# An Investigation into Chinese Cybercrime and the Applicability of Social Network Analysis


Michael Yip
Web Science Doctoral Training Centre
University of Southampton
my2e09@ecs.soton.ac.uk

SOCA
SERIOUS ORGANISED CRIME AGENCY

UNIVERSITY OF Southampton
School of Electronics and Computer Science


## Introduction


With the support from the UK's Serious Organised Crime Agency (SOCA), the findings from a two-month comparison study between the underground economy in China and the West are presented. Significant differences were found which are due to traditional boundaries of crime, such as cultural and language barriers. Lastly, Social Network Analysis (SNA) is proposed and discussed as a tool for future cybercrime research.


## Cybercrime: West versus China

This study was set out to investigate the existence of organised cybercrime in China with a specific focus on carding, a criminal practice associated with the illicit use of third party credit cards. The practitioners are known as carders. Not only is organised cybercrime found to exist in China but a sophisticated underground economy is also flourishing rapidly.

While the Western cybercriminals prefer to use closed membership online forums which commonly have a hierarchical management structure (*figure 1*) that helps to enforce a reputation based trust mechanism to fight off the relentless army of rippers who seek to cheat other members, the Chinese cybercriminals prefer to use more decentralised means such as the Baidu Tieba (*figure 3*), an open public message forum and the QQ Instant Messenger *(figure 2*), China's most popular instant messenger. Interestingly, since the posts on Baidu Tieba are indexed by Baidu's search engine, China's most popular search engine, rippers can be reported by having their details published on Baidu Tieba. Thus, anyone who seeks to avoid the rippers only need to search for the QQ number of the person they are intending to trade with. If it is found then that person is a ripper. In this sense, the Chinese cybercriminals have implemented a decentralised form of trust mechanism that eliminates the need to use forums which are vulnerable to police undercover operations.

Furthermore, some Chinese carders were found to be using Western "dump" sites (*figure 4*) to purchase stolen credit card and personal data including social security numbers and address. It is believed that this type of carding sites help to eliminate the language barriers which exist in the underground economy as negotiations are often needed to replace the absence of trust. Therefore, these websites are facilitating the trading between cybercriminals speaking different languages and in effect, globalising the underground economy of carding.

