web admins: they are usually administrators who run legitimate websites but are willing to infect their website with malware upon receiving financial reward, thus breaching the visitors trust.

Intruders & crackers: they are the hackers which are force an entry into machines and perform other cybercrimes such as spying, vandalising as well as espionage.

5. Blended services

The services in this category are support services which may or may not be illegal. The actors in this category are:

Rogue hosting: these are hosting services aimed at providing a safe haven for malicious activities. The Russian Business Network (RBN) is one such service (Bizeul 2007).

Spoof website designers: these are web designers who are willing to build websites which mirror legitimate ones.

⁴⁶ **Web-based Trojans:** this type of Trojans exploits system or application-level vulnerabilities and opens up a backdoor for attackers to infect the compromised machine with other malware.

⁴⁷ **Conventional Trojans:** these Trojans enable the remote control of infected machines (called "flesh chicken" in Chinese) and they are also used to steal personal data such as login credentials.

⁴⁸ **Virus and worm:** a virus is a malware which infects a host such as a legitimate application and will self-replicate and propagate. Worms would also self-propagate but they do not require a host. Both malware could be used to alter system or application configurations as well as disabling security measures.

6. Security services

This category of services aim at providing security services for the cybercriminals such as a Virtual Private Network (VPN) service, proxies and SOCKs (encrypted proxies) all of which would allow cybercriminals to hide their true identity as well as protecting the confidentiality of their communications. This type of service is needed by all cybercriminals who wish to be secure.

7. Virtual assets trading

The services in this category are involved in the theft of virtual assets such as avatars, clothes, weapons, accessories and most importantly, virtual currency. These assets are most often from popular Massively Multiplayer Online Role Playing Games (MMORPG) such as the World of Warcraft (WoW) Second Life and Lineage 2.

People spend a lot of time playing. More than 25 percent of gamers play for more than 30 hours every week (Muttill 2008). Since players spend so much time and effort in trying to collect virtual commodities, some prosperous gamers are willing to take shortcuts and pay real money to get advanced virtual objects to avoid boring routine work, commonly known as “grinding”.

To steal virtual assets, the first step is to steal gamer accounts and login credentials, most often carried out by the so-called “Envelope stealers”. Once they have stolen the accounts, they sell the account login credentials to the virtual asset traders who would use the information to access the accounts (open the envelope) and steal all the virtual assets registered with the account. They would then sell the assets to the prosperous gamers.

In China, the most popular MMORPGs include Dungeon N’ Fighter (DNF) Dragon Nest (DN) XYQ, ZT Online Green edition and the Enchanting Shadow. This is an increasingly lucrative business because the online gaming market is rapidly booming. Zhuge *et al.* carried out a study of the virtual assets trading via the *Taobao*⁴⁹ online business platform, a Chinese trading platform similar to eBay. They found that 1.2 million virtual goods were on sale and 8.9 million exchanges have taken place within a six-month period (Zhuge 2008). Finally, they estimated that the market value of the virtual asset exchange solely on the Taobao platform is about 223 million RMB (US\$33 million).

Furthermore, in China, not only online game assets are valuable. Tencent QQ is not only the most popular instant messaging (IM) service but it is also a social network with a wide range of service such as online games, avatars and even offers their own electronic currency known as “Q coin”. “Q coins” are required if the user wants to purchase extra accessories for his avatar or to gain access to certain service, such as creating a QQ group. Upon completing the registration, the user is assigned a unique QQ number, just like ICQ in the West. The problem is that there is a real financial value attached to some QQ numbers, such as those with fewer digits or contains certain combination of numbers e.g. 168888 or 888888. There are some prosperous people who are willing to pay real money for these “beautiful” numbers. As a result, cybercriminals recognise this demand and use various methods such as phishing and Trojans to steal QQ accounts. Not only are the QQ accounts sellable but also the virtual assets registered with account, such as the accessories worn by the avatar and the “Q coins”.

⁴⁹ Taobao - <http://www.taobao.com>

As mentioned in chapter 2.1, approximately 18.5% of malware infection victims experience theft of their online identities which is much higher than the theft of banking related assets. This highlights the increasing significance of the ownership of virtual assets. Similar trends are observed in the West where gaming Trojans and banking Trojans are found to be nearly as common (Muttill 2008).

8. Money laundering

Money laundering is required for nearly all criminal activities because ultimately, most crimes involve some form of financial exchange and the criminals must hide the true source of illicit funds. Traditional methods include electronic funds transfer, fictional companies with foreign banks, cash smuggling, bank fraud, and informal money exchange brokers. There are two methods which have become prevalent in cybercrimes in the West, money mules and exchangers.

Money mules: these are people who receive proceeds of fraud from compromised bank accounts and forward the fund to those controlled by the fraudsters for cashing out. There are two types of money mules: *innocent mules* are those who have no idea that the funds they are forwarding are proceeds of fraud; and *professional mules* are those who knowingly and purposefully provide the money laundering service for fraudsters. Money mules are recruited through a variety of methods:

- Unsolicited emails e.g. spams
- Classified adverts on legitimate recruitment websites
- Job vacancies published on fraudulent websites purporting to be a legitimate business

Attractive job titles such as “Financial Managers” and “Country representatives” are offered to lure victims and “no previous experience required” is often stated on the job adverts.

Just like their Western counterparts, the Chinese cybercriminals, in particular, those committing bank frauds, often require overseas “money mules” to launder the proceeds of fraud before cashing out in another country. During the course of this study, it was observed that an advert was placed on a QQ group recruiting Chinese overseas students in the U.K. to act as money mules, as shown in figure 18 below.

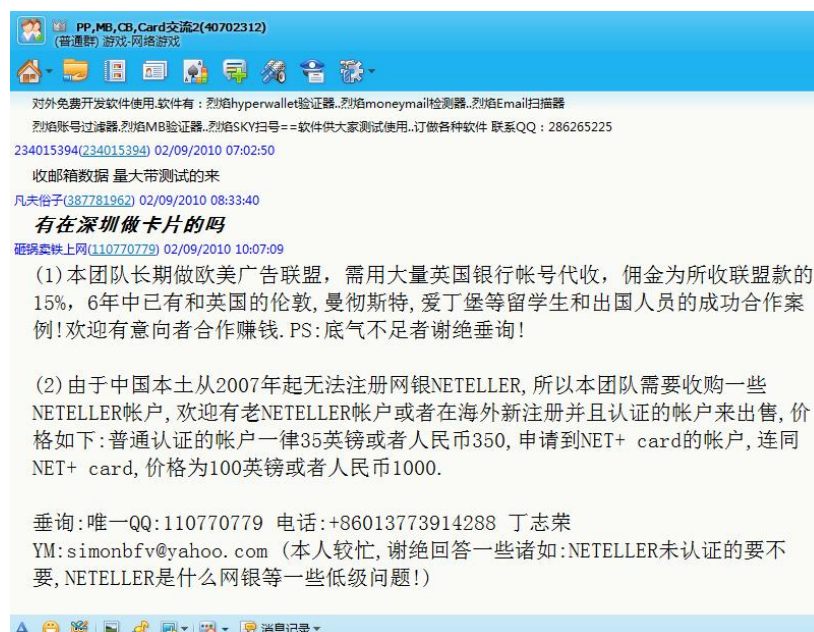


Figure 18 – advert recruiting Chinese students in the U.K. to act as money mules

The advert claims that the group engages in long term advertising campaigns in both the U.S. and Europe, thus needing a large number of bank accounts in the U.K. to receive funds on their behalf. Participants are offered a 15% return for their service. The advert also claims that there have been many successful collaboration cases involving overseas students in London, Manchester and Edinburgh. Furthermore, the advert requests for Neteller⁵⁰ accounts because registration is not available in China. The advertiser is offering £35 for a normal account and £100 for accounts with Net+ card.

Exchangers and Virtual Payment Systems (VPS):

There are three types of VPS:

- National currency backed e-currencies: e.g. WebMoney (WMZ – WebMoney dollars)
- Precious metal such as gold backed e-currencies: e.g. e-Gold, Liberty Reserve and WebMoney Gold (WMG)
- Blended payment systems: e.g. Paypal and Western Union

The main advantage of the electronic currencies (e-currencies) is that they provide the anonymity sought by the cybercriminals and no risk of a chargeback. However, identity verification may be required for transferring large sums. E.g. in order to exchange a large sum of WMZ, one would be required to perform an identity verification to obtain a WM Passport. This is troublesome for the cybercriminals and this is where the exchangers come into the chain. Some exchangers with verified accounts who have a large amount of currencies are offering exchange service to the cybercriminals. Some are willing to turn a blind eye to the source of funds and preserve the anonymity of the cybercriminals.

In China, the Chinese cybercriminals also use Liberty Reserve and WebMoney for financial exchange. However, by performing a simple text based search for “WMZ”, “LR” and “淘宝” (Taobao) within the “visa” bar on Baidu Tieba⁵¹, it was found the most preferred method of exchange for Chinese cybercriminals is Taobao because the number of carding-related posts mentioning Taobao far exceeds the number of posts mentioning the former two. There are two explanations for this: firstly, the listing and selling of items on the Taobao platform is free of charge. In order for the carders to exchange, one only has to create a fake listing specifying the agreed amount. The buyer could then buy the “item” and pay as previously agreed in private conversations. This method is far less costly than using WebMoney and Liberty Reserve which often includes charges by intermediary exchangers. The second reason is that most Chinese cybercriminals do not trade foreign carders and so, there is simply no need to use foreign services.

Other methods of money laundering are also becoming popular in both China and the West:

Virtual casinos: online casinos are also used for money laundering (Paget 2009) and from SOCA material, it is documented that one of the ways in which online poker can be exploited for money laundering is by controlling multiple online identities using virtualisation software so that the risk of losing is minimised.

⁵⁰ Neteller – <http://www.neteller.com>

⁵¹ Baidu Tieba: is a free and publicly open forum-like application where anyone can make a post or start a new thread. The “visa” bar is the most common bar for carding related topics, see chapter 4 for more details. Available at: <http://tieba.baidu.com>

Prepaid stored value cards: there are two main types of stored value cards: open system cards and closed system cards. Open system cards are those that are reloadable and there are little restrictions on where the card could be used but they normally require cardholder's name. On the other hand, closed system cards like retail store gifts cards restrict owners to use them in designated stores (Choo 2008b). There have been several reported incidents which involved the use of stored value cards in an attempt to launder money.

3.4 Chains of need shapes the underground economy

As shown in figure 17, the underground economy is a network of chains of need where people with different skill sets offer their goods and services to satisfy the needs in the market. An example of a chain of needs for the carding is as follows:

The chain begins with the **“bank data stealers”** recognising the demand for bank data by the **“carders”** and intending to satisfy such need by stealing bank data. In order to do so, the stealers begin by paying the **“malware authors”** to write customised conventional Trojans which are capable to stealing personal data from the consumers of specific banks chosen by the stealers. After the malware has been written, the stealers would then ask the **“botnet herders”** to install their Trojans on to the zombies controlled by the herders. After an agreement has been reached on the price, which is usually based on the number of successful installs, the herders would simply add the bank Trojans to the list of installs to be planted on their zombies. After the stealers begin to steal bank data, they would then sell their data on to the carders. The carders would then require the services of **“money mules”** or sometimes known as **“drops”**, which are intermediaries knowingly or unknowingly receiving the proceeds of fraud and forwarding them on to the bank accounts controlled by the carders.

Chapter 4 Understanding and Comparing the Underground Economy

According to Symantec⁵², cybercrime has surpassed illegal drug trafficking as a criminal money-maker and one in five will become a victim. There is no doubt that cybercrime has become a widespread problem for all Internet users. Unfortunately, while Western online black markets have been subject to much research since as early as 2000, the Chinese underground economy has rarely been studied, with the only prominent work on Chinese underground economy by Zhuge et al. (Zhuge 2008). Following Symantec's report on the Underground Economy (Fossi 2008), a detailed study was carried out on the underground economy in China and the findings are documented in this chapter. The aim is to provide a direct comparison between the characteristics of the Chinese underground economy and the West.

4.1 Communication and advertising platforms

As described in section 3.2.2, one of the most distinctive characteristic of Western cybercrimes is the use of online forums. From SOCA material as well as the Operation Firewall Indictment (Department of Justice 2003), hierarchical management structures are common among carding forums in the West, as shown in figure 19 below.