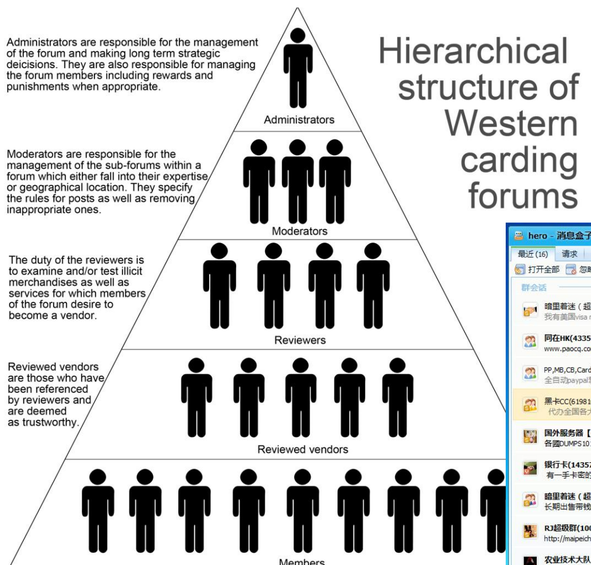


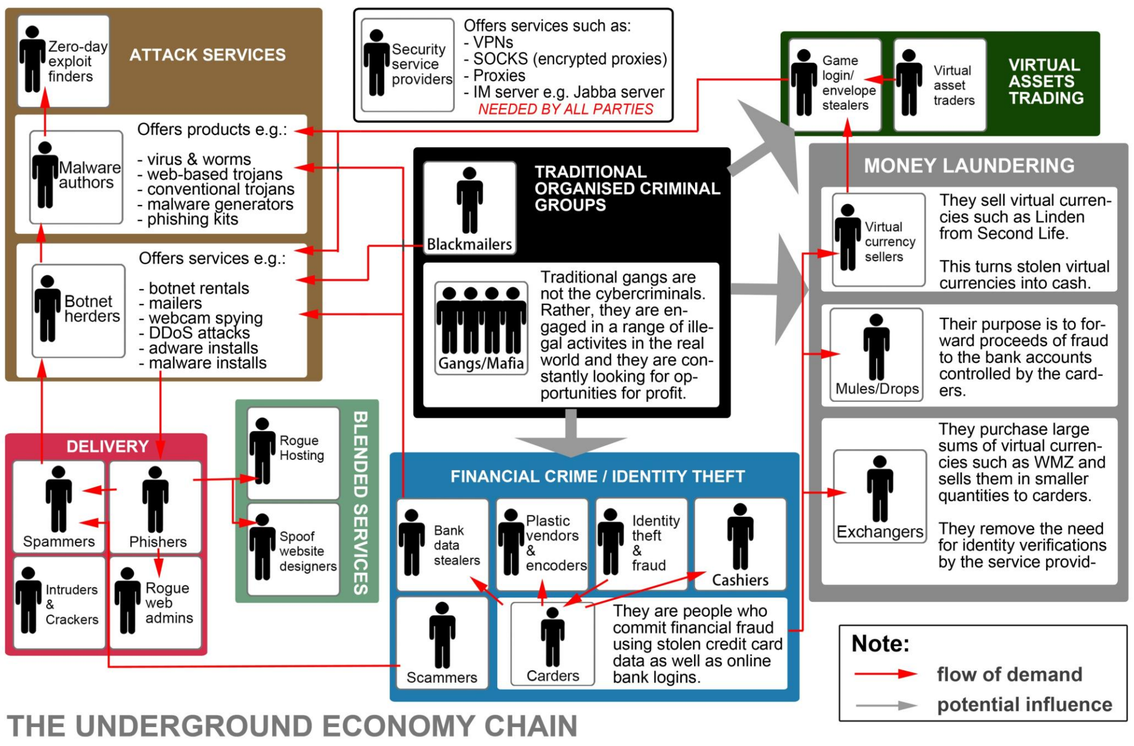

**Figure 1: Hierarchical structure of Western carding forums**




**Figure 3: the "visa" bar on *Baidu Tieba,* a popular online discussion board for Chinese carding advertisements**




**Figure 4: a foreign "dump" site which sells stolen credit card data just like conventional e-commerce websites such as Amazon**




THE UNDERGROUND ECONOMY CHAIN

**Figure 5: a mapping of the online underground economy**

## Social Network Analysis (SNA)

From the findings presented, it is evident that there is a strong need for the profit-seeking cybercriminals to establish social ties with others (*figure 5*). Therefore, to further our understanding on cybercrime, one potentially fruitful direction is to study and reason these social ties as well as the resulting network structure.

It has been proposed that the least common denominator of organised crime is human relationships. Social networking is inevitable for the provision of illicit goods and services as well as the protection, regulation and extortion of those engaged in the provision or consumption of these goods and services. This process of social networking occurs as part of a social system of organised crime, a system which explains the remarkable consistency of the process of organising crime across time and space. Therefore, to understand organised cybercrime, researchers and analysts should focus on discovering the pattern of relationships (ties) and to understand why and how they occur. This can be achieved using Social Network Analysis (SNA), which is a theoretical and methodological paradigm for sophisticated examination of complex social structures. SNA includes:

1. **Network analysis** – detection of structural changes in social networks with node and group level measurements. Node level metrics in this category includes degree centrality, betweenness and closeness. Thus, the evolution of cybercriminal networks can be studied and the changes over time can be reasoned using social psychology and criminology theories.
2. **Social psychology** – it has been argued that any network analysis on human social system risk an incomplete analysis if qualities of the actors are ignored. Such qualities include an individual's demographic factors (e.g. age, sex), capacities (e.g. skill, expertise) and also personal attitude and beliefs.

## Conclusion

As it has been shown, organised cybercrimes are flourishing in China. With a rapidly increasing Internet presence, it is in the interest of security experts to increase their attention on China's cybersecurity. Furthermore, since it has been shown that there is a strong need for profit-seeking cybercriminals to establish social ties with others, the application of Social Network Analysis could be fruitful in future cybercrime research.

## Acknowledgement


I would like to thank the Web Science Doctoral Training Centre at the University of Southampton and the Serious Organised Crime Agency for their kind support throughout this investigation.

It must be clarified that all views and conclusions presented are those of the author and should not be interpreted as representing official policies or endorsements of SOCA. All stolen data encountered during the course of this study have been reported to SOCA.