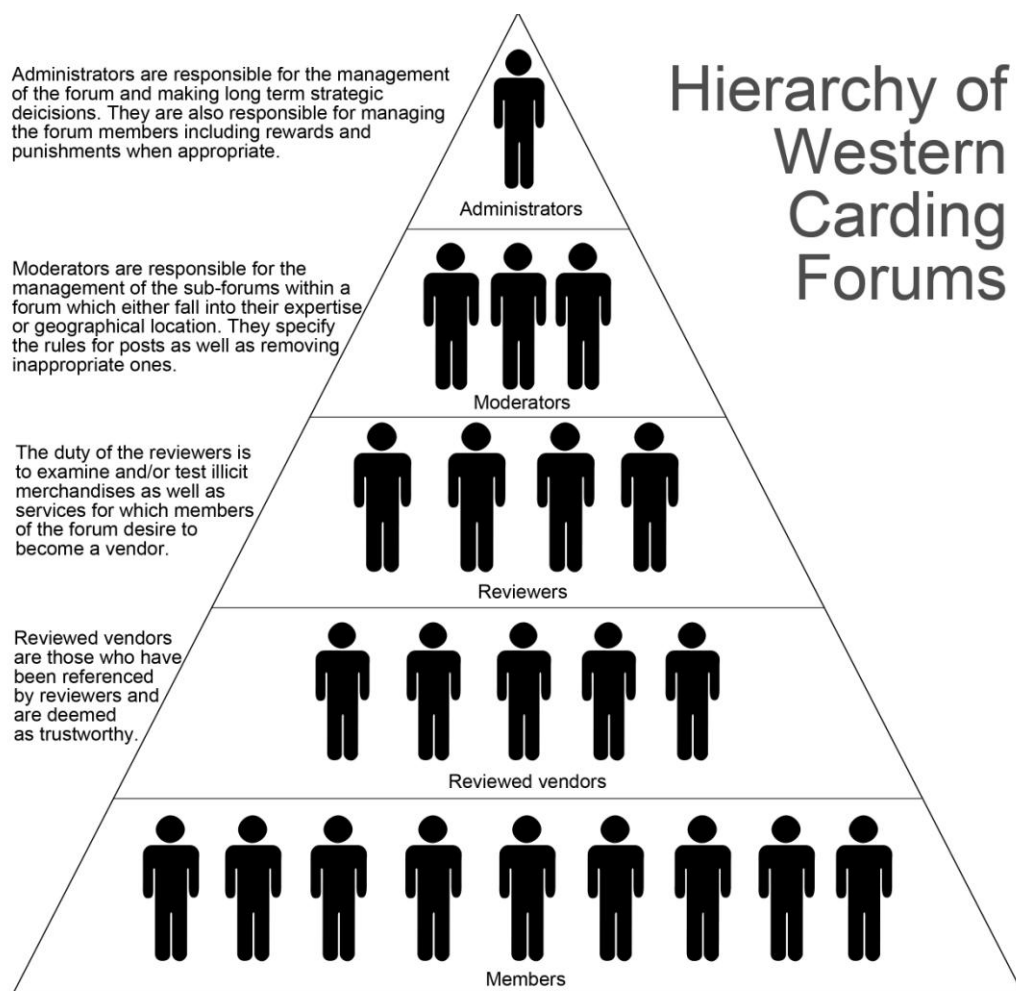


Figure 19 – hierarchical management structure of Western carding forums

⁵² Cybercrimes has surpassed illegal drug trafficking as a criminal moneymaker, 1 in 5 will become a victim. - http://www.symantec.com/about/news/release/article.jsp?prid=20090910_01

On the other hand, it has been observed that the Chinese cybercriminals prefer to use more decentralised means such as making advertisements on publicly accessible blog posts, groups and forums. The author of this thesis asked the Chinese carders why there are no such forums in China and one gave the reply saying there is simply no point because they know how quickly foreign carding forums are closed down. Indeed as described in section 3.3, the Western carding forums often attract too much attention from law enforcement as they become popular. Instead of being part of a hierarchical organisation, Chinese cybercriminals prefer forming networks of ephemeral relationships, such as those shown in figure 15 in last chapter. The features of the most popular systems used by the Chinese cybercriminals which remove the need for forums are described and summarised in this section,

4.1.1 Baidu Tieba

Baidu is China's largest search engine with 63% of the market share⁵³ in China's Web search market. However, aside from searching, Baidu also offer various social networking services, most notably the Baidu Tieba (贴吧). The Baidu Tieba is a publicly accessible and searchable message board system where specific boards (called "bar") can be freely created with a specific title by a registered user. Once the bar is created, it will become searchable within the Baidu Tieba. Users can also apply to be the administrator of the bar which would allow him/her to monitor posts as well as removing posts.

The screenshot displays the Baidu Tieba interface for the 'visa' bar. At the top, there are navigation links for News, Websites, Tieba, Knowledge, MP3, Images, Videos, and Encyclopedia. Below this is a search bar with the text 'visa' and a 'Baidu一下' button. The main content area is a table of posts. The table has columns for 'Clicks', 'Replies', 'Title', 'Author', and 'Last Reply'. The posts are listed in descending order of replies. On the right side, there is a 'Tieba Login' section with fields for username and password, and a 'Remember my login status' checkbox. Below the login section is a 'Bar Information' section showing the bar has 33 fans and a 'Follow this bar' button. At the bottom of the bar information section, there is a button to 'Apply to be a bar master!' and a section for 'Members' with a 'Join' button and a link to 'Learn about member privileges'.

Clicks	Replies	Title	Author	Last Reply
33	2	iTunes Gift Certificate 出售	180.152.30.*	14:55 60.15.231.*
5	0	合作挣钱 有带有生日的卡的进	带你出线	14:08 带你出线
53	5	收MB的请进	jamin345	13:54 jamin345
6	0	收US V.M.D卡(要能过iTunes的)	221.208.206.*	13:50 221.208.206.*
309	27	大量一手US CA DE 有需要的留QQ 5分钟加一次	us卡	13:34 59.58.137.*
11	0	所有买家请注意 公布骗子	99正义99	13:18 99正义99
6	0	收购美国信用卡, 一手的来.Q404569813	59.58.137.*	13:16 59.58.137.*
22	2	...出售台湾3D卡 包活 包有效 可以挑银行 需要加137349599	台湾卡营销	12:50 台湾卡营销
56	3	出售台湾一手卡跟资料 本人搞网络赌博生意 信用%百 可调查	鸟巢方案	12:43 yanglshuo111
111	6	小量日本V卡, JCB, 需要的联系	看pioneer	12:34 看pioneer
1720	721	JP 长期大量售日本卡 !!! 另: 懂刷货的 联系我!!!	诚信JP	11:59 诚信JP
160	12	qq 82621158 飞龙店主<tmfeilong@qq.com> 大骗子	110.173.49.*	11:45 68.16.181.*
30	3	—————大量全资料台湾信用卡—————任何行都有	jamin345	11:31 124.231.83.*

Figure 20 – a snapshot of the “visa” tieba on Baidu

Figure 20 is a snapshot of the “visa” bar, which is the most popular bar for Chinese carders. Anyone can make a post on the bar. If the user is registered, his/her username will be shown as the author. If the user is not registered, the first three range of his/her IP address is shown in the author's field. This means users' anonymity can be easily preserved. The lack of control of the Baidu Tieba coupled with the immense popularity of the Baidu portal itself, makes the Baidu Tieba the most convenient place for Chinese cybercriminals to advertise their goods and services as well as requesting for specific services. It is partly the reason why there is no need for a closed forum like those used by Western carders. A typical sale advert is as shown in figure 21 below. The typical format of an advert on Baidu Tieba consists of a short message mainly containing a brief description of the goods and services for

⁵³ Baidu's Gain from Depatruie Could Be China's Loss - <http://www.nytimes.com/2010/01/14/technology/companies/14baidu.html>

sale or request (such as the country and types of credit cards) as well as leaving the QQ number to hold further negotiations in private conversations via QQ (see next section for a more detailed examination of QQ IM).

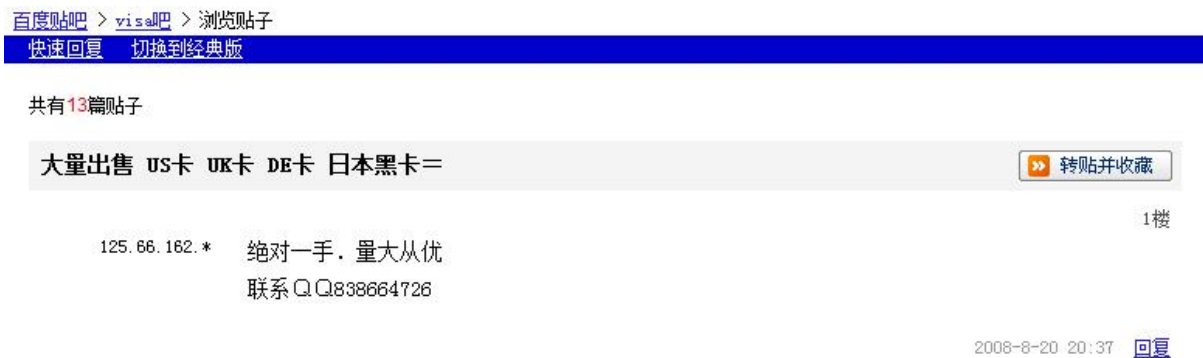


Figure 21 – an advert selling credit cards

While Western carding forums have reviewed vendors, the Chinese carders do not have such mechanism. Instead, rippers are posted and shamed on Baidu Tieba, as shown in figure 22 below:

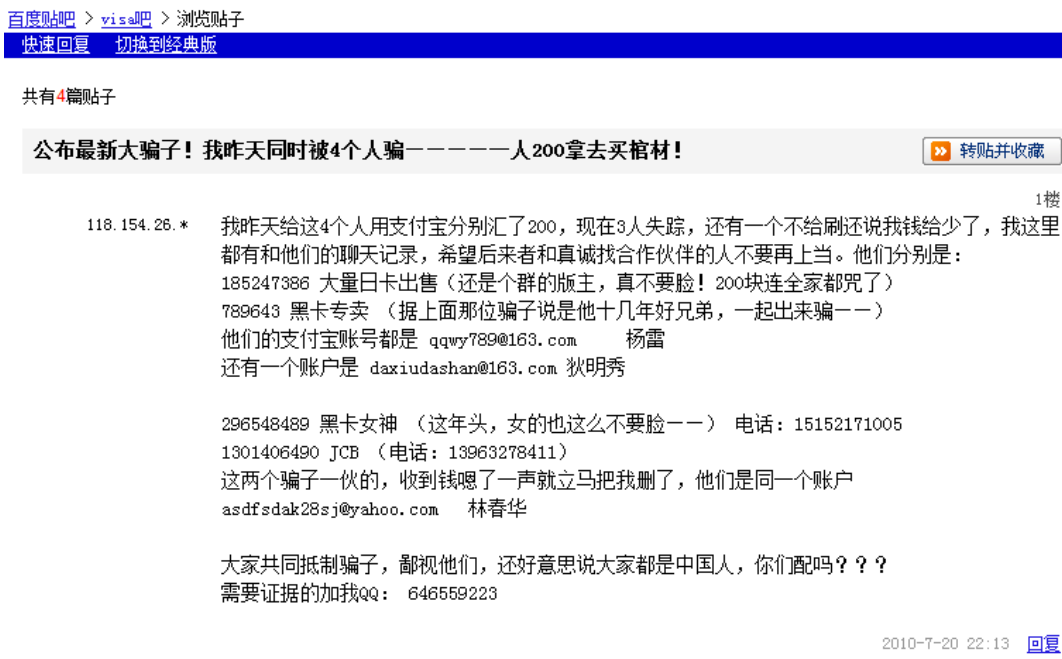


Figure 22 – dishonest seller shamed

Figure 22 shows a post warning others of the ripper. The post contains the ripper's QQ username, the QQ number and his/her account details on virtual payment system Alipay⁵⁴. The details of how the victim was ripped are also given.

Given the ease searching for specific posts on the Baidu Tieba, the Chinese cybercriminals can easily protect themselves by performing a search for the QQ number of the potential dealer they are intending to deal with, prior to performing any kind of transaction in order to avoid being ripped.

The following 'bars' are of particular interests to the underground economy:

⁵⁴ Alipay – <https://www.alipay.com>

Bar name	Note	26 th July 2010	20 th Sept 2010
visa	Most popular board for cardings	5823 topics 30214 comments	6710 topics 43426 comments
灰鸽子	Board for remote hacking and zombies “flesh chicken”	25618 topics 265276 comments	26601 topics 235303 comments
网站攻击	Contains sale and requests for attacking websites	226 topics 4710 comments	234 topics 2813 comments
入侵网站	Similar to 网站攻击	190 topics 4511 comments	242 topics 7889 comments
网马	The board is about “Web Trojans”	3973 topics 18839 comments	4087 topics 15430 comments
找黑客	Advertising hacking services as well as requests for services. There are also adverts for hacking tutorials.	487 topics 1856 comments	542 topics 4187 comments
黑客高手	Intended to gather the highly skilled hackers together but there are no guarantee that the people advertising are indeed.	615 topics 1546 comments	634 topics 1592 comments
黑客论坛	This board is for hacker forums. However, this board contains mostly adverts offering hacking services as well as requests for services. There are also adverts for hacking tutorials.	1794 topics 6405 comments	2040 topics 7732 comments
挂马	This board is about malicious code infection on legitimate Web pages. This board contains services and request for 挂马 as well as for general hacking	8715 topics 22636 comments	8750 topics 17772 comments
3389	This board is a place for adverts for the sale of zombies.	75 topics 225 comments	233 topics 508 comments

Table 2 – bars and usage statistics

Table 2 above shows a number of bars on Baidu Tieba which are used by Chinese cybercriminals as a common marketplace where demands for underground services are met by supply. Topics refer to the number of new distinctive topics created on the bar while comments are comments made within the topics. The topics can be understood as distinctive adverts for underground trading and as shown in table 2, there have been growth in the number of topics in all bars over a period of eight weeks.

Looking at the number of topics, it can be seen that the most popular bars are “visa”, “灰鸽子”, “挂马” and “网马”. This pattern also reflects the most popular underground hacking activities in cybercrime today. The “visa” bar represents carding activities, “灰鸽子” is the name of the most powerful Chinese Trojan used to gain remote control of compromised machines and this represents botnet forming activities, “挂马” (infecting legitimate Web pages with malware) is widely understood to be the most popular way of delivering malware and “网马” means Web Trojans, which are commonly used to exploit vulnerabilities in Web browsers.

4.1.2 QQ and QQ Group (群)

For private conversations, the Chinese cybercriminals prefer to use Tencent's QQ Instant Messenger⁵⁵ (IM) as it is the most popular instant messenger in China with over 567million registered users⁵⁶. The QQ IM operates in similar ways to the ICQ (I Seek You)⁵⁷ instant messenger which is popular in the West. Each registered is assigned a unique number, known as the QQ number and this number is then used to uniquely identify a user.

Below is a comparison of ICQ's user interface with QQ's:



Figure 23 – ICQ 7 VS QQ 2010

Figure 23 shows the user interface of ICQ (on the left) and QQ (on the right). Both display the contact list of individual users vertically and the users of either messenger are free to start a conversation with any other users. Figure 24 below shows a conversation between two Chinese carders in the middle of trading a track 201.

⁵⁵ QQ Instant Messger - <http://im.qq.com>

⁵⁶ The Emerging Online Giants - http://www.economist.com/node/16539424?story_id=16539424

⁵⁷ ICQ – <http://www.icq.com>



Figure 24 – negotiation with a Chinese carder

However, QQ is more than just an instant messenger. QQ also offers a social networking service called QQ Group and its functionality is identical to that of an IRC (Internet Relay Chat) channel. However, unlike an IRC channel which is purely text based, multimedia content including text, images and webcam sessions can be used on QQ groups. The web interface of the QQ group service simply provides access to all the groups the user belongs to, as shown in figure 25 below:



Figure 25 – the web interface for QQ groups

Figure 26 below shows the interface once inside the group:



Figure 26 – inside a QQ group

In order to create a QQ group, one would have to pay a fee using “QQ coin”. The exact fee depends on the maximum size of the group. The group creator has full administrative control over the group, such as deciding whether membership should be open, verified members only or closed. In addition, the group administrator has full control of whether group conversations should be kept.



Figure 27 – QQ IM interface for QQ groups

There are various sub-functions within a QQ group including a group photo gallery, a summary of recent dialogues, a forum (which the carders do not use) and records of all members and their contact details, as shown in figure 26. Moreover, QQ groups are not only accessible via its web interface. The QQ messenger allows group members to communicate with other members instantly. In figure 27 above, the conversation box for the QQ group is shown on the left while the list of QQ groups the user belongs to is shown on the right. The interface is almost identical to the interface for private conversations and group members are notified of any new comments on the group in the same way as they are notified of any private messages.

It has been demonstrated in this section that the QQ messenger is a very powerful communication tool equivalent to the combination of the ICQ and an IRC client in the West. Furthermore, the QQ messenger and the QQ group service allow the Chinese cybercriminals to form closed communities with the luxury of instant messaging each other. With the loose control of the Baidu Tieba for posting advertisements to attract new carders, it is easy to see why there is little need for the Chinese carders to operate private carding forums.

4.1.3 Online forums (BBS)

Although forums are not popular for carding in China, it has been observed during this investigation that one Chinese carding forum was launched, as shown in figure 28 below:



Figure 28 – a screenshot of fuckbank.tk

The forum is called “fuckbank” (<http://www.fuckbank.tk>) and it was first advertised on the ‘visa’ bar on Baidu Tieba by a user named “lookthebank”⁵⁸ on the 20th July, 2010. The advertiser hid the URL in an image on his Baidu profile to prevent it from being indexed and searched. The site was also seen to have been promoted on QQ groups by two QQ users: 法克 Bank (#79047314) and 白板 (#404493144).

⁵⁸ Advert for fuckbank.tk on Baidu Tieba - <http://tieba.baidu.com/f?kz=833472802>

Fuckbank is a forum akin to those observed in the West with similar layout as well as functions offered. There are sub-forums for reviewed vendors, trading, rippers reporting as well as knowledge exchange sections related to dumps, CVV and international online financial institutions such as WebMoney. Membership is free and open to anyone although access to the content posted does not require membership at all. The forum also offers a quick access to an online ICQ service called “icq 2 go”, perhaps to facilitate communication for carders using ICQ. These identical features suggests that the administrator has had affiliations with Western carding forums and has now launched his very own Chinese carding forum using the layout he has observed from the Western forums.

Lastly, since it has been first advertised, the membership has seen very slow growth with only 52 members being recorded on 20th Sept., 2010. This supports the argument above that Chinese carders prefer the use of less centralised services such as Baidu Tieba and QQ groups.

4.1.4 Taobao

Taobao⁵⁹ is China’s biggest online trading platform akin to eBay in the West. Users be sellers and sell items or be buyers and purchase items. While eBay is affiliated with Paypal, Taobao is mainly affiliated with Alipay⁶⁰, the Chinese equivalent of Paypal. During this investigation, underground economy goods have been observed to be traded openly on Taobao, as shown in figure 29 below:



Figure 29 – “flesh chicken” sold on Taobao

Figure 29 shows an advert selling compromised machines for 0.2 RMB per machine and there have been 1209 sales in the last 30 days. While it is stated in the terms and conditions that such goods are not permitted, enforcement appears to be very lax.

Taobao is a popular place for Chinese cybercriminals because there are no admin charges for sellers and buyers have the power to review the purchased goods before instructing the payment system, Alipay, to forward the paid funds to the seller to complete the transaction.

4.2 Advertised Goods and Services

⁵⁹ Taobao – <http://www.taobao.com>

⁶⁰ Alipay – <https://www.alipay.com>

This section details some of the goods and services which have been advertised during the investigation. In the list below, all listed prices are in US dollars. Due to the nature of the way Chinese cybercriminals advertise their goods and services as described in the previous section, the prices offered by Chinese cybercriminals were mostly obtained from private negotiations, unlike those obtained in Franklin and Paxson's work where they correlated prices by parsing IRC messages using natural language processing (Franklin 2007). The Western prices are drawn from Symantec's study of the underground economy (Fossi 2008) as well as (Symantec 2010).

4.2.1 Financial goods and services

Financial goods and services directly related to carding, such as those documented in appendix B.

Goods	Western Price (USD)	CN Price (USD) per unit
UK credit cards + cvv2	\$0.50 - \$12	Normal - \$3.7 - \$5 With 3D- \$22 - \$44
US credit cards + cvv2	\$0.50 - \$12	Normal - \$1.7 - \$2
EU credit cards + cvv2 e.g. DE FR	\$0.50 - \$12	Normal - FR \$5.9
CN credit cards + cvv2	\$0.50 - \$12	Normal - \$17
UK 101/201	N/A	Track 101: Classic = \$1.47 per track Gold = \$1.76 per track Platinum = \$2.06 per track Track 201: Classic = \$1.34 to 1.63 per track Gold = \$1.63 to \$2.08 per track Platinum = \$1.93 to \$2.53 per track U.S. Discover = \$15
US 101/201	N/A	Track 101: Classic = \$1.26 per track Gold = \$0.89 to \$1.71 per track Platinum = \$1.19 to \$1.937 per track
FR 101/201	N/A	Track 201: V/M = \$11.9 per track
Japan 101/201	N/A	Track 201: JCB = \$14.89 V/M = \$10.42
Dumps	\$4 - \$150	\$74.46
Bank logins	\$15 - \$850	Bank BOA Us : Balance \$7000 = \$300 Balance \$14000 = \$500 Balance \$18000 = \$800 Bank HSBC (US) : Balance \$12000 = 400 Balance \$28000 = 1000 Bank HSBC (UK) : Balance GBP 8000 = \$300 Balance GBP 17000 = \$700

Table 3 – financial goods and services offered

Table 3 above shows a comparison between the prices documented in Symantec's reports on the underground economy with the prices of similar goods offered by Chinese cybercriminals. An overall observation is that the prices offered in China generally fall within the range observed by Symantec in the West and this is because Chinese carders do not just trade among themselves but they also trade with foreign carders. As shown in figure 30 below, one interesting observation made during this investigation the Chinese carders' frequent use of foreign carding sites which sell carding

merchandises such as tracks and dumps (see Appendix B) just like normal online commerce sites where wanted goods can be added to a user basket and the user can check out and pay once finished. Using such sites, no communication is necessary and there is no doubt such sites are bring carders from around the world into a unified global carding underground economy.

BIN	Name	Exp	City	State	Country	ZIP	Price	
■■■■■	Debi	03/11	■■■■■	■■■	US	■■■■■	1.50+0	<input type="checkbox"/>
■■■■■	Tiffany	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	tiry	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	Penny	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	Jeannie	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	Jeannine	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	alfred	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	Mindy	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	dawn	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	Janet	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>
■■■■■	John	03/11	■■■■■	■■■	US	■■■■■	1.60+0	<input type="checkbox"/>

Figure 30 - interface of carding site ltdcc.com

Several other key observations include:

- U.S. goods such as Credit Card + CVV2 and tracks are the cheapest compared with other countries.
- The price of Chinese Credit Card + CVV2 is above the range documented by Symantec, possibly due to the scarcity of Chinese credit card data relative to the availability of foreign data.
- Cards with 3D credentials are approximately 7-8 times more than normal cards. A possible explanation is that 3D credentials would give the carders great convenience to cash-out as the cards can be used for online purchasing.
- The relative low prices of UK and US goods suggest that they are more often targeted than other countries such as France and Japan.

4.2.2 Malware

Malware refer to the malicious softwares that are used to exploit vulnerabilities to install more malware, steal data as well as gaining remote control of compromised machines.

Goods	Western price (USD)	CN Price (USD) per unit
Trojans (木马)	\$15 - \$40	Target China banks (ICBC and BC): \$22.33
Anti-security/Packer (木马免杀)	N/A	Guaranteed effective: For 10 days = \$14.89 For one month = \$29.78 to \$44.67
Trojan generator	N/A	\$4.46 - \$298

Table 4 – prices of malware observed in Chinese underground economy

Table 4 above shows that the Trojans targeting the Chinese banks ICBC and BC (see appendix A) are valued at \$22.33 which falls within the range of the prices observed by Symantec in the West. Although these Trojans targets Chinese banks, their prices are similar to that in the West which suggests that the technical difficulties in needing to steal the data as well as the security of the online banking data are similar to that in the West. During the investigation, it was also observed that QQ Trojan generators were offered for as little as \$4.46 and this may suggest why more QQ credentials are stolen than bank logins, as documented in section 2.2. Also, the low pricing of the generator could also suggest that there is a high supply for this kind of product.

4.2.3 Technical Support Services

Technical support services refer to those that provide the technical tools or services which would facilitate the commission cybercrimes. From table 5, it can be seen that the sale of zombies (compromised computers) are priced depending on their location e.g. household or Internet caf  s as well as whether webcam control. It can be seen that those with webcam control are nearly twice as expensive as those without.

Services	Western Price (USD)	CN Price (USD) per unit
Zombie sales	A botnet can be sold for \$550 including hosting	\$0.11 – \$0.22 per zombie \$15 for 1000 household zombies \$15 for 1500 traffic zombies/Internet caf�� zombies \$15 for 500-700 zombies with webcam control
DDoS attacks (DDoS ����)	\$60 - \$80 per day	\$89 to \$298 (24 hour attack)
Money laundering/Mule service/Cashier	N/A	50:50 split
Hacking training/tutorial	N/A	\$22 to \$149 (per student)
IP address	N/A	10,000 IPs = \$18

Table 5 – prices of technical services offered

In the West, it has been noted by SOCA that a botnet including hosting could be sold for \$550. In China though, botnets are rarely sold as a whole. Rather, zombies are sold individually or as a batch. There are also different prices depending on whether there is webcam control, where the webcam is facing and whether the user is female.

For the purpose of research, the author of the thesis made enquiries to two DDoS attackers about the typical price for a DDoS attack on a UK online casino for a period of 24 hours. An online casino was chosen because casinos are often targeted in online extortions. Subsequently, two different prices, \$89 and \$298 were offered. One explanation for the significant difference between the two offers may be attributed to the size of the botnets controlled by each of the attackers. The one with a bigger botnet would be able to offer lower prices because the attack would occupy less of his resources. Comparing with similar kinds of attack in the West, the prices from China are generally beyond the typical Western price range. Several possible explanations for this observation: first is that this may suggest the botnet sizes held by Chinese DDoS attackers may be smaller than those monitored in the West; secondly, there may be less DDoS attackers in China than in the West.

Lastly, Chinese cybercriminals were often seen offering private tutorials to newcomers and the prices observed are shown in table 5. As can be seen, the prices are very low when compared with the possible reward after learning the techniques required for committing cybercrimes and this is worrying because this further lowers the barrier to entry to cybercrime.

Chapter 5 Conclusion

With 420 million Internet users, China has now become the world's largest Internet population. In terms of Internet security, this means that the security of the Chinese Internet is significant to the global Internet and this is why cybercrime in China has been studied in this thesis.

Cybercrime, as observed by Western scholars and security experts, is a phenomenon which has arisen from many different factors from both social and technical aspects. It has been observed during this study that the most influential motivations for Chinese cybercriminals are political and economical. According to CNNIC, 94.9% of all Internet users have a monthly average salary below 5000 RMB (£479) which is equivalent to the average weekly income in the U.K.. Furthermore, around 30% of the Internet population in China are students have an average monthly income of less than 500 RMB per month (£47). Yet, the commodities in China are not always cheap and some even costs the same as in the U.K.. Coupled with widely reported news of the lucrative nature of cybercrime, it is easy to understand why cybercriminals have emerged in China.

Chinese hackers are always perceived by the Western media as mystical and powerful. In this thesis, the Chinese hacking community and hacktivism was examined. Chinese politically motivated hackers, the Chinese *hacktivists*, emerged as early as 1997. Several key cyberconflicts have seen a few large organised hacktivist groups disband and many new smaller hacker groups emerge. Coincidentally, a cyberconflict against Japan occurred during the course of this study. This incident has shown that Chinese hacktivism is not a myth and there are hackers out there who would launch organised attacks against foreign national Internet infrastructures in response to political matters. However, the problem appears not to be as widespread as some may fear. Despite evidence of a large hacking community in China, most hacker forums in China have shown no affiliation with Chinese cyberattacks on Japanese websites, only those who publicly claim to be hacktivists. Furthermore, even the hacktivists themselves disagree over the value in launching cyberattacks against websites. Lastly, it has been observed that the Chinese government do intervene with such hacktivism but leniency is shown towards the hacktivists.

As summarised in chapter two, there are three major types of cybercrimes: computer assisted crimes, pure computer crimes and computer content crime. These three types also give rise to three major types of criminals on the Internet: traditional organised criminals, cybercriminals and ideologically and politically motivated criminals. As cybercrime evolve, networks of chains of need have formed and an underground economy has emerged where labour is continuously deskilled and reskilled.

By studying news reports of the most high profile cybercrime cases in both China and the West, it can be concluded not only does organised crime exists in China, the nature of the Chinese underground economy is just as well defined as those observed in the West. In fact, the size of the Chinese underground economy may be much larger than that of the West because it has been estimated by Chinese security experts that the potential worth of the Chinese underground economy would soon reach 10billion RMB (US\$1.48 billion). This is far larger than the figure reported in 2008 by Symantec who estimated the total amount of the advertised goods they observed was worth approximately US\$276 million.

Lastly in chapter four, a detailed investigation into the Chinese underground economy has exposed the ways in which Chinese cybercriminals trade, which were found to be significantly different from the observations made in the West. It has been found that the Chinese cybercriminals prefer to form ephemeral relations and use more decentralised means to trade with each other, such as services

offered by Baidu Tieba and QQ. Underground economy goods have also been observed to be openly traded on reputable trading platform such as Taobao. This is in direct contrast to their Western counterparts who mostly trade using online forums. This is further supported by the slow emergence of a Chinese carding forum called fuckbank. Despite intense advertising as well as free open membership, it has only managed to attract 52 members after nearly two months since launched. This could perhaps be the reason why the Chinese underground economy could be as big as it has been estimated.

Finally, the prices of some of the commonly traded underground economy goods were obtained through private conversations with Chinese cybercriminals. It was found that in general, carding merchandises are priced similarly in China and in the West. One explanation is the availability of carding websites which operate in similar formats as e-commerce websites where wanted goods are added to user baskets and checkout when finish. Such sites eliminate the need for negotiations, thus removing tradition boundaries such as language and location boundaries. This suggests that carding in the West and China may not be as clearly segregated as this study has set out to be and that the Chinese cybercriminals do trade with Western cybercriminals. This further supports the view that cybercrimes are not bounded by traditional boundaries and that it is a truly global phenomenon. With regards to malware and technical support services, small variations in prices between the West and China were observed and this may be due to the need for more detailed negotiations and specific targets such as Chinese applications. Thus, the language barrier can still be an important boundary confining underground economy activities within specific countries.

References

- Akamai (2010) *The State of the Internet*. Available from: <http://www.akamai.com/stateoftheinternet/>.
- Anderson, R. (2008) *Security Engineering* 2nd ed. Indianapolis: Wiley Publishing.
- Bizuel, D. (2007) *Russian Business Network Study*. Available from: http://www.bizeul.org/files/RBN_study.pdf.
- Callahan, W. (2004) *National Insecurities: Humiliation, Salvation, and Chinese Nationalism*. Available from: <http://www.humiliationstudies.org/documents/CallahanChina.pdf>.
- Choo, K. (2008a) Organised crime groups in cyberspace: a typology. IN: *Trends in organised crime*, Vol. 11(3) pp. 270-295. DOI: <http://dx.doi.org/10.1007/s12117-008-9038-9>.
- Choo, K. (2008b) Money laundering risks of prepaid stored value cards. IN: *Trends & Issues in Crime and Criminal Justice*, No. 363. Available from: <http://www.aic.gov.au/documents/E/5/9/%7BE59FC149-DBEF-46DE-AFF4-5653992E88BE%7Dtandi363.pdf>.
- CNNIC (2010) *China Internet Development Statics Report*. Available from: <http://www.cnnic.net.cn/uploadfiles/pdf/2010/1/15/101600.pdf>.
- CNCERT/CC and CNNIC (2010) *2009 China Netizen Internet Information Security State Investigation Report*. Available from: <http://www.cert.org.cn/UserFiles/File/1.doc>.
- CyberSource (2010). *Sixth Annual UK Online Fraud Report: Online Payment Fraud Trends, Merchant & Consumer Response (2010 edition)*. Available from: <http://forms.cybersource.com/forms/FraudReport2010UKCYBSwww260110>.
- Elser, D. and Pekrul, M. (2009) *Inside the Password-Stealing Business: the Who and How of Identity Theft*. McAfee. Available from: http://www.mcafee.com/us/local_content/reports/6622rpt_password_stealers_0709_en.pdf.
- Fossi, M. et al. (2008). *Symantec Report on the Underground Economy*. Symantec. Available from: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_underground_economy_report_11-2008-14525717.en-us.pdf.
- Franklin, J. et al. (2007) An Inquiry into the Nature and Causes of the Wealth of Internet Miscreants. IN: *Proceedings of the 14th ACM conference on Computer and Communications Security*, Virginia: Computer and Communications Security, pp. 375-388. DOI: <http://doi.acm.org/10.1145/1315245.1315292>.
- Grabosky, P. (2007) The Internet, Technology, and Organized Crime. IN: *Asian Journal of Criminology*, Vol. 2(2) pp. 145-161. DOI: <http://dx.doi.org/10.1007/s11417-007-9034-z>.
- Henderson, S. (2007) *The Dark Visitor – Inside the World of Chinese Hackers*. Lulu Press.
- Holz, T., Engelberth, M. and Freiling, F. (2008) *Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones*. DOI: <http://madoc.bib.uni-mannheim.de/madoc/volltexte/2008/2160/>.
- Home Office (2010) *Cyber Crime Strategy*. Available from: <http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf>.
- Information Warfare Monitor (2009) *Tracking GhostNet: Investigating a Cyber Espionage Network*. Available from: <http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network>.
- Information Warfare Monitor and Shadowserver Foundation (2010) *Shadows in the cloud: Investigating Cyber Espionage 2.0*. Available from: <http://www.scribd.com/doc/29435784/SHADOWS-IN-THE-CLOUD-Investigating-Cyber-Espionage-2-0>.

IOSC of the PRC (2010) *The Internet In China*. Available from: http://www.gov.cn/english/2010-06/08/content_1622956.htm#.

Jellenc, E. and Zenz, K. (2007) *Global Threat Research Report: Russia*. iDefense, A VeriSign Company. Available from: <http://www.verisign.com/static/042139.pdf>.

Jewkes, Y. and Yar, M. (2010) Introduction: the Internet, cybercrime and the challenges of the twenty first century IN: Jewkes, Y. and Yar, M. (eds.) *The Handbook of Internet Crime*. Devon: Willan Publishing.

Kanich, C. et al. (2008) Spamlytics: An Empirical Analysis of Spam Marketing Conversion. IN: *Proceedings of the 15th ACM conference on Computer and Communications Security*, Virginia: Computer and Communications Security, pp. 3-14. DOI: <http://doi.acm.org/10.1145/1455770.1455774>.

Krekel, B. (2009) Capability of the People's republic of China to Conduct Cyber Warfare and Computer Network Exploitation. *U.S.-China Economic and Security Review Commission*. Available from: http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

Li, N. and Kirkup, G. (2005) Gender and cultural differences in Internet use: A study of China and the UK. IN: *Proceedings of Computers & Education*, Volume 48, Issue 2, February 2007, pp. 301-317. DOI: <http://dx.doi.org/10.1016/j.compedu.2005.01.007>.

Lu, H., Liang, B. and Taylor, M. (2010) A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States. IN: *Asian Journal of Criminology*. DOI: <http://dx.doi.org/10.1007/s11417-010-9092-5>.

McAfee (2006). *McAfee Virtual Criminology Report: Organised Crime and the Internet*. Available from: http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_virtual_criminology_report_2007.zip.

Moore, T., Clayton, R. and Anderson R. (2009) The Economics of Online Crime IN: *Journal of Economic Perspectives*, vol. 23(3), pp. 3-20. Available from: <http://people.seas.harvard.edu/~tmoore/jep09.pdf>.

Muttil, I. (2008) *Securing Virtual Worlds Against Real Attacks*. McAfee. Available from: http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_online_gaming.pdf.

Paget, F. (2009) *Financial Fraud and Internet Banking: Threats and Countermeasures*. Available from: http://www.mcafee.com/us/local_content/reports/6168rpt_fraud_0409.pdf.

Paget, F. (2010) *Cybercrime and Hacktivism*. McAfee Labs. Available from: http://entercept.biz/us/local_content/white_papers/cybercrime_20100315_en.pdf.

Peiravi, A. and Peiravi, M. (2010) Internet security – cyber crime Paradox. IN: *Journal of American Science*, Vol. 6(1) pp. 15-24. Available from: http://www.americanscience.org/journals/am-sci/am0601/02_1046_Internet_Security_am0601.pdf.

Peretti, K. (2008) *Data Breaches: What the Underground World Of “Carding” Reveals*. U.S. Department of Justice. Available from: <http://www.chtlj.org/sites/default/files/media/articles/v025/v025.i2.Peretti.pdf>.

Project Grey Goose (2008) *Russia/Georgia Cyber War – Findings and Analysis*. Available from: <http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>.

Qi, M., Wang, Y., and Xu, R. (2009) Fighting cybercrime: legislation in China. IN: *International Journal of Electronic Security and Digital Forensics*, Vol. 2(2) pp.219-227. DOI: <http://dx.doi.org/10.1504/IJESDF.2009.024905>.

- Sandywell, B. (2010) On the globalisation of crime: the Internet and new criminality IN: Jewkes, Y. and Yar, M. (eds.) *The Handbook of Internet Crime*. Devon: Willan Publishing.
- Smith, R. (2010) Identity theft and fraud IN: Jewkes, Y. and Yar, M. (eds.) *The Handbook of Internet Crime*. Devon: Willan Publishing.
- Symantec (2010) *Symantec Global Internet Security Threat Report: Trends for 2009*. Available from: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf.
- Thomas, R. and Martin, J. (2006) The underground economy: priceless. IN: *Proceedings of USENIX ;login.*, 31(6) December 2006. Available from: <http://www.usenix.org/publications/login/2006-12/openpdfs/cymru.pdf>.
- Department of Justice (2003) *Operation Firewall Indictment*. Available from: <http://www.justice.gov/usao/nj/press/files/pdffiles/firewallindct1028.pdf#search=%22firewallindct1028.pdf%22>.
- Zhuge, J. et al. (2007) Characterizing the IRC-based Botnet Phenomenon. IN: *Peking University & University of Mannheim Technical Report*. Available from: http://www.honeynet.org.cn/downloads/publication/TR_IRC_Botnet.pdf.
- Zhuge, J. et al. (2008) Studying Malicious Websites and the Underground Economy on the Chinese Web. IN: *Proceedings of the 7th Workshop on the Economics of Information Security (WEIS'08)* Hanover, NH, USA, June 2008. Available from: <http://weis2008.econinfosec.org/papers/Holz.pdf>.
- Wall, D. (2008) *Cybercrime*. Cambridge: Polity.
- Wilson C. (2008) *Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*. Congressional Research Service. Available from: <http://www.fas.org/sgp/crs/terror/RL32114.pdf>.
- Yong, P. (n/a) *Comparative Research on "Convention on Cybercrime" and Chinese Relevant Legislation*. Council of Europe. Available from: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/countryprofiles/567%20china-d-Comparative%20Research_ed1a.PDF.

Appendix A - Useful Chinese terms

Goods, services and other related terms:

Chinese	English
虚拟社会	Virtual society/world
计算机	Computer
互联网	Internet
网站	Website
网民	Netizens
骗子	Trickster
黑客	Hacker
地下经济	Underground economy
地下黑市	Underground market
地下黑色经济产业链	Underground black economy production chain
银行	Bank
银行卡	Bank card
信用卡	Credit card
信用虚拟卡	Virtual credit card
普卡, 金卡, 白金卡	Normal, gold, platinum credit card
3D 卡	Credit card with 3D credentials
磁道信息/卡料	Exact copy of the magnetic stripe
101/201	Track 101/Track 201
内料	Dumps from within China
外料	Dumps from outside China
游戏点卡	Gaming points card
平台	Platform
外挂/插件	Plug-in
肉鸡	Zombie machine
木马	Trojan
木马免杀	Preventing a Trojan from being destroyed (anti anti-virus)
数据库	Database
系统	System
流程	Flow
一手	First hand
身份证	Identity card
生成器	Generator
数据	Data
质量	Quality
技术	Technique
服务	Service
QQ 号	The user ID for the QQ instant messenger
金融	Finance
信誉	Reputation
额度	Credit limit
复制器	Copier
服务器	Server

采集器	Eavesdropper
额度	Credit card limit
刀 (=美元)	American dollar
W	The abbreviation for the Chinese pin yin of 10,000 e.g. 2W = 20k

Actions:

Chinese	English
充卡	Carding
破解	Cracking
交易	Trading
攻击	Attacking
钓鱼	Phishing
储蓄	Saving
入侵	Intruding
收买/收购	Buying/Requesting
卖	Selling
出售	For sale
刷	Swipe
合作	Collaborating
求	Requesting/begging
培训	Training
聊天	Chatting
防范	Defending/Defence
接货	Drop
汇钱	Money transfer
取钱	Money withdrawal
威胁	Threaten
远控	Remote control

Some abbreviations for virtual payment systems:

PP	Paypal
MB	Moneybooker
C2P	Click2Pay
LR	Liberty Reserve
WM	WebMoney (including WMZ)

Slangs are found to take the pin yin of the initials of the names of the banks. They could well be used to refer to banks, although no such usage has been observed.

Chinese name	English name	Abbrev.	Chinese slang
中国工商银行	Industrial and Commercial Bank of China	ICBC	“爱存不存”
中国建设银行	Construction Bank of China	CBC	“存不存？”
中国银行	Bank of China	BC	“不存。”
中国农业银行	Agriculture Bank of China	ABC	“啊,不存！”

招行银行	China Merchants Bank	CMBC	"存吗?? 白痴!"
兴业银行	Industrial Bank	CIB	"存一百。"
国家开发银行	China Development Bank	CDB	"存点吧!"
北京市商业银行	Beijing City commercial Bank	BCCB	"白存存不?"
汇丰银行	Hong Kong and Shanghai Banking Corporation	HSBC	"还是不存。"

Appendix B – Carding merchandises

Dumps: generally refers to information electronically copied from the magnetic stripe on the back of credit and debit cards. This is referred to as “full-track data” by the banking industry, referencing the two tracks of data (Track 1 and Track 2 on the magnetic stripe) (Peretti 2008). Dumps for sale often contain at least track 2 data but often contain both tracks.

Track 1 (also known as **101**): contains the customer’s name and account number.

Track 2 (also known as **201**): contains the account number, expiration date and the secure code (CVV) and discretionary institution data. This is to prevent “card present” fraud.

Credit card number (CC): this refers to the number on the face of the credit card. In order for a carder to engage in card present fraud, he must have CC + CVV.

CVV2: refers to the 3 to 4 digits printed on the back of a card. This is used to deter card-not-present frauds.

3D: this refers to the authentication details required by an additional security mechanism called 3-D Secure. It is designed to protect online payments. 3-D Secure service is offered as Verified by Visa, MasterCard SecureCode and J/Secure for Visa, MasterCard and JCB cards respectively.

Fulls or fullz: this refers to a package of personal identifying data about a victim including address, phone number, social security number, credit history report and mother’s maiden name.